Qihai Zhou (Ed.)

Theoretical and Mathematical Foundations of Computer Science

Second International Conference, ICTMF 2011
Singapore, May 2011
Selected Papers

Springer

Communications
in Computer and Information Science   164

Qihai Zhou (Ed.)

Theoretical and Mathematical Foundations of Computer Science

Second International Conference, ICTMF 2011
Singapore, May 5-6, 2011
Selected Papers

Springer

Volume Editor

Qihai Zhou
Southwestern University of Finance and Economics
No. 55 Guanghuacun Street, 610074 Chengdu, China
E-mail: qihai@iita-association.org

Preface

The present book, published as volume 164 of the *Communications in Computer and Information Sciences* (CCIS) series, includes 84 extended and revised versions of selected papers from the 2011 Second International Conference on on Theoretical and Mathematical Foundations of Computer Science (ICTMF 2011). The conference was held in Singapore together with the 2011 Second International Conference High-Performance Networking, Computing and Communications Systems (ICHCC 2011). Revised selected papers of the latter conference are published as volume 163 of the CCIS series. The ICHCC-ICTMF 2011 conferences were organized by the Intelligent Information Technology Application Research Association (IITA), Nanyang Technological University, and SMU.

The goal of ICHCC-ICTMF 2011 was to bring together researchers from academia and industry as well as practitioners to share ideas, problems, and solutions relating to the multifaceted aspects of high-performance networking, computing and communication systems, theoretical and mathematical foundations of computer science.

Being crucial for the development of high-performance networking, computing and communication systems, theoretical and mathematical foundations of computer science, our conference encompassed a large number of research topics and applications: from computational science, engineering and technology to digital signal processing; from computational biology to game theory and other related topics, which are included in the scope of this conference.

In order to ensure a high-quality international conference, we had a high-quality reviewing course, undertaken by experts from home and abroad, with low-quality papers being rejected.

Nothing would have been done without the help of the Program Chairs, organization staff, and the members of the Program Committees. Thank you!

We hope readers will gather lots of information from these meaningful papers.

April 2011   Qihai Zhou

ICHCC-ICTMF 2011 Organization

Honorary Chair

David Wang   IEEE Nanotechnology Council Cambodia Chapter, Cambodia

General Chairs

Honghua Tan   Wuhan Institute of Technology, China

Jun Zhang   Huazhong University of Science and Technology, China

Program Co-chairs

Qingyuan Zhou   Jiangsu Teachers University of Technology, China

Mark Zhou   Hong Kong Education Society, Hong Kong

Organizing Co-chairs

Liangming Zhang   Hong Kong University, Hong Kong

Qihai Zhou   Southwestern University of Finance and Economics, China

Publication Co-chairs

Yanwen Wu   Huazhong Normal University, China

Qihai Zhou   Southwestern University of Finance and Economics, China

Program Committee

Chen Da David   University of Mauritius, Mauritius

Younghoon Lee   Cheju National University, South Korea

Deng Wei   Mongolian University of Science and Technology, Mongolia

Paris Kitsos   Cheju National University, South Korea

Shi Yuanchun   Cheju National University, South Korea

Kouichi Sakurai   Cheju National University, South Korea

Yang Xiaohong   Nanjing University, China

Yi Zhang   Beijing Normal University, China

Jun Liu   Shangdong University, China

Garry Zhu	Thompson Rivers University, Kamloops, Canada
David Lee	Thompson Rivers University, Kamloops, Canada
Khine Soe Thaung	Maldives College of Higher Education, Maldives
Biswanath Vokkarane	Society on Social Implications of Technology and Engineering, Hong Kong
Zhang Yun	Hong Kong University, Hong Kong
David Zhang	Hong Kong University, Hong Kong
Deepak Agarwal	University of Guyana, Guyana
Aris Anagnostopoulos	University of Guyana, Guyana
Zhu Min	Nanchang University, China
Junqiao Xiong	Wuhan University, China
LouLuo Moucard	IEEE Gambia GRSS Chapter Chair
Mark Zhou	Hong Kong Education Society, Hong Kong
Yiyi Zhouzhou	Azerbaijan State Oil Academy, Azerbaijan
Khine Soe Thaung	Maldives College of Higher Education, Maldives
Biswanath Vokkarane	Society on Social Implications of Technology and Engineering, Hong Kong
Garry Zhu	Thompson Rivers University, Canada
Ying Zhang	Wuhan University, China
Srinivas Aluru	ACM NUS Singapore Chapter, Singapore
Tatsuya Akutsu	ACM NUS Singapore Chapter, Singapore

Table of Contents

Numerical Study for the Effects of Injection Parameters on Flow Fields of the Blockerless Thrust Reverser

Yun-Hao Zhang[1], Eriqitai[2], and Xiao-Xing Li[1]

[1] School of Mechanical Engineering and Automaiton, BeiHang University,
Beijing, 100191, P.R. China
[2] School of Jet Propulsion, BeiHang University, Beijing, 100191, P.R. China

Abstract. In this paper, CFD was used to simulate the flow fields of the blockerless thrust reverser model. Based on the numerical simulation, the effects of different injection parameters on cascade flow ratio and injection flow ratio were analyzed. The characteristics of the flow fields were also investigated. It was indicated that location, angle and slot thickness of secondary flow injection had a great influence on the performance of the thrust reverser. Base on the analysis results, we can get the optimum injection parameters.

Keywords: Blockerless thrust reverser, Numerical simulation, Secondary flow injection, Turbofan engine.

1   Introduction

The thrust reverser is the commonly used as the reduction gear, which is mainly used for reducing the landing distance of the airplane; and it is matched with the brake equipments to provide the braking. The large commercial aircraft uses the cascade thrust reverser which uses the blocker door to block engine fan flow and forces the air current turn to the cascade vanes to generate reverse thrust. With the development of the high-bypass-ratio turbofan engines, the disadvantages of the conventional cascade thrust reverser as heavy and high maintenance costs are obvious; NASA, GE and other research organizations have successively carried out the research on the thrust reverser, wherein, the blockerless thrust reverser is one new type thrust reverser [1] which draws more attention. The blockerless thrust reverser leads a small amount of high-pressure core flow and injects the current into the fan flow to form the high-pressure gas curtain blocking the fan flow; moreover, makes it turn to the cascade vanes to generate the reverse thrust[1] [2][3] [4].

In the process of the research on the thrust reverser at present, mainly uses the methods of experimental simulation and numerical simulation. For the restrictions on the experimental techniques, the understanding for the characteristic of the flow field of thrust reverser is not sufficient; however, with the development of the CFD technology, the method of using the numerical simulation to study on the flow field of thrust reverser is used more and more widely.

This paper uses the CFD technology to study the flow field of blockerless thrust reverser and analyzes the characteristics of its flow field. Through the study on the

effect of injection position, injection angle and injection pressure ratio on the performance of the reverse thrust to analyze the effect of the regularity for change in air injection parameter on the performance of the reverse thrust, which is useful for seeking the optimal design parameter when design the thrust reverser.

2   Methodology

2.1   Numerical Calculation Model

The model of the thrust reverser makes the experimental model in the reference [1] as the basis and appropriately simplifies it. This model is a 7.9%-scale model with a fan-to-core bypass ratio of 9 and the cascade vanes of the thrust reverser use the equal-width vane. The position of the secondary flow injection is the internal face of the fan nozzle. To simplify the research, this paper will not consider the effect of the core flow on the entire flow field.

2.2   Method of Calculation

This paper uses the axisymmetric model and considers the flow of the air current in the blockerless thrust reverser as the two-dimensional steady compressible flow. Without considering the effects of the gravity, thermal radiation and chemical reaction in the flow, the three-dimensional compressible flow N-S equation under the Cartesian coordinates can be written as

$$\frac{\partial U}{\partial t} + \frac{\partial F}{\partial x} + \frac{\partial G}{\partial y} + \frac{\partial H}{\partial z} = \frac{\partial Q}{\partial x} + \frac{\partial R}{\partial y} + \frac{\partial S}{\partial z} \qquad (1)$$

In the equation, U is the Conservation variable and the F, G and H are the fluxes and $\frac{\partial Q}{\partial x} + \frac{\partial R}{\partial y} + \frac{\partial S}{\partial z}$ are the viscosity terms.

Currently, in the numerical simulation for the flow field of the thrust reverser, the commonly used turbulence models are SST k-ω model, Realzable k-ε model and RNG k-εmodel[5][6][7][8]. In this paper, it uses the RNG k-ε model which fits relatively well with the experimental data to do the numerical simulation. The discrete scheme of the equation uses the second order upwind difference scheme to obtain the higher calculation accuracy.
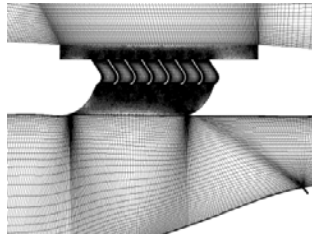
Fig. 1. Two-Dimensional CFD Mesh used to Simulate the Flow Field in the Fan Duct

3   Results and Discussions

3.1   Effect of the Injection Location

The calculation in this part selects five injecting locations to study the influencing regularities of different injection positions to performance of the reverse thrust. In the calculation of this part, set the injection angle as 45 degree. And set the injection width as 0.635mm and set the injection pressure ratio 12. The injection locations are shown in the following table.

Table 1. Setting of the Injection Position

Serial Number	1	2	3	4	5
Air Injection Position （mm）	38.4032	75.2602	85.4202	95.5802	164.0078

As shown in the figure 2, the cascade flow ratio at different injection position is quite different. The cascade flow ratio at the injection position near the throat is relatively higher than the average value; therefore, the optimal air injection position should be near the throat. With the increase of the pressure ratio, the injection flow cannot completely block the fan flow; the unblocked fan flow generates thrust to cause the sharp decline of the reverse thrust. And the injection flow ratio also sharply reduces with the increase of FNPR. The injection flow ratio is high when it is at the low FNPR because the injection flow will baffle the fan nozzle which is at the front of the cascade window; therefore, the fan flow is very low and meanwhile, will cause the engine to break down; therefore, should try the best to avoid it.
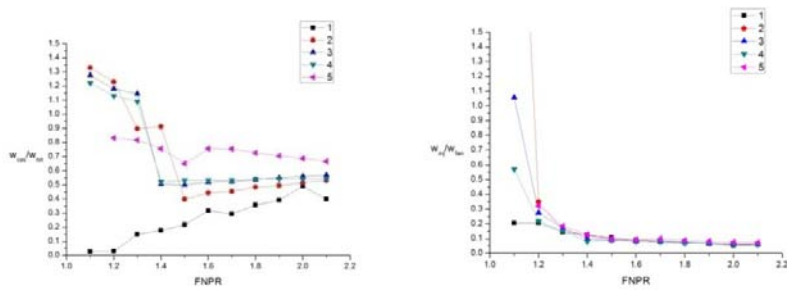
Fig. 2. Effects of the Injection Location on the Cascade Flow Ratio and Injection Flow Ratio

Select the streamlined diagram of each air injection position when FNPR is 1.6 as shown in figure 3. The reflow zone behind the air injection position will gradually increase with the air injection position becomes closer and closer to the throat. The bigger of the reflow zone becomes, the greater effect of the blocking to the fan flow will be. The first three air injection positions cannot form effective blocking for the fan flow; therefore, the cascade window will generate the bigger reflow zone, which

will affect the performance of the reverse thrust. The flow field of the air injection position 4 and 5 are relatively ideal; the flow state in the cascade channel is also similar with the flow state of the conventional cascade thrust reverser and its reverse thrust efficiency is relatively high.

（a） Injection Location 1   （b） Injection Location 2

（c） Injection Location 3   （d） Injection Location 4

（e） Injection Location 5
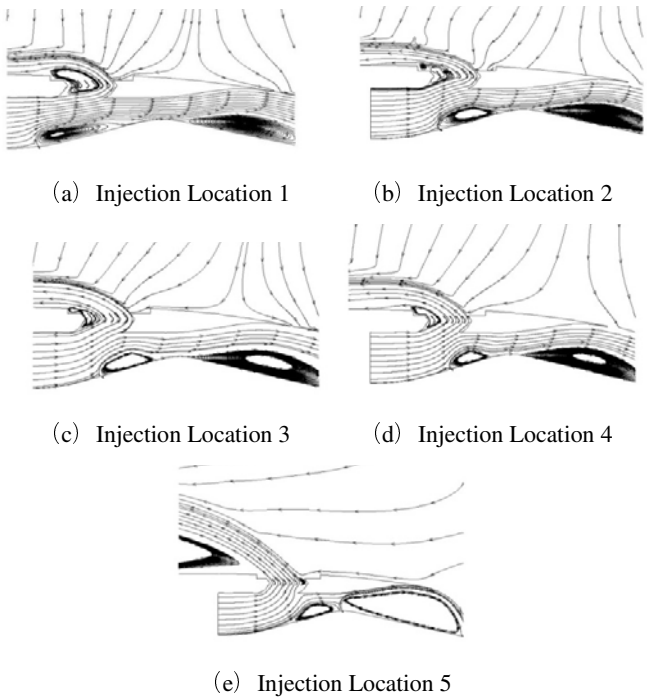
Fig. 3. Streamlined Diagram of the Flow Field at Different Injection Position

3.2   Effect of the Injection Angle

Based on the research result of the front part, select the air injection position 4 whose barrier properties are relatively ideal and change its air injection angle to study the effect on the performance of the reverse thrust. And the settings of the parameters for the air injection seam are shown as the following table.

Table 2. Settings of the Injection Parameters at Different Injection Angles

Parameter	Value
Injection Width （mm）	0.635
Injection Angle （°）	15, 30, 45, 60, 75, 90
Injection Pressure Ratio	12
Injection Location	4

From the calculated results shown in figure 4, we can find that with the increase of the angle, the cascade flow ratio is gradually declining; with the increase of FNPR, the cascade flow ratio sharply dropped at first and then kept steady. For one certain air injection position, there's a optimal air injection angle where its reverse thrust efficiency is the highest. Moreover, the injection flow ratio decreases with the increase of the angle and they seem to be the same at the high FNPR. When the air injection angle is relatively small at the low FNPR, the injection flow ratio is far more than the restriction of 0.05; therefore, selecting the optimal air injection angle needs to consider the reverse thrust efficiency and the injection flow ratio.
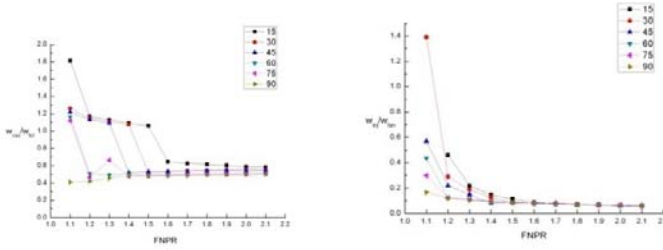
Fig. 4. Effect of Injection Angle on the Cascade Flow Ratio and Injection Flow Ratio

（a）15 Degree   （b）30 Degree

（c）45 Degree   （d）60 Degree

（e）75 Degree   （f）90 Degree
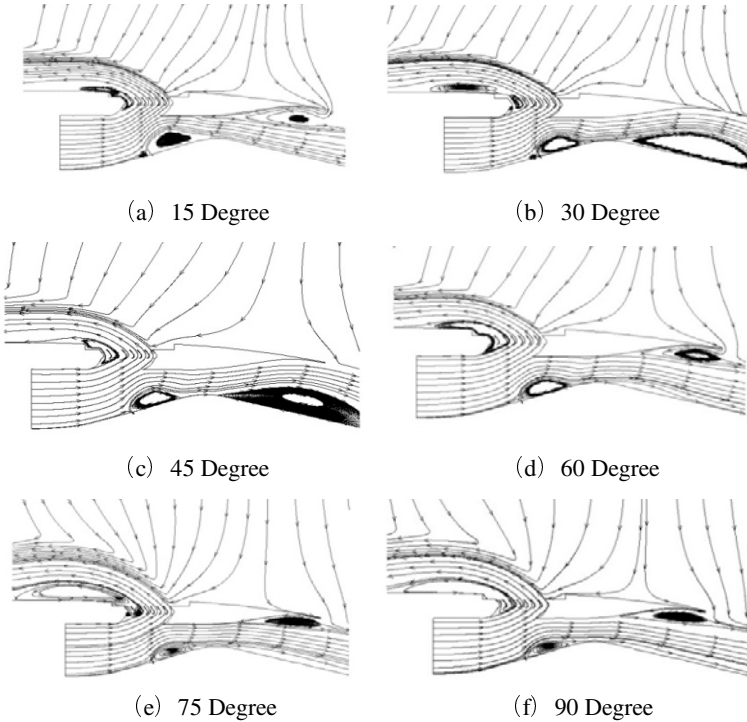
Fig. 5. Streamlined Diagram of the Thrust Reverser at Different Injection Angle

When set the FNPR as 1.6, the streamlined diagrams for each air injection angle are shown as follow and study its characters of the flow field. As shown in the figure 5, it generates relatively large separation zone when the air injection is small and the barrier properties for the external bypass are also good. Because when the air injection angle is relatively small, the component velocity of the air current of the air injection along the flow direction of the air current in the external bypass is relatively larger, which has better barrier properties for the air current in the external bypass. When the air injection angle is too big or too small, then it cannot form the big separation zone to barrier the external bypass. We can notice that when the air current of the air injection cannot barriers the external well, there will form a relatively large recirculation zone at the cascade window, which will affect the reverse thrust efficiency of the entire device. There's an optimal air injection angle at the certain position where its reverse thrust efficiency is low and the flow of the air injection is relatively low. The optimal air injection angle is related with the air injection position, pressure ration of the external bypass and the flow of the air injection.

3.3   Effect of the Injection Pressure Ratio

The injection pressure ratio affects the flow of the air injection much; in the calculation of this part, select four injection pressure ratios to calculate. The settings for the parameters are shown as follow.

Table 3. Settings of the Injection Parameter at Different Injection Pressure Ratios

Parameter	Value
the Injection Width（mm）	0.635
Injection Angle（°）	45
the Injection Pressure Ratio	1.6, 8, 10, 12
Injection Location	4

As shown in the figure 6, the cascade flow ratio o increases with the increase of the injection pressure ratio and the reverse thrust increases with the increase of the injection pressure ratio. When the pressure ratio if bigger than 10, the curve for the cascade flow ratio keeps steady, which means the flow passed through the cascade window is almost saturated and there's no great effect on the reverse thrust when the injection pressure ratio is increased; therefore, there's an optimal injection pressure ratio. For the curve diagram for the injection flow ratio, we can get to know that the injection flow ratio increases with the increase of the injection pressure ratio.

When select the pressure ratios as 1.6, the streamlined diagrams for the different pressure ratios of the air injection are shown as follow. With the increase of the pressure ratio, the separation zone at the back part of the air injection is gradually increased; therefore, the barrier properties for the external bypass will become better and better. All the four air current of the air injections do not completely barrier the external bypass; there's a big recirculation zone at the cascade window, which will affect the reverse thrust efficiency of the entire device.
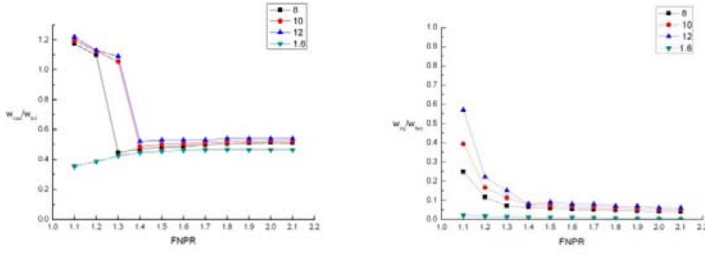
Fig. 6. Effect of the Injection Pressure Ratio on the Cascade Flow Ratio and Injection Flow Ratio

(a) Injection Pressure Ratio 1.6

(b) Injection Pressure Ratio 8

(c) Injection Pressure Ratio 10

(d) Injection Pressure Ratio 12
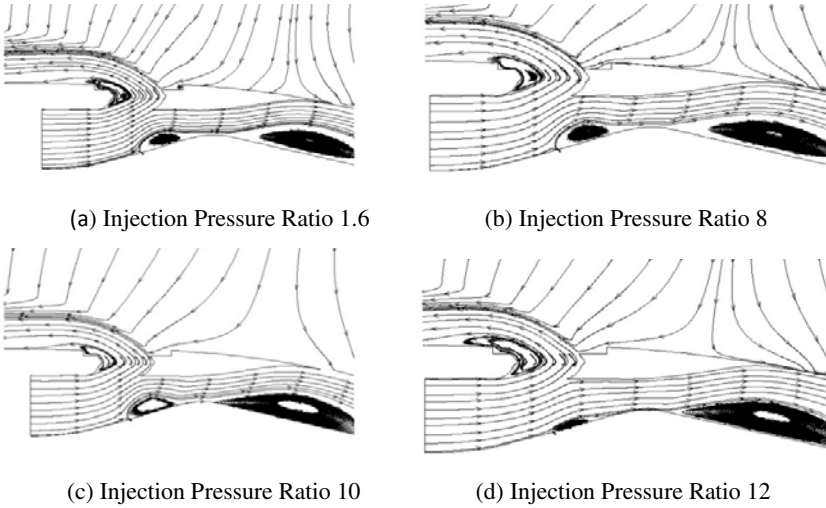
Fig. 7. Streamlined Diagrams for the Thrust Reverser at Different Injection Pressure Ratio when the Pressure Ratio is 1.6

4   Conclusion

This paper uses the CFD technology to do the numerical simulation on the flow field of the blockerless thrust reverser; moreover, it inspects the effect of the injection position, injection angle and the injection width on the performance of the thrust reverser and gets the conclusions as follow:

（1）   To change the injection position, injection angle and the injection width can obviously affect the performance of the reverse thrust in the blockerless thrust reverser. To obtain the optimal injection position near the throat. When the injection angle is relatively small, it can obtain the optimal injection angle. And the injection width can significantly affect the injection flow and further affects the performance of the thrust reverser.

（2） Thrust reverser efficiency and flow injection ratio are two paradoxical performance indexes; to satisfy the design requirement of the injection flow ratio, the reverse thrust efficiency is always discarded to seek the optimal balance point.

（3） The cascade flow does not change a lot with the different air injection states; to seek the optimal reverse thrust performance, it is necessary to improve the design of the cascade vanes according to the concrete characteristics of the flow field.

References

1. Asbury, S.C., Yetter, J.A.: Static Performance of Six Innovative Thrust Reverser Concepts for Subsonic Transport Applications. NASA/TM-2000-210300 (2007)
2. Gilbert, B., Marconi, F.: Innovative concept for cascade thrust reverser without blocker doors. AIAA 1997-0823 (1997)
3. Marconi, F., Gilbert, B.: Computational fluid dynamics support of the development of a blockerless engine thrust reverser concept. AIAA 97-3151 (1997)
4. Hall, S., Cooper, R.: Fluidic Flow Control in a Natural Blockage Thrust Reverser. AIAA 2006-3513 (2006)
5. Yao, H., Raghunathan, S.: Numerical Simulation on Flow Field of the Nature Blockage Thrust Reverser. AIAA 2005-631 (2005)
6. Yao, H., Cooper, R.K.: The effect of the porous diverter fairing on the aerodynamic performance of natural blockage thrust reverser. AIAA 2004-1239 (2004)
7. Nobel, T.P., Wooden, P.A.: Experimental thrust reverser design with computational analysis. AIAA 94-0021 (1994)
8. Romine, B.M., Johnson, W.A.: Performance Investigation of a Fan Thrust Reverser for a High By-Pass Turbofan Engine. AIAA-84-1178 (1984)

Nonconforming H^1-Galerkin Mixed Finite Element Method for Dispersive-Dissipative Wave Equation

Yanmin Zhao[1,2,*], Dongwei Shi[3], and Liang Wu[3]

[1] School of Mathematics and Statistics, Xuchang University,
Xuchang 461000, People's Republic of China
[2] Department of Mathematics, Zhengzhou University,
Zhengzhou 450052, People's Republic of China
[3] Department of Mathematics, Henan Institute of Science and Technology,
Xinxiang 453003, People's Republic of China
{mathzhao,shidw99,nidewuliang}@163.com

Abstract. Based on H^1-Galerkin mixed finite element method, which may get off the requirement of LBB consistency condition, a numerical approximate scheme is established with nonconforming quasi-Wilson element for the dispersive-dissipative wave equation(DDWE). As quasi-Wilson element possesses a special property i.e. the consistency error is one order higher than interpolation error, the corresponding optimal error estimate is derived by the interpolation technique instead of the generalized elliptic projection which is necessary for classical error estimates of finite element method.

Keywords: Dispersive-dissipative wave equation, nonconforming quasi-Wilson element, H^1-Galerkin mixed finite element method, optimal error estimates, interpolation technique.

1 Introduction

With the development of the mixed finite element methods, Pani [1] proposed a new mixed finite element method named H^1-Galerkin mixed finite element method which need not satisfy the LBB consistency condition. From then on, the method has applications in many practical problems, for example, the method is applied to the parabolic partial differential equations[1], hyperbolic type integro-differential equation[2], pseudo-hyperbolic equations[3], Sobolev equations[4] and so on. On the other hand, it is known that the famous nonconforming Wilson element is much better than conforming bilinear element. As an improved Wilson element, quasi-Wilson element is convergent for arbitrary quadrilateral meshes. Recently, Jiang and Cheng[5] proposed a simple quasi-Wilson element which passes Irons patch test and is convergent for arbitrary quadrilateral meshes, this idea comes from Shi and Chen[6]. Shi and Chen[7] extended this element to

---

[*] Corresponding author.

a class of quasi-Wilson elements. Experiments showed that these elements have good numerical results. Chen and Shi[8] proved the consistency error due to non-conformity of elements in [5], Shi and Chen[8] proved that the consistency error of quasi-Wilson element was an order $O(h^2)$, one order higher than of Wilson element. Because of this, the qausi-Wilson element have the better convergence behavior. In this paper, we establish a H^1-Galerkin mixed scheme with non-conforming quasi-Wilson element for the following dispersive-dissipative wave equation[9]

$$
\begin{cases}
u_{tt} - \Delta u_t - \Delta u_{tt} - \Delta u &= f(X), & \text{in } \Omega \times [0,T], \\
u(X,t) &= 0, & \text{on } \partial\Omega \times [0,T], \\
u(X,0) = u_0(X), \quad u_t(X,0) = u_1(X), & & \text{in } \Omega,
\end{cases} \tag{1}
$$

where Ω is a convex polygonal domain in $\mathbb{R}^2$ with Lipschitz continuous boundary $\partial\Omega$, $[0,T]$ is the time interval, $u_0(X), u_1(X)$ are given functions and $f(X)$ is a smooth function. Then, we derive optimal order error estimate by using the above superiority of the proposed method.

2 Construction of the Elements

Let $\hat{K} = [0,1] \times [0,1]$ be a reference element on $\xi - \eta$ plane and $\hat{A}_1 = (0,0), \hat{A}_2 = (1,0), \hat{A}_3 = (1,1), \hat{A}_4 = (0,1)$ be its four vertices.

Next, we define the finite elements $\{\hat{K}, \hat{P}^i, \hat{\Sigma}^i (i = 1,2)\}$

$$
\hat{P}^1 = \text{span}\{N_i(\xi,\eta), (1 \le i \le 4)\}, \quad \hat{\Sigma}^1 = \{\hat{v}_1, \hat{v}_2, \hat{v}_3, \hat{v}_4\},
$$

$$
\hat{P}^2 = \text{span}\{N_i(\xi,\eta), (1 \le i \le 4), \varphi(\xi), \varphi(\eta)\}, \quad \hat{\Sigma}^2 = \{\hat{v}_1, \hat{v}_2, \hat{v}_3, \hat{v}_4, \hat{v}_5, \hat{v}_6\},
$$

where

$$
N_1(\xi,\eta) = (1-\xi)(1-\eta), \ N_2(\xi,\eta) = \xi(1-\eta), \ N_3(\xi,\eta) = \xi\eta, \ N_4(\xi,\eta) = (1-\xi)\eta,
$$

$$
\varphi(t) = -\frac{3}{4}t(t-1) + \frac{5}{32}[(2t-1)^4 - 1],
$$

$$
\hat{v}_i = \hat{v}(\hat{A}_i) \ (1 \le i \le 4), \ \hat{v}_5 = \int_{\hat{K}} \frac{\partial^2 \hat{v}}{\partial \xi^2} d\xi d\eta, \ \hat{v}_6 = \int_{\hat{K}} \frac{\partial^2 \hat{v}}{\partial \eta^2} d\xi d\eta.
$$

The interpolation functions which are well-posed can be expressed as follows:

$$
\hat{I}_h \hat{v} = \sum_{i=1}^{4} N_i(\xi,\eta)\hat{v}_i, \ \hat{I}_h^1 \hat{v} = \sum_{i=1}^{4} N_i(\xi,\eta)\hat{v}_i + \varphi(\xi)\hat{v}_5 + \varphi(\eta)\hat{v}_6.
$$

Let $\Omega \subset \mathbb{R}^2$ be a convex polygonal domain with boundaries $\partial\Omega$ parallel to the axes, and Γ_h be a family of decomposition of Ω with $\bar{\Omega} = \bigcup_{K \in \Gamma_h} K$.

$\forall K \in \Gamma_h$, let $O_K = (x_K, y_K)$ be the center of K, and h_x, h_y be the perpendicular distances between O_K and two sides of K which are parallel to the two coordinate planes, respectively.

The K can be written as

$$K = [x_K - h_x, x_K + h_x] \times [y_K - h_y, y_K + h_y], \ h_K = \max\{h_x, h_y\}, \ h = \max_{K \in \Gamma_h} h_K.$$

The affine mapping $\mathcal{F}_K : \hat{K} \to K$ is defined as follows:

$$\begin{cases} x = x_K + h_x \xi, \\ y = y_K + h_y \eta. \end{cases}$$

Then, the associated finite element spaces V_h and W_h are defined by

$$V_h = \{v^h : v^h \mid_K \in \hat{P}^1 \circ \mathcal{F}_K^{-1}, v^h \mid_{\partial \Omega} = 0\};$$

$W_h = \{\overrightarrow{w}^h = (w_1^h, w_2^h) : w_i^h \mid_K \in \hat{P}^2 \circ \mathcal{F}_K^{-1}, \text{ for any nodal point } a \in \partial \Omega, \overrightarrow{w}^h(a) = (0,0)\}$, then for all $v \in H^2(\Omega)$, $\overrightarrow{w} = (w_1, w_2) \in (H^1(\Omega))^2$, we define the interpolation operators I_h and Π_h as

$$I_h : H^2(\Omega) \to V_h, \ I_h \mid_K = I_K, \ I_K v = (\hat{I}_h \hat{v}) \circ \mathcal{F}_K^{-1}$$

and

$$\Pi_h : (H^1(\Omega))^2 \to W_h, \ \Pi_h \mid_K = \Pi_K, \quad \Pi_K \overrightarrow{w} = ((\hat{I}_h^1 \hat{w}_1) \circ \mathcal{F}_K^{-1}, \ (\hat{I}_h^1 \hat{w}_2) \circ \mathcal{F}_K^{-1}),$$

respectively.

3   Semi-discrete Scheme of the H^1-Galerkin Mixed Finite Method

We split the first equation of (1) into the following system of two equations

$$\nabla u = \overrightarrow{q}, \quad u_{tt} - div \overrightarrow{q_t} - div \overrightarrow{q_{tt}} - div \overrightarrow{q} = f. \tag{2}$$

The weak form of (2) is defined to be a pair $\{u, \overrightarrow{q}\} : [0, T] \to H_0^1(\Omega) \times H(div, \Omega)$ satisfying

$$\begin{cases} (\nabla u, \nabla v) = (\overrightarrow{q}, \nabla v), \quad \forall v \in H_0^1(\Omega), \\ (\overrightarrow{q_{tt}}, \overrightarrow{w}) + (div \overrightarrow{q_t} + div \overrightarrow{q_{tt}} + div \overrightarrow{q}, div \overrightarrow{w}) = (f, div \overrightarrow{w}), \ \forall \overrightarrow{w} \in H(div, \Omega), \\ u(X, 0) = u_0(X), \quad u_t(X, 0) = u_1(X), \qquad \text{in } \Omega. \end{cases} \tag{3}$$

The semi-discrete procedure of H^1-Galerkin mixed finite element method for system (3) is to find a pair $\{u^h, \overrightarrow{q}^h\} : [0, T] \to V_h \times W_h$ such that

$$\begin{cases} (\nabla u^h, \nabla v^h) = (\overrightarrow{q}^h, \nabla v^h), \quad \forall v^h \in V_h, \\ (\overrightarrow{q_{tt}}^h, \overrightarrow{w}^h) + (div \overrightarrow{q_t}^h + div \overrightarrow{q_{tt}}^h + div \overrightarrow{q}^h, div \overrightarrow{w}^h) = (f, div \overrightarrow{w}^h), \ \forall \overrightarrow{w}^h \in W_h, \\ u^h(X, 0) = I_h u_0(X), \quad u_t^h(X, 0) = I_h u_1(X), \qquad \text{in } \Omega. \end{cases} \tag{4}$$

4   Error Estimates

At first, we give a lemma which is important for the error analysis and can be found in [8].

Lemma 1. $\forall u \in H_0^1(\Omega) \bigcap H^2(\Omega), \ \forall \overrightarrow{\psi} \in W_h, \ $ then there holds

$$\Big| \sum_{K \in \Gamma_h} \int_{\partial K} u(\overrightarrow{\psi} \cdot \overrightarrow{n}) ds \Big| \leq Ch|u|_2 \|\overrightarrow{\psi}\|_0,$$

where $\|\overrightarrow{\psi}\|_0^2 = \sum_{K \in \Gamma_h} \|\overrightarrow{\psi}\|_{L^2(K)}^2$ and $\|\overrightarrow{\psi}\|_{H(div;\Omega)}^2 = \|\overrightarrow{\psi}\|_0^2 + \|div\,\overrightarrow{\psi}\|_0^2.$ Here and later, h_K is the length of the longest side of K, $h = \max_{K \in \Gamma_h} h_K$ and C denotes a general positive constant which is independent of h.

Now, we will state the following main result of this paper.

Theorem 1. Suppose $\{u, \overrightarrow{q}\}$ and $\{u^h, \overrightarrow{q}^h\}$ are solutions of (3)and(4), respectively. There holds

$$\|u - u^h\|_h^2 + \|\overrightarrow{q} - \overrightarrow{q}^h\|_{H(div;\Omega)}^2 \leq Ch^2 \int_0^t \chi(\tau) d\tau,$$

where $\chi(\tau) = \|u\|_2^2 + \|u_{tt}\|_1^2 + \|\overrightarrow{q_{tt}}\|_1^2 + \|\overrightarrow{q}\|_1^2 + \|div\overrightarrow{q_t}\|_1^2 + \|div\overrightarrow{q_{tt}}\|_1^2 + \|div\,\overrightarrow{q}\|_1^2.$

Proof: Let $u - u^h = (u - I_h u) + (I_h u - u^h) = \eta + \xi, \quad \overrightarrow{q} - \overrightarrow{q}^h = (\overrightarrow{q} - \Pi_h \overrightarrow{q}) + (\Pi_h \overrightarrow{q} - \overrightarrow{q}^h) = \overrightarrow{\rho} + \overrightarrow{\theta}$, then the error equations can be rewritten as

$$
\begin{cases}
(\nabla \xi, \nabla v^h) = -(\nabla \eta, \nabla v^h) + (\overrightarrow{\rho}, \nabla v^h) + (\overrightarrow{\theta}, \nabla v^h), \\
(\overrightarrow{\theta_{tt}}, \overrightarrow{w}^h) + (div\,\overrightarrow{\theta} + div\overrightarrow{\theta_t} + div\overrightarrow{\theta_{tt}}, div\overrightarrow{w}^h) = \\
\quad -(\overrightarrow{\rho_{tt}}, \overrightarrow{w}^h) - (div\overrightarrow{\rho_t} + div\overrightarrow{\rho_{tt}} + div\,\overrightarrow{\rho}, div\overrightarrow{w}^h) + \sum_{K \in \Gamma_h} \int_{\partial K} u_{tt} \overrightarrow{w}^h \cdot \overrightarrow{n} ds.
\end{cases}
\tag{5}
$$

Setting $v^h = \xi, \quad \overrightarrow{w}^h = \overrightarrow{\theta}$ in (5) and summing its two equations, we get

$$\|\nabla \xi\|_0^2 + \frac{1}{2}\frac{d}{dt}\|\overrightarrow{\theta_t}\|_0^2 + \frac{1}{2}\frac{d}{dt}\|div\overrightarrow{\theta_t}\|_0^2 + \frac{1}{2}\frac{d}{dt}\|div\,\overrightarrow{\theta}\|_0^2 = -(\nabla \eta, \nabla \xi) +$$
$$(\overrightarrow{\rho}, \nabla \xi) + (\overrightarrow{\theta}, \nabla \xi) - (\overrightarrow{\rho_{tt}}, \overrightarrow{\theta_t}) - (div\overrightarrow{\rho_t}, div\overrightarrow{\theta_t}) - (div\overrightarrow{\rho_{tt}}, div\overrightarrow{\theta_t}) -$$
$$(div\overrightarrow{\rho}, div\overrightarrow{\theta_t}) + \sum_{K \in \Gamma_h} \int_{\partial K} u_{tt} \overrightarrow{\theta_t} \cdot \overrightarrow{n} ds = \sum_{i=1}^{8} A_i.
\tag{6}$$

Using Cauchy-Schwartz inequality and Lemma 1, terms on the right side of (6) can be estimated as follows

$$|A_1| = |-(\nabla \eta, \nabla \xi)| \leq C(\|\nabla \eta\|_0^2 + \|\overrightarrow{\rho}\|_0^2) + \varepsilon_1 \|\nabla \xi\|_0^2;$$

$$|A_2| = |(\overrightarrow{\rho}, \nabla \xi)| \leq C(\|\nabla \eta\|_0^2 + \|\overrightarrow{\rho}\|_0^2) + \varepsilon_1 \|\nabla \xi\|_0^2;$$

$$|A_3| = |(\overrightarrow{\theta}, \nabla \xi)| \leq C\|\overrightarrow{\theta}\|_0^2 + \varepsilon_1 \|\nabla \xi\|_0^2;$$

$$|A_4| = |-(\overrightarrow{\rho_{tt}}, \overrightarrow{\theta_t})| \leq C\|\overrightarrow{\rho_{tt}}\|_0^2 + \varepsilon_2 \|\overrightarrow{\theta_t}\|_0^2;$$

$$|A_5| = |-(div\overrightarrow{\rho_t}, div\overrightarrow{\theta_t})| \leq C\|div\overrightarrow{\rho_t}\|_0^2 + \varepsilon_3\|div\overrightarrow{\theta_t}\|_0^2;$$

$$|A_6| = |-(div\overrightarrow{\rho_{tt}}, div\overrightarrow{\theta_t})| \leq C\|div\overrightarrow{\rho_{tt}}\|_0^2 + \varepsilon_3\|div\overrightarrow{\theta_t}\|_0^2;$$

$$|A_7| = |-(div\overrightarrow{\rho}, div\overrightarrow{\theta_t})| \leq C\|div\overrightarrow{\rho}\|_0^2 + \varepsilon_3\|div\overrightarrow{\theta_t}\|_0^2;$$

$$|A_8| = \sum_{K \in \Gamma_h} \int_{\partial K} u_{tt}(\overrightarrow{\theta_t} \cdot \overrightarrow{n})ds \leq Ch|u_{tt}|_2\|\overrightarrow{\theta_t}\|_0 \leq Ch^2\|u_{tt}\|_2^2 + \varepsilon_2\|\overrightarrow{\theta_t}\|_0^2.$$

Integrating both sides of (6) form 0 to t, employing the above estimates and noticing $\int_0^t \|\overrightarrow{\theta}\|_0^2 d\tau \leq \int_0^t (\int_0^\tau \|\overrightarrow{\theta_t}\|_0^2 ds)d\tau \leq C\int_0^t \|\overrightarrow{\theta_t}\|_0^2 d\tau$, the following estimate will be derived by Gronwall's lemma

$$\|\overrightarrow{\theta_t}\|_0^2 + \|div\overrightarrow{\theta_t}\|_0^2 + \|div\overrightarrow{\theta}\|_0^2 \leq C\int_0^t (\|\nabla\eta\|_0^2 + \|\overrightarrow{\rho_{tt}}\|_0^2 + \|\overrightarrow{\rho}\|_0^2 + \|div\overrightarrow{\rho_t}\|_0^2 +$$

$$\|div\overrightarrow{\rho_{tt}}\|_0^2 + \|div\overrightarrow{\rho}\|_0^2)d\tau + Ch^2 \int_0^t \|u_{tt}\|_2^2 d\tau = \sum_{j=1}^7 B_j. \tag{7}$$

By interpolation theory, we have the following estimates

$$B_1 = \int_0^t \|\nabla\eta\|_0^2 d\tau \leq Ch^2 \int_0^t \|u\|_2^2 d\tau;$$

$$B_2 = \int_0^t \|\overrightarrow{\rho_{tt}}\|_0^2 d\tau \leq Ch^2 \int_0^t \|\overrightarrow{q_{tt}}\|_1^2 d\tau;$$

$$B_3 = \int_0^t \|\overrightarrow{\rho}\|_0^2 d\tau \leq Ch^2 \int_0^t \|\overrightarrow{q}\|_1^2 d\tau;$$

$$B_4 = \int_0^t \|div\overrightarrow{\rho_t}\|_0^2 d\tau \leq Ch^2 \int_0^t \|div\overrightarrow{q_t}\|_1^2 d\tau;$$

$$B_5 = \int_0^t \|div\overrightarrow{\rho_{tt}}\|_0^2 d\tau \leq Ch^2 \int_0^t \|div\overrightarrow{q_{tt}}\|_1^2 d\tau;$$

$$B_6 = \int_0^t \|div\overrightarrow{\rho}\|_0^2 d\tau \leq Ch^2 \int_0^t \|div\overrightarrow{q}\|_1^2 d\tau.$$

Based on the above estimates, we gain $\sum_{j=1}^7 B_j \leq Ch^2 \int_0^t \chi(\tau)d\tau.$ (8)

Combining (7) and (8), we can deduce that

$$\|\overrightarrow{\theta_t}\|_0^2 + \|div\overrightarrow{\theta_t}\|_0^2 + \|div\overrightarrow{\theta}\|_0^2 \leq Ch^2 \int_0^t (\|u\|_2^2 + \|u_{tt}\|_1^2 + \|\overrightarrow{q_{tt}}\|_1^2 + \|\overrightarrow{q}\|_1^2 +$$

$$\|div\overrightarrow{q_t}\|_1^2 + \|div\overrightarrow{q_{tt}}\|_1^2 + \|div\overrightarrow{q}\|_1^2)d\tau. \tag{9}$$

Noticing that $\overrightarrow{\theta}(0) = \overrightarrow{0}$, we get $\overrightarrow{\theta}(t) = \int_0^t \overrightarrow{\theta_t}(\tau)d\tau$ and $\|\overrightarrow{\theta}\|_0^2 \leq C\int_0^t \|\overrightarrow{\theta_t}\|_0^2 d\tau$.

Thus, the following estimate can be obtained by (9)

$\|\overrightarrow{\theta}\|_{H(div;\Omega)}^2 = \|\overrightarrow{\theta}\|_0^2 + \|div\,\overrightarrow{\theta}\|_0^2 \leq Ch^2 \int_0^t (\|u\|_2^2 + \|u_{tt}\|_1^2 + \|\overrightarrow{q_{tt}}\|_1^2 + \|\overrightarrow{q}\|_1^2 + \|div\overrightarrow{q_t}\|_1^2 + \|div\overrightarrow{q_{tt}}\|_1^2 + \|div\,\overrightarrow{q}\|_1^2)d\tau$, then the proof of Theorem 1 is completed by use of triangle inequality.

References

1. Pani, A.K.: An H^1-Galerkin Mixed Finite Element Methods for Parabolic Partial Differential Equations. SIAM J. Numer. Anal., 35, 712–727(1998)
2. Shi, D.Y., Wang, H.H.: A New H^1-Galerkin Mixed Finite Element Method for Hyperbolic Type Integro-Differential Equation. Chinese J. Eng. Math., 26(4), 648–652(2009)
3. Liu, Y., Li, H.: H^1-Galerkin Mixed Finite Element Methods for Pseudo-Hyperbolic Equations. Appl. Math. Comput. 212, 446–457(2009)
4. Shi, D.Y., Wang, H.H.: Nonconforming H^1-Galerkin Mixed FEM for Sobolev Equations on Anisotropic Meshes. Acta Math. Appl. Sin., 25(2), 335–344(2009)
5. Jiang, J.S., Cheng, X. L.: A Nonconforming Element Quasi-Wilsons for Second Order Problems. Acta Numer. Math., 14(3), 274–278(1992)
6. Shi, Z.C., Chen, S.C.: An Analysis of A Nine Degree Plate Bending Element of Specht. Acta Numer. Math., 11(3), 312–318(1989)
7. Shi, D.Y., Chen S.C.: A Kind of Improve Wilson Arbitrary Quadrilateral Elements. Numer. Math. J. Chinese Univ., 16(2), 161–167(1994)
8. Chen, S.C., Shi, D.Y.: Accuracy Analysis for Quasi-Wilson Element. Acta Math. Sci. 20(1), 44–48(2000)
9. Shang, Y.D.: Initial Boundary Value Problem of Equation $u_{tt} - \Delta u - \Delta u_t - \Delta u_{tt} = f$. Acta Math. Appl. Sin. 23(3) 385–393(2000)

One Dynamic Hierarchical Data Acquisition Model for Pre-geohazards Information Acquisition

Honghui Wang, Xianguo Tuo, Guiyu Zhang, and Zhaoyi Zhang

State Key Laboratory of Geohazard Prevention and Geoenvironment Protection,
Chengdu University of Technology, Box 5256,
No.1 Erxian Qiao, Dongsan Road,
610059 Chengdu, Sichuan, China
wanghh_945@163.com, txg@cdut.edu.cn

Abstract. In recent years, the geohazards are very serious all over the world, especially in China such as the Wenchuan earthquake-trriggered geohazards and Zhouqu debris flows. As one of the effective and inexpensive approaches, pre-geohazards information monitoring technology is being more and more valued and has attached lots of researchers' interests. Some modern information technologies are adopted to develop the geohazards equipments such as GPRS/GSM/GPS, WSN, and MEMS and the effects are obvious. However, almost most monitoring equipments use fixed-period sampling model which has caused some conflicts among the data redundancy, data integrity, communication costs and the system power consumptions. Thus, one dynamic hierarchical data acquisition (DHDA) model according to the geohazard development characteristics is proposed and the implementation technology is described. Finally, one case study about the model application is developed in the Panzhihua Airport Landslide, China. The results have evinced the DHDA model is effective for pre-geohazards information acquisition.

Keywords: Geohazards – Information acquisition – Landslide displacement – Monitoring – Early warning.

1   Introduction

1.1   Severity of the Geohazard Situation

Every year, countries all over the world have been struck by lots of geohazards. All geohazards have caused substantial human and financial losses. Furthermore, China is one of the countries with serious geohazards in the world, estimated at the annual dead of about 1000 people and the annual cost of approximately 10 billion Yuan (Zhang et al. 2005).

On Monday, May 12, 2008, a devastating mega-earthquake of magnitude 8.0 struck the Wenchuan area, northwestern Sichuan Province, China. The earthquake has triggered lots of secondary geohazards such as rock avalanches, landslides, landslides dams and debris flows. China Geological Survey has identified 4,970 potentially risky sites, 1,701 landslides, 1,844 rock avalanches, 515 debris flows, and 1,093 unstable

slopes (Cui et al. *2009*). There are more than 10,000 potential geohazard sites induced by the Wenchuan earthquake (Yin et al. *2009*). Meanwhile, Lessons from Wenchuan Earthquake tell us that geohazards will continue after the earthquake in active fault regions (Cui et al. *2009*). In all, the geohazard situation of China is very severe.

1.2   Importance and Urgency of the Geohazards Monitoring

Facing to the lots of geohazards and the expensiveness of the mechanical reinforcement measures (Uchimura et al. *2010*), the geohazards monitoring and early warning work is undoubtedly important.

Cui P et al. (Cui et al. *2009*) indicated that after the Wenchuan earthquake, Landslides and rock avalanches will continue for the next 5 or 10 years in the affected areas and debris flow activity for 10 or 20 years. As China has more than 20 earthquake zones in the mountainous area, it is very urgent to carry out geological hazards monitoring work.

As all we know, Geohazards risk reduction is a pressing societal need in mountainous countries and along many coasts, lakes and rivers in other areas. Engineering measures to stabilize dangerous slopes can be costly or impractical in many cases. Monitoring and Warning are the most economical risk-reduction measures for rapid-onset geohazards, and development of early warning systems for mitigating natural risks is a topic of much research around the world (Sassa et al. *2010*). We should take effective monitoring and warning measures to reduce the disaster losses.

1.3   Status of the Pre-geohazards Information Acquisition

According to geohazards characteristics, they can be monitored by catching the pre-hazards information before the disasters. The pre-hazards information can be divided into two parts and one is generated by the geologic bodies such as the earth fissures, rock cracks and tilts, and sonic waves. Another is the external factors which may trigger the geohazards such as rainfalls, typhoons and earthquakes. All the pre-hazards information is the foundation of the geohazards monitoring and early warning. It is very important for geohazard monitoring that how can we obtain these information efficiently.

Yin YP et al. (Yin et al. *2010*) have developed related works, he and his colleagues have established one geohazards monitoring and warning demonstrate station in the Three Gorges Reservoirs area since 1999. The monitoring system mainly acquires the GPS, BOTDR and deep displacement data, and adopts GPRS to transfer data within hours, minutes, or even shorter. Uchimura et al. (Uchimura et al. *2010*) present a low-cost and simple monitoring method for early warning of landslides by employing MEMS tilt sensors in place of extensometers on the slope surface and volumetric water content sensors, and the data are transferred through a wireless network with the cycle of 10 minutes. Sassa et al. (Sassa et al. *2010*) present a study aimed at developing a new computer simulation code integrating the initiation and motion of rapid landslides triggered by earthquake, rain, or their combined effects.

After summarizing the predecessors' research achievements, we can obtain the following primary conclusions about the current situations of the pre-hazards information acquisition: Generally speaking, there are mainly two methods for the pre-hazards information acquisition currently, one is the artificial field acquisition and another is automatic acquisition. The first method needs our technical persons

acquiring the concern data by professional equipments at the monitoring sites and the acquisition cycle is fixed according to the degree of the disaster. At the same time, the automatic approach uses the wireless communication platforms to collect the motoring information. Specifically, first we install the acquiring equipments at the disaster site, and then under the controlling of the MCU (Micro-Control-Unit) embedded in the acquiring equipments, the data will be uploaded to the remote controlling center or saved locally on the basis of the acquisition cycle set by the MCU instruction. The GSM/GPRS/CDMA technologies are always adopted to establish the wireless communication platform. Furthermore, both methods have a common feature that the acquisition cycle is fixed (Also known as fixed-period sampling) and always can't be modified.

2   Model Buildings

2.1   Development Characteristics of Geohazards

On basis of the geohazards characteristics, the developmental process can be divided into two periods: developmental period and disaster-coming period. During the developmental period, the variation of pre-geohazard is too small and the geohazard parameters changing cycle is about several days or even several ten days. On the contrary, the variation is large and the geohazard parameters changing cycle is about several hours or even several minutes.

In this case, if we use the fixed-period sampling method, it will undoubtedly give rise to the data redundancy during the developmental period and data missing during the disaster-coming period. Specifically, a smaller sampling interval will ensure the integrity of data during the disaster-coming period but lead to the data redundancy during the developmental period, and furthermore, the effectiveness of the monitoring system will be greatly reduced because of the promotion of the communication costs and the system power consumptions during the developmental period.

On the other hand, a larger sampling interval will reduce the degree of the data redundancy, the communication costs and the system power consumptions during the developmental period, but lead to the data missing during the disaster-coming period and that is not conducive to disaster early warning and forecast.

Thus, one more effective, dynamic hierarchical data acquisition (DHDA, dynamic hierarchical data acquisition) approach according to the geohazards characteristics is proposed in this paper and the corresponding model and implementation technology are described too.

2.2   Model Present

On basis of the discussion about the geohazards development characteristics, we have merged the dynamic and hierarchical data acquisition thought. The basis thought of the DHDA model is that: on basis of the geohazard risk hierarchical table, we dynamically regulate the current sampling interval according to the pre-geohazard information we have previously acquired. The DHDA model consists of 6 steps as follows:

Step I: Determining the category of the pre-geohazard information concerned. According to the monitoring object's condition, there are mainly - several ten categories we can choose such as displacement, pressure, rainfall, tilt angle, and volumetric water content and so on. We mark the concern category as PGIC-a for example.

Step II: Classing the geohazards based on the risk reflected by the pre-geohazard information we concerned such as PGIC-a. In other words, here we class the geohazards in view of the level of the PGIC-a, not of the risk of the geohazards itself. According to the PGIC-a, the geohazards are classed into $1, 2, 3 \ldots N-1$, N in total of n grades, and then we set the sampling interval as $t_1, t_2, t_3 \ldots t_{N-1}, t_N$ corresponding to the risk grade $(t_1 > t_2 > t_3 > \ldots > t_{N-1} > t_N)$.

Step III: Acquiring the initial value of the PGIC-a. With the motoring equipment set in situ, the MCU embedded in the motoring equipment obtains the initial value as V0 and stores the V0 into the information-comparison memory. The initial sampling interval is determined by experiences and we mark it as $t_m (1 < m < N)$. Especially, here we used a timer integrated in the MCU controlling the data sampling.

Step IV: Acquiring the current value of the PGIC-a. When the sampling interval time is coming, the motoring equipment will acquire the current PGIC-a as V_c.

Step V: Determining the current risk grade of the geohazard. We mark the previous sampling as V_{c-1}, and then we calculate the difference between V_c and V_{c-1} by formula (Equation 1):

$$\triangle = | V_c - V_{c-1} | \tag{1}$$

According to the $\triangle$ value above, we can determine the current risk grade on basis of the geohazard risk hierarchical table.

Step VI: Modifying the current sampling interval. Using the current risk grade determined in the step V, we can modify the sampling interval by using the MCU embedded in the motoring equipment.

In order to facilitate interpretation, finally, one case study about the model application is developed in the Panzhihua Airport Landslide, China.

3   Case Study: The Panzhihua Airport Landslide Displacement Information Acquisition

3.1   Basic Characteristics of the Panzhihua Airport Landslide

Panzhihua City is located in Panzhihua-Xichang Rift Valley, where the topography and geological conditions are quite complex and the Panzhihua Airport is in this belt.(Qin. *2008*). Since September 2009, the NO.12 landslide located in the east of Panzhihua Airport filling body part P140-160 has been developed. The back edge of the landslide appears obvious traction cracks and the cracks begin to widen coupled with slippage. The front retaining walls have been pushed and begin to appear deformation cracks. October 3, the landslide severely slides and is being an unstable state. The landslide is a typical tongue shape, with length of 450m, width of 400m,

thickness of 40m, the volume of about 5 million m^3 and the sliding distance of about 400~450m. By the preliminary estimate, the landslide is a very large one produced in the airport high-fill body.

3.2 Displacement Monitoring

According to site survey situation, we have developed the displacement monitoring programs along the surface fissure groove and Fig. 1 shows the schematic and the field photo of the monitoring approach in situ.
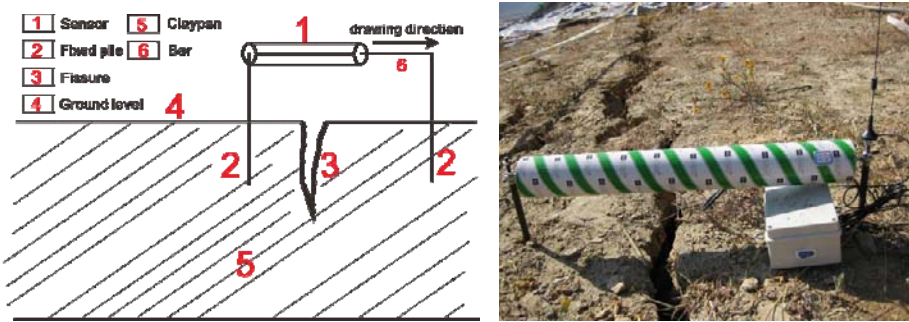
Fig. 1. Schematic and field photo of the monitoring approach in situ

In this case, the system used the resistance-type rod-type displacement sensor and the sensor was set above the fissure. When the fissure enlarges, the pull rod of the sensor will move along the drawing direction. Through the lead wire, the sensor is connected with the data acquisition equipment.

According to the status of the fissure development, we determined 4 grades: 1-grade, 2-grade, 3-grade and 4-grade. At the same time, 4 sampling interval one-to-one corresponding to the 4 risk grades are determined. The t_1 is 3 hours, t_2 is 2 hours, t_3 is 1 hours and the t_4 is 0.5 hours. Furthermore, Table 1 shows the fissure displacement risk grades.

Table 1. Fissure displacement risk hierarchical table

Sampling interval	Grade	The variation of displacement during t_1-sampling interval	The variation of displacement during t_2-sampling interval	The variation of displacement during t_3-sampling interval	The variation of displacement during t_4-sampling interval
t_1=3 hours	1-grade	0~5 mm	0~3 mm	0~2 mm	0~1 mm
t_2=2 hours	2-grade	6~10 mm	4~7 mm	3~4 mm	2~3 mm
t_3=1 hours	3-grade	11~15 mm	8~10 mm	5~6 mm	4~5 mm
t_4=0.5 hours	4-grade	•16 mm	≥11 mm	≥7 mm	≥6 mm

For example, if the Δ value during the t_1 sampling interval is 13 mm, then the current risk grade should be 3-grade according the Table 1. And thus, we should regulate the current sampling interval into t_3 mean to 1 hours sampling interval. Furthermore, if the Δ value during the t_1 sampling interval is 8 mm, then the current risk grade should be 2-grade. And thus, we should regulate the current sampling interval into t_2 mean to 2 hours sampling interval.

3.3   Monitoring Results and Performance Analysis

Table 2 and Table 3 show that the displacement information acquired by using the DHDA model.

Table 2. Displacement value from 00:41:43 to 21:39:19 on Feb 28, 2010

Day time	Sampling time	Displacement value/mm	Δ/mm	Sampling interval/hours
2010/02/28	00:41:43	85	---	3
2010/02/28	03:41:10	85	0	3
2010/02/28	06:40:38	85	0	3
2010/02/28	09:40:06	85	0	3
2010/02/28	12:40:01	85	0	3
2010/02/28	15:39:28	85	0	3
2010/02/28	18:39:24	85	0	3
2010/02/28	21:39:19	85	0	3

Table 3. Displacement value from Dec 4 to Dec 5, 2009

Day	Sampling time	Displacement value /mm	Δ/mm	Sampling interval /hours	Day	Sampling time	Displacement value /mm	Δ/mm	Sampling interval /hours
12/04	11:09:06	119	---	3	12/05	05:41:19	214	9	0.5
12/04	14:09:10	125	6	2	12/05	06:11:50	223	8	0.5
12/04	16:09:38	130	5	2	12/05	06:41:35	231	10	0.5
12/04	18:10:06	132	2	2	12/05	07:11:28	241	6	0.5
12/04	20:10:15	136	4	2	12/05	07:41:56	247	7	0.5
12/05	00:10:28	144	8	2	12/05	08:12:25	254	6	0.5
12/05	01:10:56	151	7	1	12/05	08:42:52	260	6	0.5
12/05	01:40:19	157	6	0.5	12/05	09:12:19	266	7	0.5
12/05	02:11:29	165	8	0.5	12/05	09:42:35	273	7	0.5
12/05	02:41:38	172	7	0.5	12/05	10:12:58	280	7	0.5
12/05	03:11:06	180	8	0.5	12/05	10:42:27	287	9	0.5
12/05	03:41:15	186	6	0.5	12/05	11:12:09	296	10	0.5
12/05	04:10:28	193	7	0.5	12/05	11:42:02	306	12	0.5
12/05	04:40:56	200	6	0.5	12/05	12:41:33	318	20	0.5
12/05	05:10:34	206	8	0.5	12/05	13:11:50	338	24	0.5

From Table 2, if the risk grade is low such as 1-grade, this DHDA model can only acquire 8 data per day and the communication cost is about 0.8 Yuan if the communication service provider is Chinese companies. On the contrary, take 2 hours

sampling interval for example, the traditional approaches which use the fixed-interval sampling technology can acquire 12 data per day and the cost is about 1.2 Yuan. Thus, on the condition of the low risk grade, the DHDA model can save about 1/3 costs per day and the data redundancy is only 2/3 of the traditional method. Furthermore, the larger sampling interval needs the little boot time and so the system power consumption could be reduced considerably.

From Table 3, if the risk grade is high such as 3-grade, the traditional approach can only acquire 13 data on the condition of 2 hours fixed sampling. But the DHDA approach can acquire about 30 data because of the dynamic hierarchical mechanism. So it assures the integrity of the pre-geohazard information during the disaster-coming period although the communication costs and the system power consumption can be slightly increased.

4   Conclusions

Aiming at the traditional geohazards information acquisition conflicts among the data redundancy, data integrity, communication costs and the system power consumptions, one dynamic hierarchical data acquisition model is proposed.Several cognitions are formed from the research as follows:

I: The DHDA model and the corresponding technology enable our monitoring work finding one equilibrium point among the data redundancy, data integrity, communication costs and the system power consumption. Specifically, it can effectively induce the data redundancy during the developmental period and assure the integrity of the information during the disaster-coming period. At the same time, it can also visibility reduce the communication costs and the system power consumption so as to promote the practical applicability and long-lasting of the geohazards monitoring instruments.

II: The DHDA model proposed can also been put into other measuring areas such as environmental monitoring, health monitoring of the buildings and bridges.

III: The risk grade hierarchical table was designed depending on the researchers' experiences and thus there were some errors because of uncertainty. But with the progress of the geohazards monitoring and early warning, the errors will be less and less and the monitoring effect will be better and better.

IV: Because different geohazards have different development characteristics, it needs us designing different risk grade hierarchical tables according to the special sites, and that is the shortcoming of the model.

V: There are still spaces for the implementation algorithm of the model such as two-dimensional fuzzy control and nonlinear algorithm so as to improve the performances.

In all, the application results have evinced that the DHDA model is effective although there are several points need to be studied further.

References

1. Cui, P., Chen, X.Q., Zhu, Y.Y.: The Wenchuan Earthquake, Sichuan Province, China, and resulting geohazards. Nat Hazards 56, 19–36 (2009)
2. Qin, H.: Governance on the Panzhihua Airport NO. 3 landslide. Airport Construction 4, 10–11 (2008) (in Chinese)
3. Sassa, K., Picarelli, L.: Preface for the thematic issue "Early Warning of Landslides". Landslides 7, 217 (2010)
4. Uchimura, T., Towhata, I., Anh, T.T.L.: Simple monitoring method for precaution of landslides watching tilting and water contents on slopes surface. Landslides 7, 351–357 (2010)
5. Yin, Y.P., Wang, H.D., Gao, Y.L.: Real-time monitoring and early warning of landslides at relocated Wushan Town, the Three Gorges Reservoir, China. Landslides 7, 339–349 (2010)
6. Yin, Y.P., Wang, F.W., Sun, P.: Landslide hazards triggered by the 2008 Wenchuan earthquake, Sichuan, China. Landslides 6, 139–152 (2009)
7. Zhang, L.J., Wei, S.H.: Early Warning and Prevention of Geohazards in China. Landslides 4, 285–289 (2005), doi:10.1007/3-540-28680-2_36

Network Content Security Evaluation Method Analysis

Dongyan Zhang[1], Lihua Yin[2], and Hongsong Chen[3]

[1] Dept. of Computer Science & Technology
University of Science & Technology Beijing
Beijing, China
zhangdy@263.net
[2] Institute of Computing Technology
Chinese Academy of Sciences
Beijing, China
yinlihua@software.ict.ac.cn
[3] State key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Dept. of Computer Science & Technology
University of Science and Technology Beijing
Beijing, China
Nowpower_123@yahoo.com.cn

Abstract. The network content security system of Internet information requires a controlling force over information flows which allows the access to some information and prohibits some other information. The complexity of Internet information flows makes it difficult to control precisely over the Internet. Consequently, corresponding evaluation shall be conducted over all kinds of controlling methods. In the paper, precision rate and error rate metrics are proposed to evaluate the network content security system. Consequently we use the evaluation methods in intrusion detection and information retrieval for reference to evaluate the network content security system. We take a deep analysis for the evaluation methods from two aspects which are "monotony" of evaluation methods and the sensibility of evaluation methods and point out which of these methods are applicable to network content security controlling system. At last, we state briefly the application range of CID, ECC, NAMI and other metrics.

Keywords: content security; access control; evaluation method; metric.

1   Introduction

The fast development of the Internet has enabled people to acquire information in a more convenient way. Currently, the Internet has replaced newspapers, TV and other traditional media as the main information source for people, especially for the youth. However, there are also large amount of pornographic, violent and terrorism information that spread on the Internet [1][2], which endangers the physical and psychological health of youngsters. In order to control the illegal flow of the

information, we shall classify and filter all the information during the transmission process, as well as at the target end. As for this, network content security was considered to prevent the harmful information transmission. But how to evaluate the efficiency of the network content security system is very important. Therefore, evaluation of the controlling capability of content security system on the Internet is in fact a research concentration [3].

At present, research on information content security of network still remain at the preliminary stage and they paid more attention to network security evaluation. [4] provides several effective and efficient methods for modeling and analysis of network security, and also analyze network survivability. [5] proposes a model for Information Security Management, called an Information Security Management Model (ISM2) which introduces the idea of international security criteria or international security standards. [6] presents a Colored Petri Net based tool which allows to describe graphically a given network topology, the network security mechanisms and the security goals required. Few researches are conducted on the evaluation methods of network content security. In this paper, we paid more attention to evaluate the content security of the Internet.

However, there are some similarities between the objective of network content security and the objective of intrusion detection and information retrieval. At the same time, there are also obvious differences between content security and intrusion detection, as well as information retrieval. For this reason, we will have to make corresponding research on related evaluation methods over them and make sure which of these methods are applicable to the evaluation of network content security.

The paper mainly discusses evaluation methods that related with precision rate and error rate, so as to analyze which of these methods are applicable to network content security systems evaluation. As for this, we would mainly proceed from three aspects: (1) Equivalency of evaluation methods; (2) "Monotony" of evaluation methods; (3) Sensibility of evaluation methods. Here, sensibility refers to the situation that: if a slight value change of a certain evaluation method A would lead to a major value change of another evaluation method B, we can say that B's sensibility is higher than that of A. Many systems have requirements in sensibility.

2   Overview of Performance Evaluation Methods

Because of the similarity among the network content security and intrusion detection and information retrieval, we are able to use the evaluation methods in intrusion detection and information retrieval for reference to evaluate the network content security system. So we first analyze the evaluation methods in intrusion detection and information retrieval.

The most commonly used evaluation methods [7-12] in information retrieval are: Precision, Recall, Normalized Precision and Recall, ε, F, Receiver Operating Characteristic (ROC), Average Search Length (ASL), Expected Search Length (ESL), response time, system stability and resource occupancy rate. Precision and Recall are the basis of all other evaluation methods (except for ASL, ESL, response time, system stability and resource occupancy rate).

The most frequently used evaluation methods[13-16] in intrusion detection are: True Position Rate (TPR), False Position Rate (FPR), Positive Predictive value (PPV), Negative Predictive value (NPV), CID(Intrusion Detection Capability), ROC, Cost-based Analysis, response time, system stability and resource occupancy rate. True Position Rate and False Position Rate are the basis of all other evaluation methods (except for ASL, ESL, response time, and system stability and resource occupancy rate) for intrusion detection.

2.1   Intrusion Detection Evaluation Metrics

Basic Methods for Intrusion Detection Evaluation:

$$TPR = \frac{a}{a+b} \qquad\qquad FPR = \frac{c}{c+d} \qquad\qquad (1)$$

For intrusion detection, 'a' stands for the volume of intrusion events that have been detected. 'b' stands for the volume of intrusion events that have not been detected. 'c' stands for the volume of normal events that have been mistaken as intrusion events. 'd' stands for the volume of normal events. When using in information retrieval and content security, the meaning of 'a', 'b', 'c' and 'd' remains the same and we will not be explained any more.

We can see that TPR is the probability that intrusion events are successfully detected, while FPR is the probability that normal events are mistaken as intrusion events. The evaluation on TPR and FPR is double-metric evaluation. In most occasions, what we need is synthetically evaluation metric. For this reason, we have to integrate these metrics. In the following, we are going to discuss integration methods applied in intrusion detection.

Set X as the input variable of the Intrusion detector, in which, X=1 stands for that the specified event is intrusion event, while X=0 stands for that the event is normal event. Set Y as the output variable of the intrusion detector, in which, Y=1 stands for warning, while Y=0 stands for non-warning. Consequently the CID method shall be:

$$C_{ID} = \frac{I(X;Y)}{H(X)} \qquad\qquad (2)$$

In the method, H(X) is the information entropy of the variable X. It represents the uncertainty of the variable X. I(X;Y) stands for the mutual information of X and Y. It represents the decrement of the uncertainty of X under the situation that the variable Y is given.

In information theory, $0 \leq I(X;Y) \leq H(X)$, therefore, $0 \leq CID \leq 1$.

When TPR=1 and FPR=0, I(X;Y)=H(X) and CID =1. That is the method of CID can obtain a maximum value when the detection rate is 1 and the false detection rate is 0. It complies with practical meaning.

Normalized Mutual Information (NMI):

$$NMI = \frac{H(X)+H(Y)}{H(X,Y)} \qquad\qquad (3)$$

Entropy Correlation Coefficient (ECC):

$$ECC = 2 - \frac{2H(X,Y)}{H(X) + H(Y)} \tag{4}$$

Normalized Asymmetric Mutual Information (NAMI):

$$NAMI = \frac{I(X;Y)}{H(Y)} \tag{5}$$

The above listed all evaluation methods. The methods were conducted by setting TPR and FPR as the basic evaluation methods without giving consideration to the consequences of false detection and miss detection.

2.2   Specifications Information Retrieval Evaluation Metrics

In the following, we will discuss basic evaluation metrics in information retrieval. In information retrieval, Precision and Recall are separately defined as:

$$Precision = \frac{a}{a+c} \quad Recall = \frac{a}{a+b} \tag{6}$$

Precision stands for the ratio of related documents among all the retrieved documents. Recall stands for the ratio of related documents among all the documents. In order to unify Precision and Recall, researchers have put forward the following evaluation method:

$$\varepsilon = 1 - \frac{2}{Precision^{-1} + recall^{-1}} \tag{7}$$

$$\mathbb{F} = 1 - \varepsilon = \frac{2}{Precision^{-1} + recall^{-1}} \tag{8}$$

Apparently, ε and F contradict with each other. When ε increases, F will decrease.

3   Research on Network Content Security System Evaluation Metric

In content security control, we focus on the detection rate (precision rate) of illegal information flows, as well as the probability that legal information flows are mistaken as illegal information flows (error rate). However, if we merely evaluate the network content security controlling system with precision rate and error rate, we would sometimes feel it difficult to evaluate whether the content security controlling system is good or bad. For example, if the precision rate of A is 0.90, the error rate of A is 0.05, the precision rate of B is 0.85 and error rate of B is 0.02, it would be difficult for us to tell which one is better. Due to the similarity between the content security controlling system and intrusion detection, as well as information retrieval, we can draw lessons from them. We don't make discussions on response time, system stability and resource occupancy rate in intrusion detection and information retrieval.

Different evaluation methods can reflect the different characteristics of the system that we are studying of. In most occasions, these evaluations are incompatible and some of them even conflict with each other. Thus, we should take a deep analysis to observe the methods which are applicable to the network content security.

3.1   Evaluation Metric Analysis

In order to unify the description, we have established four parameters: α, β, γ and δ.

$$\alpha = \frac{d}{c+d} \quad \beta = \frac{a}{a+b} \quad \delta = \frac{c}{a+c} \quad \gamma = \frac{a+b}{a+b+c+d} \tag{9}$$

3.2   Basic Definition

Definition 1 (Basic Input Set, Metrics Set, and Measurement): A tetrad set as the basic input set, $\Delta = \{(\alpha, \beta, \gamma, \delta) \mid 0 \leq \alpha, \beta, \gamma, \delta \leq 1\}$. The meanings of α, β, γ, δ are shown as above. Assume R_1 as the real number set, and R_2 as the finite set. The elements in R_2 are elements in the chain, then:

Quantitative Measurement: M_1: $\Delta \rightarrow R_1$, i.e. The Quantitative Measurement is a mapping from Δ to R_1;

Qualitative Measurement: M_2: $\Delta \rightarrow R_2$, i.e. The Qualitative Measurement is a mapping from Δ to R_2;

From now on, quantitative measurement and qualitative measurement are called measurement for generalization.

In the definition, every element in R_2 shall be combined as the elements in the same chain, i.e. every two random elements shall be comparable. It is necessity for qualitative evaluation.

Definition 2 (Equivalent Measurement): Assume that M_i and M_j are measurements in Δ. For each x $\in$ Δ, we can say that M_i and M_j are equivalent if $M_i(x) = M_j(x)$. We describe it as $M_i \equiv M_j$. If there is a x $\in$ Δ which leads to the result that $M_i(x) \neq M_j(x)$, we can say that M_i and M_j are non-equivalent, described as $M_i \not\equiv M_j$.

If we want to achieve a same evaluation result with different evaluation methods, especially for qualitative measurement, definition 1 is suitable. In quantitative measurement, it is not necessary to always follow such strict equivalent measurement. Instead, we just need to keep certain monotony. As for this, the following definition is then given:

Definition 3 (Mono-equivalent Measurement): Assuming that Mi and Mj are measurements inΔ. For any x, y $\in$ Δ, $M_i(x) \leq M_i(y)$ if and only if $M_j(x) \leq M_j(y)$. For any x, y $\in$ Δ, $M_i(x) > M_i(y)$ if and only if $M_j(x) > M_j(y)$. We can say that Mi and Mj are mono-equivalent measurements which is described as $M_i \triangleq M_j$.

Obviously, ε and F are not mono-equivalent measurements. For any x, y $\in\Delta$, $\varepsilon(x)$ $\leqslant\varepsilon(y)$, if and only if $F(x)\geqslant F(y)$. Defining that $M_1=\alpha/(\alpha+\beta)$, $M_2=2\alpha/(\alpha+\beta)$, then M_1 and M_2 are non-equivalent measurements. However, they are mono-equivalent measurements.

Definition 4 (Interval Mono-equivalent Measurement): Assuming that Mi and Mj are measurements in Δ. We set $\Delta'\subseteq\Delta$. For any x, y$\in\Delta'$, $M_i(x)\leqslant M_i(y)$ if and only if $M_j(x)\leqslant M_j(y)$. We can say that Mi and Mj are mono-equivalent measurements in the interval Δ', described as $M_i \triangleq M_j$.

Mono-equivalent measurement reflects whether different measurement methods lead to the same evaluation result over the same system. However we shall not only give consideration to mono-equivalence, but also take into account the sensibility of different measurement methods in many quantitative measurements. The sensibility of evaluation metric refers to the sensibility of evaluation metric variables.

4   Analysis of Evaluation Metric

Error rate '1-α' and precision rate 'β' are basic evaluation metrics in network content security system evaluation. When we analyze other evaluation methods, we shall take into consideration the relationship between these methods and 'α', 'β' in order to analyze the effective evaluation methods of network content security system. We will discuss separately in the following part.

4.1   C$_{ID}$ Method

CID method is based on information theory and its algorithm is shown in the following:

$$C_{ID} = \frac{I(X;Y)}{H(X)} = \sum_{x,y} Pr(x,y)\log\frac{Pr(x,y)}{Pr(x)\,pr(y)} \tag{10}$$

Firstly, we'll talk about the relationship between CID and error rate.
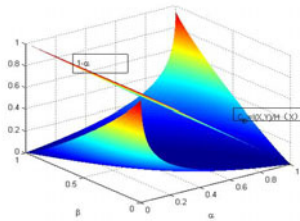
Fig. 1. Comparison between CID and error rate 1-α, γ =0.01

In Figure 1, curved surface can show the variation trend of CID along with the variation of α and β, in which, γ=0.01. The surface closing to a straight line represents

the variation trend of the error rate$1-\alpha$ along with the variation of α and β (actually, the value of $1-\alpha$ has nothing to do with β). The azimuth angle of Figure 2 is -37.5°, and elevation angle is 30°. (The azimuth angle in all figures in the paper is -37.5° and the elevation angle is 30°. We will not explain any more.) From Fig. 2, we can find that the surface of $1-\alpha$ crosses the curved surface of CID. Therefore, CID and the error rate are neither equivalent measurements, nor mono-equivalent measurements. It means that "qualitative" differences may be caused if adopting CID and error rate to evaluate the same system.

Then we analyze the sensibility of CID to α and β. From Fig. 1, we find that the sensibility of CID to α and β would be very strong when the error rate and miss rate are quite large or quite small. The sensibility of CID to α and β would be weaker when α and β approach to 0.5. When α and β approach to 0, the sensibility of CID to α is strong than its sensibility to β. Similarly, the sensibility of CID to α is strong than its sensibility to β when α and β approach to 1.

The curved surface in Fig. 2 shows the variation trend of CID along with α and β, in which γ=0.01. The flat surface in Fig. 3 complies with the β as the measurement. From Fig. 2, we also find the curved surface of CID crosses the flat surface with β. It indicates that CID and error rate are neither equivalent nor mono-equivalent.

Fig. 3 shows the comparison between CID and β in the interval of [0.5, 1], in which γ=0.01. In the figure, we can find that the method CID is always located below the interval of [0.5, 1]. It indicates that CID and β are mono-equivalent in the interval of [0.5, 1].In network content security system, α and β may be larger than 0.50
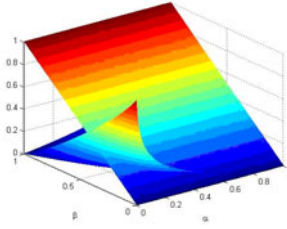
Fig. 2. Comparison between CID and the precision β, γ =0.01
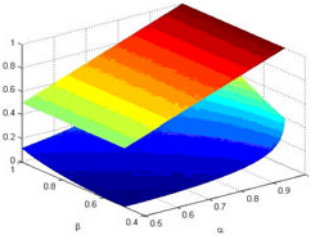
Fig. 3. Comparison between CID and β in the Interval of [0.5, 1]

because information channels are difficult to be captured and contents are not easy to be identified. In Fig. 3 also shows that the controlling effect is under a poor situation and CID still approaches to it maximum value 1 when α and β approaches to 0. It contradicts with practical significance. The fact can prove that CID would not be suitable for evaluation method for content security system when error rate and miss rate are very large.

4.2   Methods of ECC and NAMI

Fig. 4 and Fig. 5 are separately comparison between ECC and $1-\alpha$, as well as NAMI and $1-\alpha$, in which γ=0.01. We find that $1-\alpha$ has divided NMI into two parts. Thus, ECC, NAMI and error rate are not mono-equivalent. When miss rate and error rate approaches to 0 or 1, the value of both ECC and NAMI would approach to 1. It means that ECC and NAMI are not suitable to the valuation of network content security system with larger miss rate and error rate. It also shows that ECC and NAMI would be suitable only if there are strict controlling requirements over the miss rate and error rate of the network content security system. Besides, Fig. 4 and Fig. 5 also show that ECC and NAMI are quite sensitive to error rate and their sensibility to miss rate is weak.
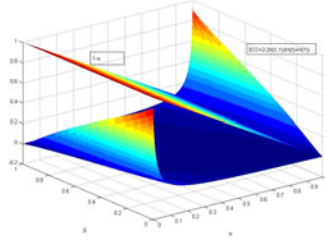
Fig. 4. Comparison of ECC and $1-\alpha$, γ=0.01
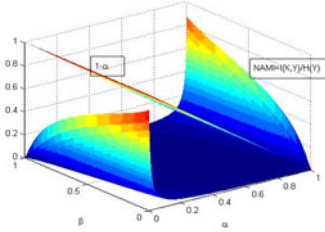
Fig. 5. Comparison of NAMI and $1-\alpha$, γ=0.01

5   Conclusion

Network content security system is to control the illegal flow of the information and prevent the harmful information transmitting in the Internet. In the paper, metrics of

precision rate and error rate are proposed to evaluate the network content security system. Because of similarity with the intrusion detection and information retrieval, we analyze the evaluation methods using in intrusion detection and information retrieval from two aspects which are "monotony" of evaluation methods and the sensibility of evaluation methods. We also find evaluation methods which are suitable to network content security controlling system. From experiments, the results show that the sensibility of CID, ECC and NAMI to error rate is higher than their sensibility to miss rate if the rate of illegal information flow is less than 0.5. It is suitable for using CID evaluation method when miss rate and error rate are less than 0.5. ECC and NAMI are applicable to the environment with higher requirements on miss rate and error rate. All these measures have provided theoretical references for selecting different evaluation metrics according different applications.

References

[1] Stanton, J.J.: Terror in cyberspace: terrorists will exploit and widen the gap between governing structures and the public. American Behavioral Scientist 45(6), 1017–1032 (2002)

[2] Goth, G.: Terror on the Internet: a complex issue and getting harder. IEEE Distributed Systems Online 9(3), 3 (2008)

[3] Fang, B., Guo, Y., Zhou, Y.: Information content security on the Internet: the control model and its evaluation. Science China: Information Sciences 53(1), 30–49 (2009)

[4] Lin, C., Wang, Y., Li, Q.L.: Stochastic modeling and evaluation for network security. Chinese Journal of Computers 28(12), 1943–1956 (2005)

[5] Solms, R.V., Haar, H.V., Solms, S.H., Caelli, W.J.: A framework for information security evaluation. Information & Management 26(3), 143–153 (1994)

[6] Laborde, R., Nasser, B., Barrère, F., Benzekri, A.: A formal approach for the evaluation of network security mechanisms based on RBAC policies. Electronic Notes in Theoretical Computer Science 121(4), 117–142 (2005)

[7] Singhal, A.: Modern information retrieval: A brief overview. Bulletin of the IEEE Computer Society Technical Committee on Data Engineering 4(4), 35–43 (2001)

[8] Christopher, D., Manning, P.R., Hinrich, S.: Introduction to information retrieval. Cambridge University Press, Cambridge (2008)

[9] Melvin, E.: An historical note on the origins of probabilistic indexing. Information Processing and Management 44, 971–972 (2008)

[10] Turpin, A., Scholer, F.: User performance versus precision measures for simple search tasks. In: Proceedings of the 29th Annual international ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 11–18 (2006)

[11] Information retrieval,
`http://en.wikipedia.org/wiki/Information_retrieval`

[12] Bace, R.: Intrusion detection. Macmillan Technical Publishing, vol.156, pp. 237–238 (2000)

[13] Northcutt, S., Novak, J.: Network intrusion detection. New Riders Publishing, Indianapolis (2002)

[14] Tsai, J.J.P.: Intrusion detection: a machine learning approach. Imperial College Press, London (2011)

[15] Denning, D.: An intrusion-detection mode. IEEE Transactions on Software Engineering 13(2), 222–232 (2006)

[16] Mukherjee, B., Heberlein, L.T., Levitt, K.N.: Network intrusion detection. IEEE Network 8(3), 26–41 (1994)

Images Denoising by Improved Non-Local Means Algorithm

Ning He[1] and Ke Lu[2]

[1] School of Information, Beijing Union University, Beijing, 100101, China
`xxthening@buu.edu.cn`
[2] College of Computing & Communication Engineering,
Graduate University of Chinese Academy of Sciences, Beijing, 100049, China
`luk@gucas.ac.cn`

Abstract. A variety of methods have been introduced to remove noise from digital images. However, many algorithms remove the fine details and structure of the image in addition to the noise because of assumptions made about the frequency content of the image. The non-local means algorithm does not make these assumptions, but instead assumes that the image contains an extensive amount of redundancy. This work will implement the non-local means algorithm and compare it to other denoising methods in experimental results. The main focus of this paper is to propose an improved non-local means algorithm addressing the preservation of structure in a digital image. The NL-means algorithm is proven to be asymptotically optimal under a generic statistical image model. The powerful evaluation method to be the visualization of the method noise on natural images.

Keywords: Image denoising; Non-Local means; Local Smoothing Filter.

1   Introduction

Image denoising is a classical problem in image processing [1]. The goal is to estimate the original image f of a given observed image I using some regularization. Many algorithms have been proposed to solve this problem. Basic approaches for denoising, such as Gaussian and median filtering, have a tendency to over-smooth edges and remove image detail. More sophisticated approaches use the properties of natural image statistics to enhance large intensity edges and suppress lower intensity edges. This property has been used by wavelet methods [2], anisotropic diffusion [3], bilateral filtering [4], and Field of Experts models [5]. The non-local means (NL-means) image denoising algorithm [6] is introduced based on weighted averaging and similarity of patches. In addition to standard, direct comparison, reduction of computational cost using principal component analysis (PCA) has been employed with promising results [7]. The NL-means method allows a large number of pixels of the search window participate in denoising. Although this means participation of many relevant pixels, at the same time a large number of irrelevant pixels will be considered in the averaging. Removing irrelevant candidate pixels based on the set of low dimensional features

(obtained in PCA method) has also been used successfully [8]. An alternative strategy based on the singular value decomposition to eliminate non-similar pairs has been used [9]. In this work, a robust selection of the relevant pixels method is proposed which is completely automatic.

2   Non-Local Means Denoising

The NL-means denoising algorithm replaces the noisy gray-values $I(i)$ of each pixel i with a weighted average of the gray-values of all pixels on the image I. We denote by i the pixel to be denoised (or target pixel) and by j the candidate pixel used to denoise. The estimate value $\hat{I}(i)$ for a pixel i is computed based on the weighted average of all the pixels j on the image:

$$\hat{I}(i) = \sum_{j \in N_i^s} w_{ij} I(j) \cdot$$

(1)

where the family of weights w_{ij} depends on the similarity between the pixels i and j, and satisfy the usual conditions $0 \le w_{ij} \le 1$ and $\sum_j w_{ij} = 1$. w_{ij} computed depending on the similarity of their patches and is defined as

$$w_{ij} = \frac{1}{Z_i} \exp^{-\frac{1}{h^2} G_d * \left\| I\left(N^d(i)\right) - I\left(N^d(j)\right) \right\|_2^2}.$$

(2)

where Z is the normalizing term, $Z_i = \sum_j w_{ij}$, G_d is a Gaussian spatial kernel, * is the convolution operator and h acts as a filtering parameter. It controls the decay of the exponential function and therefore the decay of the weights as a function of the Euclidean distances. This parameter is typically adjusted manually in the algorithm.

There are many dissimilar pixels in the search window. These pixels must be excluded from the weighting (1). In [10], a variational method has been proposed. In this work, an automatic method has been devised to select the most relevant pixels tfrom the candidate pixels.

3   The Improved NL-Means Method

To deal with computational burden, our main idea is to select only the pixels x_j in P_i that will have the highest weights $w(x_i, x_j)$ without having to compute all the Euclidean distances between $I(N^d(i))$ and $I(N^d(j))$, and on the similarity of the average over the neighbourhoods $N^d(i)$ and $N^d(j)$ of the gradient orientation at pixel x_i and x_j. Intuitively, similar neighbourhoods have the same mean and the

same gradient orientation. But the computation of the gradient orientation is sensitive to noise. For this reason, the preselection of pixels is based on the mean and the variance of $I\left(N^d(i)\right)$ and $I\left(N^d(j)\right)$ which allows to decrease the computational burden. Let us estimate the original value at a pixel i, $u(i)$, as the mean of the noisy grey levels $v(j)$ for $j \in J \subset I$. One expects averaged pixels to have a non noisy grey level value, $u(j)$, similar to $u(i)$ in order to reduce the noise and restore the original value. Assuming this fact,

$$\hat{u}(i) = \frac{1}{|J|}\sum_{j \in J} v(j) \approx \frac{1}{|J|}\sum_{j \in J}\left(u(i) + n(j) - u(j)\right)^2 .$$ (3)

Because the average of noise values tends to zero.

If the averaged pixels have a non noisy grey level value close to $u(i)$, as expected, then the variance of the average should be close to σ^2. If it is a posterior observed that this variance is much larger than σ^2. This fact can hardly be caused by the noise only. This means that Non-Local is averaging pixels whose original grey level values were very different in the original. At those pixels, a more conservative estimate is required, and therefore the estimated value should be averaged with the noisy one.

The smoothing parameter h depends on the standard deviation of the noise σ, and typically a good for 2D images is $h = 11\sigma$. Equation 2 shows that h also needs to take into account $I\left(N^d(i)\right)$, if we want a filter independent of of the neighbourhood size. Let X and Y be two real random variables. Then, the linear estimate $\hat{Y}$,

$$\hat{Y} = \arg\min_{Y} \frac{1}{\sigma^2}\|X - Y\|_2^2 + \sum \|Y - EY\|_2^2 .$$ (4)

Repeating this procedure we arrive to the recursive algorithm

$$\hat{Y}^{(k)} = \arg\min_{Y} \frac{1}{\sigma^2}\left\|X - Y^{(k-1)}\right\|_2^2 + \sum_r \left\|Y_r - E\hat{Y}^{(k-1)}\right\|_2^2 .$$ (5)

In our case, $X = Y + N$ where N is independent of Y, with zero mean and variance σ^2. This equation defines the aggregation in this algorithm.

This strategy can be applied to correct any local smoothing filter. The NL-means algorithm converges to the conditional mean. The conditional variance van be also computed by the NL-means, by taking $\phi(x) = x^2$ and then computing the variance as $EX^2 - (EX)^2$. In the case of images, this stationary condition amounts to say that as the size of the image grows, we are able to find in the image many similar patches for all the details of the image. This is a crucial point to understand the performance of the NL-means algorithm.

4   Experimental Results

The NL-means algorithm chooses for each pixel a different average configuration adapted to the image. The most favorable case for the NL-means is the periodic case. In this situation, for every pixel i of the image one can find a large set of samples with a very similar configuration, leading to a noise reduction and a preservation of the original image, see Figure.1 for an example.
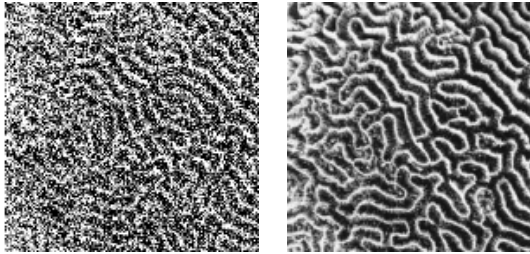
Fig. 1. NL-means denoising experiment with a nearly periodic image. Left: Noisy image with standard deviation 30. Right: NL-means restored image.
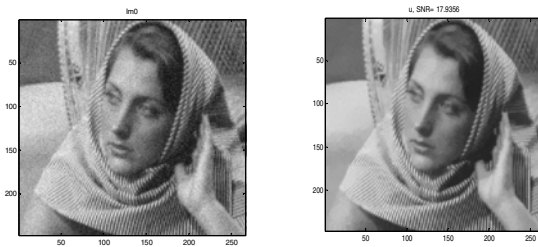
Fig. 2. NL-means denoising experiment with a Brodatz texture image. Left: Noisy image with standard deviation 20. Right: NL-means restored image.

Fig. 3. NL-means denoising experiment with a natural image. Left: Noisy image with standard diviation 20. Right: Restored image.

Another case which is ideally suitable for the application of the NL-means algorithm is the textural case. Texture images have a large redundancy. In Figure.2 one can see an example with a Brodatz texture.

The NL-means is not only able to restore periodic or texture images. Natural images also have enough redundancy to be restored by NL-means. The same algorithm applies to the restoration of color images and films, see Figure 4.

Fig. 4. NL-means denoising experiment with a color image. Left: Noisy image with standard deviation 15 in every color component. Right: Restored image.

Fig. 5. Optimal correction experience. Left: Noisy image. Middle: NL-means solution. Right: NL-means corrected solution. The average with the noisy image makes the solution to be noisier, but details and fine structure are better preserved.

4.1   Visual Quality Comparison

The visual quality of the restored image is an important criterion to judge the performance of a denoising algorithm. Let us present some experiences on a set of standard natural images. The objective is to compare the visual quality of the restored images, the non presence of artifacts and the correct reconstruction of edges, texture and fine structure. Figure 6 present this experiences comparing the visual quality of previous methods.

Figure 6 illustrates the fact that a non local algorithm is needed for the correct reconstruction of periodic images. Local smoothing filters and local frequency filters are not able to reconstruct the wall pattern. Only the NL-means algorithm and the

global Fourier Wiener filter reconstruct the original texture. The Fourier Wiener filter is based on a global Fourier transform which is able to capture the periodic structure of the image in a few coefficients. Now, in practice, this is an ideal filter because the Fourier Transform of the original image is used.
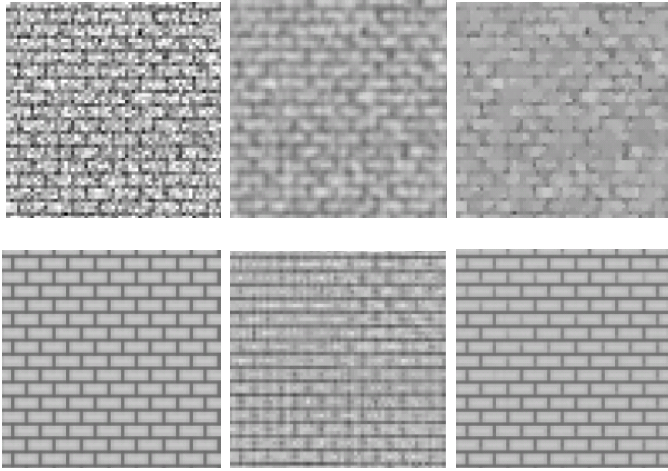
Fig. 6. Denoising experience on a periodic image. From left to right and from top to bottom: noisy image (standard deviation 35), Gauss filtering, Total variation, Wiener filter (ideal filter), DCT empirical Wiener filtering, NL-means algorithm.

5   Conclusion

After the analysis of the test results the non-local means algorithm proved to be a better algorithm for image denosing, than its predecessors. The non-local means method performed exceptionally well. As expected, the non-local means did a better job of preserving edges than the other methods. It performed best on periodic textures like the stripped pants from the Barb test case. In all test cases for the non-local means method, the method noise contained little structure from the image. The non-local means algorithm accomplished its goals of removing noise and preserving detail. So the NL-means method is a highly successful way of approaching image denoising.

References

1. Dabov, K., Foi, A., Katkovnik, V., Egiazarian, K., Member, S.: Image denoising by sparse 3d transform-domain collaborative filtering. IEEE Trans. Image Process 16, 2007–2016 (2007)
2. Portilla, J., Strela, V., Wainwright, M., Simoncelli, E.: Image denoising using scale mixtures of gaussians in the wavelet domain. IEEE TIP 12(11), 1338–1351 (2003)
3. Yuan, L., Sun, J., Quan, L., Shum, H.Y.: Progressive interscale and intra-scale non-blind image deconvolution. ACM Transactions on Graphics 27(3), 1–10 (2008)
4. Roth, S., Black, M.J.: Fields of experts: A framework for learning image priors. In: CVPR 2005, pp. 860–867 (2005)
5. Gilboa, G., Osher, S.: Nonlocal Linear Image Regularization and Supervised Segmentation. SIAM Multiscale Modeling and Simulation (MMS) 6(2), 595–630 (2007)
6. Tasdizen, T.: Principal components for non-local means image denoising. In: IEEE Proc. Int. Conf. Image Proc., pp. 1728–1731 (2008)
7. Mahmoudi, M., Sapiro, G.: Fats image and video denoising via nonlocal means of similar neighborhoods. IEEE Sig. Proc. Let. 12(12), 839–842 (2005)
8. Orchard, J., Ebrahimi, M., Wong, A.: Efficient nonlocal-means denoising using the svd. In: Proc. of IEEE Int. Conf. on Image, pp. 1732–1735 (2008)
9. Karnati, V., Uliyar, M., Dey, S.: Fast non-local algorithm for image denoising. In: Proc. of IEEE ICIP, Cairo, Egypt (2009)
10. Dor´e, V., Cheriet, M.: Robust NL-means filter with optimal pixel-wise smoothing parameter for statistical image denoising. IEEE Trans. on Signal Processing 57(5), 1703–1716 (2009)

A Controllable Quantum Sequential Multi-signature Scheme

Ma Ying[1,2], Tian Wei-Jian[1], and Fan Yang-Yu[1]

[1] School of Electronic and Information,
Northwestern Polytechnical University 710072, China
[2] School of Electronic Information Engineering,
Xi'an Technological University 710032, China

Abstract. A controllable quantum sequential multi-signature scheme is proposed, in order to realize digital signature validly and reliably in multi-user quantum environment. The signature of cryptograph and users validation are achieved by using the property of quantum entanglement swapping in Bell states; The choice of target users and the transmission of signature-information between users are implemented by controllable quantum teleportation; The quantum key and one-time pad ensures the safety of our scheme. The verification for each terminal and the center is required in our scheme, so it can position where the error happens accurately, is with strong practicability.

Keywords: Quantum signature, Controllable, Sequential, Entanglement swapping.

Digital signature scheme has been wildly researched and applied in information security field because of those features, such as reliable distinguishment, unforgement, non-repudiation. However, the safety of digital signature scheme, which belongs to the classic cryptography, is still based on calculation abliity. But the emergence of quantum computers and related algorithms, directly make classical digital signature schemes lose efficacy. Because of the unconditional security of quantum effects, quantum digital signature scheme gradually become the research hotspot.

In 2001, Gottesman and Chuang first proposed a quantum signature scheme based on quantum one-way function[1]; in the same year, ZengGuiHua and etc put forward a arbitration quantum signature scheme based on trusted third party, by using GHZ 3 particle states[2]; by 2004,Lee and etc brought forward a arbitration quantum signature scheme with message recovery[3]; Lu and etc proposed two quantum signature scheme[4, 5], one is arbitration quantum message signature scheme based on GHZ states, another is quantum digital signature scheme based on quantum one-way function. By 2006, WangJian and etc proposed a quantum signature scheme using quantum key distribution and one-time pad[6], avoid using quantum entanglement states; And WenXiaoJun proposed two non-arbitration information signature schemes using the characters of EPR entanglement Particles and quantum teleportation, solving the problems which Previous scheme depend on the arbitration[7, 8]. In 2008, YangYuGuang and etc put forward quantum threshold group signature scheme and Proxy signature scheme, namely t users in n users can generate or verify a group

signature[9, 10]. In 2010, ChenYongZhi, put forward a proxy signature scheme based on controlled quantum teleportation [11].

Considering the Actual situation in instructions issue and message transmission, this paper aim at the frequently situation, which the message sender needs sequential choose users to transfer and get the ciphertext, then verify users signature successively, Propose a controllable quantum sequential multi-signature scheme.

1   Basic Principles

In this paper, the Entanglement Swapping in Bell states is used to achieve and verify message signature. Entanglement swapping refers to the process that two independent entangled pairs exchange their entangled photons in some ways and become to two new entangled pairs.

For example, there are four entangled photons, photons $1^\#$ and $2^\#$ are in entangled state $\left|\psi^-\right\rangle_{12}$, photons $3^\#$ and $4^\#$ are in entangled state $\left|\phi^-\right\rangle_{34}$. So, the four particles are in the state $\left|\psi\right\rangle_{1234}$:

$$\left|\psi\right\rangle_{1234}=\left|\psi^-\right\rangle_{12}\otimes\left|\phi^-\right\rangle_{34}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_1\left|1\right\rangle_2-\left|1\right\rangle_1\left|0\right\rangle_2)\otimes\frac{1}{\sqrt{2}}(\left|0\right\rangle_3\left|0\right\rangle_4-\left|1\right\rangle_3\left|1\right\rangle_4)\qquad(1\text{-}1)$$

If we measure particles $1^\#$ and $3^\#$ in Bell basis, it will result in corresponding spectral decomposition and states collapse right now. The formula (1-1) now can be rewritten with four Bell basis decomposition as:

$$\left|\psi\right\rangle_{1234}=\frac{1}{2}(\left|\phi^+\right\rangle_{13}\left|\psi^+\right\rangle_{24}-\left|\phi^-\right\rangle_{13}\left|\psi^-\right\rangle_{24}-\left|\psi^+\right\rangle_{13}\left|\phi^+\right\rangle_{24}+\left|\psi^-\right\rangle_{13}\left|\phi^-\right\rangle_{24})\qquad(1\text{-}2)$$

The measurement will be collapsed into one of the four entangled states in equiprobability. For example, if our measurement is $\left|\phi^+\right\rangle_{13}$, then the particles $2^\#$ and $4^\#$ must in bell state $\left|\psi^+\right\rangle_{24}$.

From the above, we can see that if we measure particles $1^\#$ and $3^\#$ in Bell basis, it will certainly cause particles $1^\#$ and $3^\#$ be entangled, which are never in an entanglement state before, and collapsed into the corresponding quantum states, similar to particles $2^\#$ and $4^\#$.The process we call it Entanglement Swapping.

The character of quantum entanglement swapping is very important in quantum information technology field, It can be used in quantum digital signature, data transmission and etc. The specific evolution rule can be found in references[8].

2   Controllable Quantum Sequential Multi-signature Scheme

The participants include the ciphertext sender and the last verifier Alice, all may received messages users ($U_1\cdots U_n$), all received message and sign their name users U_i.

Normally, Alice may only require some rather than all users to read the ciphertext and sign. So, it's necessary for Alice to choose or approve users who have permissions to know about the ciphertext, in advance. Here, only offer U_1, U_2 and U_i as chosen users to expound our scheme.

According to implementation process, our scheme can be roughly divided into preparation stage, signature stage and verification stage.

2.1   Preparation Stage

(1) Alice and each user($U_1 \cdots U_n$) distribute quantum keys K_1-K_n, the method of quantum key distribution could use protocol BB84,which is unconditional safe and simple.

(2)Alice and each user($U_1 \cdots U_n$) rule segmenting the classic information every 2bit as an unit, every unit corresponding to a Bell state, the corresponding relationship is as follows:

$$00 \rightarrow \left| \phi^+ \right\rangle, \ 01 \rightarrow \left| \phi^- \right\rangle, \ 10 \rightarrow \left| \psi^+ \right\rangle, \ 11 \rightarrow \left| \psi^- \right\rangle \qquad (2\text{-}1)$$

(3) Each user U_i generates two entangled pairs sequence B_{Ti} and B_{Ti}', then send one photon of each entanglement pair sequence to Alice, both of them keep those photons properly, and used them as a bridge when Alice choose target user.

2.2   Signature Stage

(1) Alice encrypts plain text M,M={m(1),m(2),...,m(t)},with quantum key K_1,then send the ciphertext to the first user,U1, by classic channel.

(2) User U_1 decrypts the ciphertext and gets M, then updates the communication key(K_1) with Alice immediately. According to the rules, U_1 segments M every 2bit, then generates corresponding Bell states. For example, M={010010}, U_1 will generate Bell state sequence BM={$\left| \phi^- \right\rangle$, $\left| \phi^+ \right\rangle$, $\left| \psi^+ \right\rangle$} according to M.

(3) U_1 generates corresponding Bell states sequence according to previously K_1, note for B_{K1}={$b_{k1}(1)$, $b_{k1}(2)$,$\cdots$, $b_{k1}(t)$}. For example, if K1=111000, the B_{K1} will be B_{K1}={$\left| \psi^- \right\rangle$,$\left| \psi^+ \right\rangle$,$\left| \phi^+ \right\rangle$}.

(4) U_1 begins entanglement swapping for those every 2qbit 4 photons belonging to B_M and B_{K1}, and measures entanglement photons in Bell basis after swapping. One group of the measurement result is recorded as $b_{s1}(i)$; Another is $b_{s1}(i)$'. In that way, U_1 gets measurement sequence B_{S1} and B_{S1}' after entanglement swapping.

(5) U_1 converts B_{S1}' into classical bit sequences according to congruent relationship of formula (2-1),notes for S_1', then uses updated quantum key to encrypt S_1',and send it back to Alice; Alice obtains S_1' and stores it for verifying user signature; Alice simultaneously records all previous key information formed with U_1; U_1 use S_1' as a key encryption B_M, $B_{K1}$and B_{S1} sequence, so U_1 gets his signature sequence S_{U1}=$E_{S1'}${B_M,B_{K1},B_{S1}}.

(6) Alice selects next signature users in term of needs. For example, Alice select U_2 as next signature user, Alice firstly entangle local stored photons of B_{T1} and B_{T2}. By that

way, Alice constructs entanglement pairs sequence between U_1 and U_2.Then through quantum teleportation, U1 can transmit signature information SU1 directly to U2.

(7) After U2 gets signature information SU1=ES1'{BM,BK1,BS1} from U1, Alcie uses K2 to encrypt S1',and sends it to U2 by classic channel. Then, U2 know about the information in SU1 by decrypting S_1'. Referencing step (2-5), U_2 generates together corresponding Bell states sequence from K_2 and B_{S1}, according to congruent relationship of formula (2-1), and begins a new entanglement swapping, the results note for B_{S2} and B_{S2}'. Here, U_2 obtain plain text M, and give his signature $S_{U2}=E_{S2'}\{B_M,B_{K1},B_{S1},B_{K2},B_{S2}\}$. Meanwhile, U_2 encrypts S_2' and send it back to Alice.

(8) Similarly, Alice chooses last signature user U_i. Alice firstly entangle local stored photons of B_{T2}' and B_{Ti}, constructing entanglement pairs sequence between U_2 and U_i. Then through quantum teleportation, U_2 transmits signature information S_{U2} to U_i. U_i using Ki decrypts ciphertext form Alice by classic channel and gets S_2'. U_i farther kown about all information in S_{U2} including B_{S2}, then swapping entanglement with B_{S2} and B_{Ki}, the result note for B_{Si} and B_{Si}'. Thus, U_i has his own signature $S_{Ui}=E_{Si'}\{B_M,B_{K1},B_{S1},B_{K2},B_{S2}, B_{Ki}, B_{Si}\}$.

(9) U_i converts S_{Ui} and B_{Si}' into classic bits and encrypts them by K_i, then send it back to Alice.

2.3   Verification Stage

This scheme requires all U_i (i=2, ···, n) verifying signature of preceding user U_{i-1}; At last, Alice will verify the validity of all signature user.

(1) U_2 verify signature of U_1

Alice encrypts S_1' using K_2 and sends it to U_2, U_2 obtains information of $\{B_M,B_{K1},B_{S1}\}$ in S_{U1} and B_{S1}' using S_1'. U_2 should verify if Bell state of every photons in B_{S1} and B_{S1}' march direct product evolution rules of B_M and B_{K1} sequence, namely whether the following is accordant:

$$b_m(i) \otimes b_{k1}(i) \rightarrow b_{s1}(i) \cdot b_{s1}(i)' \qquad (i=1,2,\cdots,t) \qquad (2\text{-}2)$$

If the above is accordant, U_2 think the signature of U_1 for M is effective; Otherwise is ineffective, U_2 refuses to continue to sign for plain text, and terminates the entire digital signature process.

(2) U_i verify signature of U_2

Similarly, U_i obtains the information of $\{B_M,K_1,B_{S1},K_2,B_{S2}\}$ by decrypting S_{U2} using S_2' from Alice. U_i should verify if Bell state of every photons in B_{S2} and B_{S2}' march direct product evolution rules of B_{S1} and B_{K2} sequence, namely whether the following is accordant:

$$b_{s1}(i) \otimes b_{k2}(i) \rightarrow b_{s2}(i) \cdot b_{s2}(i)' \qquad (i=1,2,\cdots,t) \qquad (2\text{-}3)$$

If the above is accordant, U_i think the signature of U_2 for M is effective; Otherwise is ineffective, U_i refuses to continue to sign for plain text, and terminates the entire digital signature process.

(3)   Alice verify the effectiveness of signature to all chosen users

Alice obtains S_{Ui} and B_{Si}' by decrypting ciphertext from U_i. Alice firstly contrast the accordant of M stored in local, K_1, K_2 and K_i in entanglement swapping. If the result is

correct, combing information of B_{S1}' and B_{S2}' stored in local, Alice verify ordinally every user if accords with rules of Bell states quantum entanglement swapping. If all verification results of entanglement swapping for chosen users accord with the rules, Alice finally accepts the validity of the whole quantum signature process; otherwise, no matter any user errors, Alice refuses to accept the whole signature.

3   Analysis of Security and Validity

(1)   Deceptive attack

If any signature user U_i maliciously tamper with signature to deceive the subsequent signer and verifier, maybe he can make U_{i+1} get wrong message, but will ultimately fail to pass Alice's verification. Because Alice will first check M, all corresponding K_i, then verify the validity of signature ordinally. In that way, Alice will locate users, which maliciously tamper with information, and examine the integrity of all signature users.

(2)   The validity of signature

For any signer U_i, in the process of forming his own signature information, not only need to use quantum key, K_i, consulted with Alice, to transfer $S_{(i-1)}$' as important signature information and decryption password, but also K_i takes part in the process of signature as an element to form signature, further more, K_i itself is a important symbol of user identity.

Secondly, B_{Si}', as one of the signature information, is measured immediately and sent to Alice safely after entanglement swapping, only when the next user U_{i+1} verifies the validity of signature for U_i, Alice will send it to U_{i+1} by safe channel. Therefore, singnature user U_i must have two terms: one is the quantum key, K_i, formed with Alice in advance; another is B_{Si} and B_{Si}', which is of uniqueness, measured after current entanglement swapping. So it has property that can't be denied.

(3)   The confidentiality of signature

In this scheme, the user U_i only selected by Alice can might kown about the message M, and signs his own signature S_{ui}. And Ui sends S_{ui} by quantum teleportation controlled by Alice to next user assigned by Alice too, the user U_i itself doesn't know who is the next user; Further more,U_{i+1} can obtain the information only after being authorized(decryption password of signature) by Alice. This ensures that the whole signature process has high confidentiality.

(4)   Intermediary attack

The eavesdropper attempts to intercept message M, quantum key K_i, or user's signature information S_i', in order to master and tamper with the message and signature of users'. Due to the above information encrypts by quantum key during transmission, use the quantum key distribution protocols have been proved as unconditional security, such as BB84.And Alice updates keys with U_i in every communication process, namely ensures one-time-pad in communication. Therefore, the eavesdropper would be unable to get any useful information, and to say nothing of mastering and tampering with any message and signature of users.

The eavesdropper can intercept entanglement pairs sequence for choosing signature user, sent by U_i to Alice, and generate the same entanglement pairs sent to Alice. If what U_i transfers is plain text by quantum teleportation, the Eavesdropper can completely unnoticed acquire all the information including message M of U_i. Although

the signature has still the property that can not be denied, it makes scheme meaningless in some degree. After encrying signature information by S_i', the eavesdropper can't get any useful information totally. Moreover, because S_i' is formed in randomness, for the every bit in S_i', the eavesdropper has only $\dfrac{1}{32}$ probability to "guess" the right bit, so the behavior of the eavesdropper will easily be detected, the attack will not be successful.

4   Conclusion

This paper proposes a quantum sequential multi-signature Scheme strictly controlled by message sender, by using the property of entanglement swapping in Bell states, and with the help of quantum teleportation. The scheme possesses a high degree of confidentiality, security, and can't be counterfeited and repudiated. it's particularly suitable for small scale network, with strong practicability.

References

1. Gottesman, D., Chuang, I.: Quantum Digital Signatures(DB/OL) 2001-05-08, `http://arxiv.org/abs/quant-ph/0105032`
2. Zeng, G., Ma, W., Wang, X., et al.: Signature Scheme Based on Quantum Cryptography. Acta Electronica Sinaca 29(8), 1098–1100 (2001) (in Chinese)
3. Lee, H., Hong, C., Kim, H., et al.: Arbitrated Quantum Signature Scheme with Message Recovery. Physics Letters A 321, 295–300 (2004)
4. Lü, X., Feng, D.-G.: An arbitrated quantum message signature scheme. In: Zhang, J., He, J.-H., Fu, Y. (eds.) CIS 2004. LNCS, vol. 3314, pp. 1054–1060. Springer, Heidelberg (2004)
5. Lu, X., Feng, D.G.: Quantum Digital Simnature Based on Quantum One-Way Functions(EB/OL) (2004), `http://arxiv.org/abs/quant-ph/0403046`
6. Wang, J., Zhang, Q., Tang, C.-J.: Quantum signature scheme with single photons. Optoelectronics Letters 2(3), 209–212 (2006)
7. Wen, X., Liu, Y., Zhang, P.: Information Signature Protocols Using Einstein-Podolsky-Rosen Pairs. Journal of Dalian University of Technology 47(3), 424–428 (2007) (in Chinese)
8. Wen, X., Liu, Y.: A Realizable Quantum Sequential Multi-Signature Scheme. Acta Electronica Sinaca 35(6), 1079–1083 (2007) (in Chinese)
9. Yang, Y., Wen, Q.: Proxy quantum signature scheme with shared threshold verification. Science in China 38(7), 834–843 (2008) (in Chinese)
10. Yang, Y., Wen, Q.: Quantum group signature with threshold. Science in China 38(9), 1162–1170 (2008) (in Chinese)
11. Chen, Y., Liu, Y., Wen, X.: A Proxy Signature Scheme Based on Controlled Quantum Teleportation. Journal of Beijing Jiaotong University 34(5), 127–134 (2010) (in Chinese)

Improving Detection Rate in Intrusion Detection Systems Using FCM Clustering to Select Meaningful Landmarks in Incremental Landmark Isomap Algorithm

Seyed Mehdi Iranmanesh[1,*], Mehdi Mohammadi[1],
Ahmad Akbari[1], and Babak Nassersharif[2]

[1] Iran University of science and technology, Computer Engineering Department,
University Road, Hengam Street, Resalat Square, Tehran,
Tel.: 0098-915-341-5869, Iran
`m_iranmanesh@comp.iust.ac.ir`
[2] School of Computer Engineering, Faculty of Engineering, University of Guilan, Rasht, Iran
`{mh_mohammadi,akbari,nasser_s}@iust.ac.ir`

Abstract. Dimension reduction is crucial when it is applied on intrusion detection systems. Many data mining algorithms have been used for this purpose. For example, manifold learning algorithms, especially Isometric feature mapping (Isomap) have been investigated. Researchers successfully applied Isomap on intrusion detection system as a nonlinear dimension reduction method. But it had some problems such as operation on batch mode and being disabled to handle new data points, additionally, it had computational cost and could not be properly applied on huge datasets. Losing time and reducing speed of detection is another problem of Isomap in intrusion detection systems. Incremental Landmark Isomap which selects landmarks among whole data points has been invented for solving these problems. In this paper, we use FCM as a data reduction method to select meaningful landmarks for Incremental L-Isomap instead of choosing them randomly. This method is implemented and applied on some UCI datasets and also NSLKDD dataset. The results demonstrate higher detection rate for the proposed method, comparing to classical Incremental L-Isomap which chooses landmarks randomly.

Keywords: Intrusion Detection System, Manifold Learning, Landmark, Incremental Landmark Isomap, FCM Clustering, Dimension Reduction.

1 Introduction

With rapidly development of communication, there is no restriction of real distance for people to contact with each other. Besides the improvement and efficiency of the network, it is distinguished that unauthorized activities by external attacker or internal sources are increased dramatically. Accordingly, computer network's becomes an urgent issue. So the intrusion detection system which was introduced by Anderson [1] is an important problem nowadays. Anomaly detection and misuse detection are two

---

* Corresponding author.

prominent approaches in computer intrusion detection. In misuse detection, intrusions are detected by comparing activities with known signatures of intrusions. Those matched are then detected as attacks. This approach fails in detecting novel intrusions. Anomaly detection identifies activities that deviate from the normal. Although this method can handle novel attacks, it suffers from the difficulty of defining "Normal". We investigate anomaly detection in this study.

Many techniques based on data mining and machine learning approaches, such as neural networks, support vector machines [2] have been applied in anomaly intrusion detection. These algorithms work on all of data points' features. But in many datasets such as intrusion detection many features are redundant or less important [3].So reducing feature space by extracting features would be a good method for improving detection rate and reducing the time of processing.

PCA [4] and MDS [5] are two prominent methods for linear dimension reduction. These methods fail to act properly on real-world datasets, because these datasets are non-linear.

Manifold learning is one of the methods that used for dimension reduction. Non-linear manifold learning algorithms such as Locally Linear Embedding (LLE) [6] and Isometric Feature Mapping (Isomap) [7] have been used for nonlinear dimension reduction. In linear methods, usually linear kernels and Euclidean distances have been used. These restrictions can be eliminated in non-linear methods. Non-linear manifold learning methods are divided in two main categories. First category includes methods that try to maintain globally structure of dataset while second category maintains locally structures. For instance, Isomap is based on maintaining globally geometry of dataset. This method attempts to preserve Geodesic distances between data points while mapping them from high dimensions to low dimensions. LLE is one of the non-linear dimension reduction algorithms that global geometry is inferred only from local interactions between data points.

Landmark Isomap [8] is a variation of Isomap, which preserve all of attractive attributes, but is more efficient. It selects some data points as landmarks to construct the map. Landmark points are chosen, randomly. While L-Isomap embeds data points that have smooth manifolds with a little loss of information, it does not perform well on data points with more complex manifolds. If the landmark points are selected in a meaningful way rather than randomly, L-Isomap will perform better on these kinds of manifolds.

An important fact that exists in data mining domain is that sometimes the information should be collected sequentially through dataflow. Manifold learning algorithms operate in "batch" mode. It means that all data should be available during training and they cannot be applied on dataflow. Incremental manifold learning has been invented for this purpose. Martin law et all in [9] proposed incremental Isomap and incremental L-Isomap that can solve this problem. Their method can handle unseen data, and it can be applied on data stream too.

In this paper, we use the incremental version of L-Isomap. This method could handle the problem of data streams, and, because of landmark part of this algorithm, it also can solve bottlenecks of classical Isomap.

Experiments indicated that if landmarks are chosen in a way that they can show distribution of whole data points, L-Isomap will be able of reaching the same level of feature reduction as classical Isomap without losing important information. In order to

choose landmarks, we used clustering method. Clustering can be considered as the most important unsupervised learning problem. So, as every other problem of this kind, it deals with finding a structure in a set of unlabeled data point. Moreover, it can be used as a method for data reduction. Output of clustering method contains data points that will be used as landmarks for L-Isomap. In this work, Fuzzy-C means (FCM) algorithm [10] is used for clustering.

The rest of the paper is organized as follows. Section 2 provides a brief overview on FCM clustering, Isomap, L-Isomap and Incremental Isomap and finally it describes proposed method. The experimental results are described in section 3. The conclusions are presented in section 4.

2   Methodology

2.1   Isomap

Isomap [7] is a generalization of MDS (Multi-Dimensional Scaling) [5] in which the pairwise distance matrix is replaced by the matrix of pairwise geodesic distances. The algorithm contains three steps:

1. Construct graph that shows manifold of data points in high dimensional space.
2. Compute pairwise distance matrix D with the Floyd or Dijkstra algorithm.
3. Apply MDS on D.

2.2   Landmark Isomap

Landmark Isomap [8] is a variation of Isomap, which preserve all of the attractive attributes, but is more efficient. Landmark Isomap saves three bottlenecks that exist in classical Isomap algorithm: storage, calculation of distance matrix, and the eigenvalue problem.

2.3   Incremental Isomap

Suppose that data points X_i for $1 \leq i \leq n$ exist. Batch Isomap algorithm can calculate Y_i for $1 \leq i \leq n$, so that Y_i is embedded form of original data points in low dimensional space. Then, the new data point X_{n+1} arrives. The goal of incremental Isomap [9] is to update the transformed data points Y_i so that to best preserve the updated geodesic distances. This is done in three stages:

1- Updating the Geodesic Distance for the original n vertices.
2- Updating the embedded data points regarding to the new Geodesic Distance matrix.
3- Calculating the transformed instances of new data point X_{n+1}.

2.4   Fuzzy C-Means (FCM)

The fuzzy c-means algorithm is one of the clustering methods that belongs to overlapping clustering category. Like fuzzy logic, in fuzzy clustering, each data point

belongs to clusters with a degree. The degree of membership for each cluster would be different. For each data point, sum of the membership degree of belonging to clusters would be one:

$$\forall x\left(\sum_{k=1}^{num.cluster} u_k(x) = 1\right)$$ (1)

The centroid of the cluster would be mean of all data points, that belong to that cluster. As the formula shows, the coefficient of each data point is related to its degree of belonging to the cluster:

$$center_k = \frac{\sum_x u_k(x)^m x}{\sum_x u_k(x)^m}$$ (2)

For each data point, the degree of belonging to each cluster is related to the inverse of distance to the cluster center:

$$u_k(x) = \frac{1}{d(center_k, x)}$$ (3)

Then the gained coefficient are normalized and fuzzyfied with a real parameter m > 1 so that their sum is 1:

$$u_k(x) = \frac{1}{\sum_j \left(\frac{d(center_k, x)}{d(center_j, x)}\right)^{2/m-1}}$$ (4)

FCM method includes these three steps:

1. Choose a number of clusters.
2. Assign a coefficient to each data point that indicates the degree of belonging to each cluster, randomly.
3. Repeat until the algorithm is converged(the coefficient's change is smaller than threshold criteria)

   3.1. For each cluster compute its center, using above formula
   3.2. For each data point determine the degree of being in each cluster using above formula.

2.5 Our Approach

We applied FCM in a way that is more useful for the problem of incremental landmark Isomap. Using FCM method, there are two ways to choose the landmarks. The first solution sets number of clusters equal to number of landmarks, and chooses one data point in each cluster as an indicator of that cluster. These indicators would be landmark points. This method has some problems. The first problem is that if the number of landmark points is high, this method should assign high number of clusters to data points. When the number of clusters becomes high, FCM has computational complexity. The second problem is that choosing one data point from each cluster is not a good way to gather landmarks. Because different clusters contains different number of data points. Some clusters are bigger than the others, and as a result they have more priority in a dataset. But, in this method one data point has been chosen from each cluster, and this indicates that it assigns the same priority to all clusters.

The second solution, which is the approach used in our proposed method, does not allocate equal priority to each cluster. At the beginning, this method assigns weight to each cluster. Assigning weights to clusters is based on the number of data points that each cluster contains.

$$W_k = \frac{\sum_{i=1}^{num.data\ points} u_{ik}}{\sum_{k=1}^{num.cluster} \sum_{i=1}^{num.data\ points} u_{ik}} \qquad (5)$$

After assigning weights, the number of landmarks that should be chosen from each cluster calculated according to this formula:

$$L_k = \lfloor W_k \rfloor * L_T \qquad (6)$$

Which L_k is the number of landmarks that have been selected from cluster k, and L_T is the whole number of landmarks that would be representative of all data points.

For selecting data points from each cluster, the data points having bigger membership degrees are chosen.

It is worth mentioning here that, the main contribution of this paper would be the second solution which firstly assigns weights to the clusters. It then selects the appropriate landmarks based on the assigned weights from each cluster. After this step, these landmarks are used in L-Isomap algorithm to reduce the features of data points. We used this algorithm in intrusion detection systems to could obtain better detection rates. In next section, some of the experimental results are described.

3   Results

In this section, we present the experimental results in evaluating the proposed method. The proposed methods are evaluated on the following datasets selected from UCI repository in addition to NSL-KDD dataset. [11]. NSL-KDD is a dataset suggested to solve   the inherent problems of the KDD'99 dataset mentioned in [11]. However, this new version of the KDD dataset still suffers from the problems discussed by McHugh [12] and may not be a perfect representative of existing real networks. Because of the lack of public datasets for network-based IDS, we believe that it still can be considered as a suitable benchmark allowing researchers to compare different intrusion detection methods. Table 1 shows the properties of these datasets. As Table 1 shows the CMC and Waves train datasets are not separated from the test part. In these experiments, 70% of whole dataset is considered as train set and the remain dataset would be test set.

Table 1. Summery of used datasets

	No. Samples	No. Class	No. Features
CMC	1472	3	10
Waves	5000	3	41
Train NSL-KDD	25192	2	41
Test + NSL-KDD	22544	2	41
Test – NSL-KDD	11850	2	41

In these experiments, firstly data reduction with FCM is performed, and finally incremental L-Isomap via selecting landmark points based on FCM method is investigated.

1. Data reduction with FCM:

The proposed FCM is used for selecting meaningful landmarks. We applied this method on datasets shown in Table 1 to reduce data points. The reduced data points could be considered as landmark points for incremental L-Isomap algorithm. But, in this step we want to show that the reduced data points are appropriate representatives for whole dataset. As Tables 2-5 show, the proposed algorithm was able to reduce the number of data points in each dataset. After reduction of data points, datasets are classified with decision tree. The proposed FCM has two parameters: number of clusters and number of reduced data points. After setting these two parameters, we executed this method 30 times. Consequently, for each time executing this method, the reduced dataset, is classified by decision tree. Accuracy of classifying reduced datasets is shown in Tables 2-5. Table 6 shows the accuracy of classifying original datasets before reduction. It can be seen that the accuracy of selecting data points using proposed FCM is near to the accuracy of original data points before reduction. This fact shows us that selecting landmarks via proposed FCM preserves the distribution of original dataset.

Table 2. CMC

Train size	Number of clusters			
	10	50	75	100
100	38.59	40.56	38.60	39.69
300	42.51	40.20	41.10	40.85
500	43.92	42.16	42.37	43.38
800	43.14	43.33	44.01	43.75

Table 3. Waves

Train size	Number of clusters			
	10	50	75	100
500	62.54	63.46	63.17	62.57
1100	64.91	65.59	64.92	65.48
2000	68.60	69.68	69.21	69.29
3000	72.60	73.07	73.01	73.33

Table 4. NSL-KDD (+)

Train size	Number of clusters			
	10	50	75	100
5000	58.97	59.08	59.03	59.03
10000	65.03	74.64	70.08	71.22
15000	64.51	71.22	70.51	73.06
20000	75.22	73.79	72.93	75.51

Table 5. NSL-KDD(-)

Train size	Number of clusters			
	10	50	75	100
5000	51.40	51.36	51.38	51.38
10000	51.38	55.43	56.36	54.80
15000	53.99	55.80	55.99	56.06
20000	57.80	56.17	57.62	57.99

Table 6. Accuracy of classifying original datasets before reduction

Dataset	Train-size	Accuracy
CMC	1000	44.4909
Waves	3500	73.3983
NSL-KDD(+)	25192	78.0119
NSL-KDD(-)	25192	58.1941

2.   Incremental L-Isomap via selecting landmark points based on FCM method:

We applied incremental manifold learning on datasets shown in Table 1 to transform data points from high dimensional space to low dimensional space. Number of features is reduced to half for each data point. Number of features of each dataset after performing manifold learning algorithm is shown in Table 7. The number of neighbors to construct manifold, for each dataset is presented, too. Number of landmarks and number of clusters for FCM landmark selection are two parameters that have to be set. In classical incremental L-Isomap, landmark points are chosen randomly. But, Landmark points have to be chosen in a way that they show characteristic of all data points. In the proposed method, landmark points are selected using FCM algorithm. These landmarks should be representative of all data points. After feature reduction with incremental L-Isomap, we classified data points with decision tree classifier. Table 8 shows that when we applied incremental L-Isomap with selecting landmarks via FCM, results are more accurate in comparison with selecting landmarks randomly. Besides, original datasets without applying manifold learning algorithms are classified. It can be seen that incremental L-Isomap improves accuracy of classifying. This shows that some features are irrelevant or noise and using incremental manifold learning can omit them.

Table 7. Parameters of proposed incremental L-Isomap and number of features befor and after reduction

Dataset	Number of neighbors	Number of landmarks	Number of cluster for FCM landmark selecting	Number of features after embedding
CMC	20	50	10	5
Waves	35	150	25	20
NSL-KDD(+)	40	500	50	20
NSL-KDD(-)	40	500	50	20

Table 8. Comparison between accuracy value in the proposed incremental L-Isomap and classical incremental L-Isomap and original dataset without feature reduction

Dataset	Classical incremental landmark Isomap	Proposed incremental landmark Isomap	Original dataset
CMC	37.4028	46.8512	44.4909
Waves	70.0469	71.3083	73.3983
NSL-KDD(+)	79.2119	82.2367	78.0119
NSL-KDD(-)	60.7713	63.2828	58.1941

4   Conclusion

This paper firstly discusses the concept of incremental landmark Isomap and its advantages to classical Isomap. The proposed FCM landmark selection is applied on incremental landmark Isomap method and is compared with classical incremental landmark Isomap. The results show that the landmark points chosen by FCM algorithms are better representatives of whole dataset. Therefore, they can construct similar manifold in less processing time. In addition, applying FCM to select landmarks makes incremental L-Isomap more robust. Consequently, this method could be more useful for large datasets.

We applied Incremental L-Isomap on UCI and NSLKDD datasets. To evaluate the applicably of our method, we used decision tree as the classifier for intrusion detection system. Experiment results demonstrate higher detection rate.

The use of Incremental L-Isomap improves the overall performance of IDS mainly due to two reasons. Firstly, it reduces the dimension, thereby making the computational efforts less. Second reason is the reduction of noise in the data. By reducing the noise, we can expect a better classification of normal and abnormal data.

References

1. Anderson, J.P.: Computer Security Threat Monitoring and Surveillance, James P. Anderson Co., Fort Washington, PA, Tech. Rep. 79F296400 (1-56) (April 1980)
2. Ambwani, T.: Multi Class Support Vector Machine Implementation to Intrusion Detection. In: Proc. of the Intl. Joint Conf. on Neural Networks, pp. 2300–2305. IEEE Press, New York (2003)
3. John, G.H., Kohavi, R., Pfleger, K.: Irrelevant Features and the Subset Selection Problem. In: Proc. of the 11th Int. Conf. on Machine Learning, pp. 121–129. IEEE Press, New York (1994)
4. Jolliffe, I.T.: Principal Component Analysis. Springer, New York (1986)
5. Cox, T.F., Cox, M.A.A.: Multidimensional Scaling. Chapman &Hall, London (1994)
6. Roweis, S.T., Saul, L.K.: Nonlinear Dimensionality Reduction by Locally Linear Embedding. Science 290, 2323–2326 (2000)
7. Tenenbaum, J.B., de Silva, V., Langford, J.C.: A Global Geometric Framework for Nonlinear Dimensionality Reduction. Science 290, 2319–2323 (2000)
8. De Silva, V., Tenenbaum, J.B.: Global Versus Local Methods in Nonlinear Dimensionality Reduction. In: Advances in Neural Information Processing Systems, vol. 15, pp. 705–712. MIT Press, Cambridge (2003)
9. Law, M., Zhang, N., Jain, A.: Nonlinear manifold learning for data stream. In: Berry, M., Dayal, U., Kamath, C., Skillicorn, D. (eds.) Proc. of the 4th SIAM International Conference on Data Mining, Lake Buena Vista, Florida, USA, pp. 33–44 (2004)
10. Bezdek, J.: Pattern Recognition with Fuzzy Objective Function Algorithms. Plenum Press, NY (1981)
11. Mahbod, T., Ebrahim, B., Wei, L., Ali, A.G.: A Detailed Analysis of the KDD CUP 99 Data Set. In: Proceeding of Computational Intelligence in Security and Defense Application, CISDA 2009 (2009)
12. McHugh, J.: Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory. ACM Transactions on Information and System Security 3, 262–294 (1998)

An Efficient and Provably Secure Certificate-Based Encryption Scheme

Yang Lu

College of Computer and Information Engineering,
Hohai University
Nanjing City, Jiangsu Province, China
`luyangnsd@163.com`

Abstract. Certificate-based encryption (CBE) is a new asymmetric encryption paradigm which combines traditional public-key encryption and identity-based encryption (IBE) while preserving some of their most attractive features. It provides an efficient implicit certificate mechanism which eliminates the third-party queries and simplifies the certificate revocation problem in the traditional PKI. It also solves the key escrow problem and the key distribution problem inherent in IBE. In this paper, we propose a quite efficient CBE scheme which is chosen-ciphertext secure in the random oracle model. The proposed CBE scheme requires computing only one bilinear pairing and introduces no redundancies in ciphertext. Compared with the existing CBE schemes, our scheme enjoys better performance on both the computation efficiency and the communication bandwidth.

Keywords: Certificate-based encryption, chosen-ciphertext secure, bilinear pairing, random oracle model.

1 Introduction

In Eurocrypt 2003, Gentry [12] introduced the notion of certificate-based encryption (CBE), which combines identity-based encryption (IBE) and traditional public key encryption (PKE) while preserving some of their most attractive features. As in the traditional PKE, each user in CBE generates his own public/private key pair and requests a certificate from a CA. The CA generates a certificate and is responsible for pushing a fresh certificate to the holder of the public key. A certificate in CBE has all the functionalities of a traditional PKI certificate, and also acts as a partial decryption key. This additional functionality provides an implicit certificate so that the sender is not required to obtain fresh information on certificate status and the recipient can only decrypt the ciphertext using his private key along with a fresh certificate from its CA. The feature of implicit certificate allows us to eliminate third-party queries for the certificate status and simplify the public key revocation problem. Therefore, CBE can be used to construct an efficient PKI requiring fewer infrastructures. Furthermore, there is no key escrow problem (since CA does not know the private keys of users) and key distribution problem (since the certificates need not be kept secret) in CBE.

In the original work [12], Gentry constructed the first CBE scheme in the random oracle model from the BF-IBE scheme [5]. A subsequent paper by Yum and Lee [24] provided a formal equivalence theorem among IBE, certificateless public key encryption (CL-PKE) [1] and CBE, and showed that IBE implies both CBE and CL-PKE by giving a generic construction from IBE to those primitives. However, Galindo et al. [10] pointed out that a dishonest authority could break the security of their generic constructions. Actually, these generic constructions were inherently flawed due to a naive use of double encryption without further treatments. In [17], Lu et al. solved this problem by using the Fujisaki-Okamoto conversions [8, 9] and gave a method to achieve generic CCA-secure CBE constructions in the random oracle model. In [7], Dodis and Katz claimed that their generic technique which was proposed to build multiple-encryption schemes from PKE schemes can also be applied to IBE and PKE (instead of two PKEs) to build CBE schemes without resorting to the random oracle model. However, their construction encrypts the messages in parallel by the encryption algorithms of IBE and PKE, which results in long ciphertext size. In [2], Al-Riyami and Paterson gave an analysis of Gentry's CBE concept and repaired a number of problems in the original definitions of CBE and its security model. They also presented a generic conversion from CL-PKE to CBE and claimed that a secure CBE scheme could be constructed from any secure CL-PKE scheme using this conversion. Kang and Park [14] pointed out that their conversion was incorrect due to the flaw in their security proof. This implies that the derived CBE scheme by Al-Riyami and Paterson [2] is therefore invalid. In [25], Yum and Lee proposed a separable implicit certificate revocation system called status CBE to relieve the certifier's burden of certificate revocation, in which the authenticity of a public key is guaranteed by a long-lived certificate and the certificate revocation problem is resolved by a short-lived certificate. However, Park and Lee [21] pointed that their status CBE scheme is insecure under the public key replacement attack. In [19], Morillo and Ràfols proposed the first concrete CBE scheme in the standard model from the Waters-IBE scheme [23] and the BB-IBE scheme [4]. Galindo et al. [11] revised this CBE scheme and proposed an improved one. In [16], Liu and Zhou proposed a new CBE scheme in the standard model from the Gentry-IBE scheme [13]. Recently, Lu et al. [18] proposed a quite efficient CBE scheme in the random oracle model from the SK-IBE scheme [22, 6] which requires computing only one pairing.

In this paper, we propose a new CBE scheme which is secure under the hardness of the computational Diffie-Hellman problem and the gap bilinear Diffie-Hellman problem in the random oracle model. The proposed CBE scheme requires computing only one pairing and introduces no redundancies in ciphertext. Compared with the existing CBE schemes, our scheme enjoys better performance on both the computation efficiency and the communication bandwidth. What is worth mentioning is that our scheme has low communication bandwidth and is more suitable for the bandwidth limited network.

The rest of this paper is organized as follows: In Section 2, we briefly review some background definitions including certificated-based encryption, symmetric encryption, bilinear map and hard problems on which the security of our scheme is based. In Section 3, we describe our CBE scheme. In Section 4, we give the result about the security of our scheme and make an efficiency comparison between our CBE scheme and the existing ones. In Section 5, we conclude our paper.

2   Preliminaries

In this section, we briefly review some background definitions including certificate-based encryption, symmetric encryption, bilinear map, and the hard problems on which the security of our CBE scheme is based.

2.1   Certificate-Based Encryption

In a CBE scheme, a CA will first generate the system parameter including a master key and a list of public system parameters. Then, the CA will use the system parameter to generate certificates for users in the system. Users will generate their own public/private key pairs and contact the certifier to obtain the corresponding certificates. A user should use its private key and certificate from the CA as the decryption key to decrypt the ciphertext which is sent to him. The following definition of CBE is taken from [1] essentially, where the original definition given in [12] was reconsidered.

Definition 1. A CBE scheme is defined by following five algorithms:

– Setup is a probabilistic algorithm taking as input a security parameter k. It returns CA's master-key msk and the public parameters $params$ that include the descriptions of a finite message space $MSPC$ and a finite ciphertext space $CSPC$. Usually, this algorithm is run by a CA. We consider the public parameters $params$ to be an implicit input to the rest of the algorithms.
– UserKeyGen is a probabilistic algorithm that outputs a public and private key pair (upk, usk).
– CertGen is a deterministic algorithm that takes the master key msk, an index τ of the current time period, a user's identity id and a public key upk as input. It returns a certificate $Cert_{id,\tau}$, which is sent to the user id through an open channel. Here τ is a string identifying a time period, while id contains other information needed to certify the user. Usually, this algorithm is run by a CA.
– Encrypt is a probabilistic algorithm that takes an index τ of the current time period, a user's identity id, a user's public key upk and the message $M \in MSPC$ as input. It returns a ciphertext $C \in CSPC$ for the message M.
– Decrypt is a deterministic algorithm that takes a user's private key usk, a user's certificate $Cert_{id,\tau}$ and a ciphertext C as input. It returns either a message M or the special symbol $\perp$ indicating a decryption failure.

Naturally, it is required that these algorithms must satisfy the standard consistency constraint, that is $\forall M \in MSPC$, Decrypt($params$, $Cert_{id,\tau}$, usk, Encryp($params$, τ, id, upk, M)) = M where $Cert_{id,\tau}$ = CertGen($params$, msk, τ, id, upk), and (upk^c usk) is a valid key-pair generated by the algorithm UserKeyGen.

The strongest security notion of a CBE scheme is IND-CBE-CCA2. Due to the space limitation, we omit the concrete definition here and refer the readers to [12, 1] for more details about the security notions of CBE.

2.2   Symmetric Encryption

A symmetric encryption scheme SE is specified by a deterministic encryption algorithm E and a deterministic decryption algorithm D. Let λ be a security parameter. Algorithm E takes a symmetric key $K \in \{0, 1\}^{\lambda}$ and a message M as input, and returns a ciphertext $C = \mathsf{E}_K(M)$. Algorithm D takes $K \in \{0, 1\}^{\lambda}$ and a ciphertext C as input, and returns either a message $M = \mathsf{D}_K(C)$ or a special symbol $\bot$ denoting a decryption failure.

Next, we review the notion of chosen-ciphertext security for a symmetric encryption scheme described in [15].

Definition 2. A symmetric encryption scheme $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ is said to be IND-SE-CCA2 secure if no adversary A has non-negligible advantage in the following game:

- The challenger randomly chooses a key $K \in \{0, 1\}^{\lambda}$.
- The adversary A issues a series of queries to the encryption oracle and the decryption oracle. The challenger responds these queries by using the key K.
- The adversary A outputs two plaintexts M_0 and M_1 which were not submitted to the encryption oracle or obtained from the decryption oracle. The challenger chooses a random bit $b \in \{0, 1\}$ and encrypts M_b using the key K. It then outputs the resulting ciphertext C^* to the adversary A.
- The adversary A issues more queries as in Phase 1, but with the restrictions that C^* can not be submitted to the decryption oracle and M_0, M_1 can not be submitted to the encryption oracle.
- The adversary A outputs a guess $b^{'} \in \{0, 1\}$ for β and wins the game if $b = b^{'}$. A's advantage in this game is defined to be $\mathsf{Adv}(\mathsf{A}) = 2|\Pr[b = b^{'}] - 1/2|$.

2.3   Bilinear Map and Hard Problems

Let G_1 be an additive cyclic group of a large prime order q and G_2 denotes a multiplicative cyclic group of the same order. Let P be a generator of G_1. A mapping e: $G_1 \times G_1 \rightarrow G_2$ is called a bilinear map if it satisfies the following properties:

- Bilinearity: $\forall P_1, P_2 \in G_1, \forall a, b \in Z_q^{*}$, we have $e(aP_1, bP_2) = e(P_1, P_2)^{ab}$.
- Non-degeneracy: $e(P, P) \neq 1$.
- Computability: $\forall P_1, P_2 \in G_1, e(P_1, P_2)$ can be efficiently computed.

Definition 3. The computational Diffie-Hellman (CDH) problem in G_1 is, given (P, aP, bP) with uniformly random choices of $a, b \in Z_q^{*}$, to compute $abP \in G_1$. Let $\mathcal{B}$ be an adversary against the hardness of the CDH problem. $\mathcal{B}$'s advantage is defined to be $Adv(\mathcal{B}) = \Pr[\mathcal{B}(P, aP, bP) = abP]$.

Definition 4 [20]. The gap bilinear Diffie-Hellman (Gap-BDH) problem in (G_1, G_2) is, given (P, aP, bP, cP) with uniformly random choices of $a, b, c \in Z_q^{*}$, to compute $e(P, P)^{abc}$ with the help of a DBDH oracle $\mathcal{O}_{DBDH}(\cdot)$ that takes (P, aP, bP, cP, T) as input

and outputs 1 if $T = e(P, P)^{abc}$ and 0 otherwise. Let $\mathcal{B}$ be an adversary against the hardness of the Gap-BDH problem. $\mathcal{B}$'s advantage is defined to be $Adv(\mathcal{B}) = \Pr[\mathcal{B}(P, aP, bP, cP, \mathcal{O}_{DBDH}(\cdot)) = e(P, P)^{abc}]$.

3   A New CBE Scheme

Our scheme is constructed based on a hybrid variant of the BF-IBE scheme proposed by Libert and Quisquater [15]. It is described as follows:

Setup(1^k): It performs the following steps:

- Generate a pair of cycle groups (G_1, G_2) of prime order q and a bilinear map e: $G_1 \times G_1 \rightarrow G_2$.
- Choose a random generator $P \in G_1$ and a random element $s \in Z_q^*$, compute $P_{pub} = sP$.
- Choose two cryptographic hash functions H_1: $\{0, 1\}^* \rightarrow G_1^*$ and H_2: $(G_1)^3 \times G_2 \rightarrow \{0, 1\}^{\lambda}$, as well as a symmetric encryption scheme $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ of keylength λ, where λ is polynomial in k.
- Output s as the master key msk and $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, \lambda, \mathsf{E}, \mathsf{D}, n\}$ as the public parameters $params$, where n denotes a bound on the size of plaintexts. The plaintext space is $MSPC = \{0, 1\}^n$ and the ciphertext space is $CSPC = G_1 \times \{0, 1\}^n$.

UserKeyGen($params$): It chooses a random element $x \in Z_q^*$ as the private key usk and sets xP as the corresponding public key upk.

CertGen($params$, msk, τ, id, upk): It computes and outputs $Cert_{id, \tau} = sQ_{id}$ as the certificate for the identity id in the time period τ, where $Q_{id} = H_1(\tau, id, upk)$.

Encrypt($params$, τ, id, upk, M): It performs the following steps:

- Choose a random $r \in Z_q^*$ and compute $U = rP$. Compute $SK = H_2(Q_{id}, U, r \cdot upk, e(P_{pub}, Q_{id})^r)$ where $Q_{id} = H_1(\tau, id, upk)$.
- Compute $V = \mathsf{E}_K(M)$ and outputs $C = (U, V)$ as the ciphertext.

Notice that once $e(P_{pub}, Q_{id})$ has been pre-computed, the above encryption algorithm does not require any pairing computations to send messages to the user id in the time period τ.

Decrypt($params$, $Cert_{id, \tau}$, usk, $C = (U, V)$): It computes $SK = H_2(Q_{id}, U, usk \cdot U, e(U, Cert_{id, \tau}))$ and outputs the message $M = \mathsf{D}_K(V)$.

The consistency of the above CBE scheme is easy to check as we have

$$SK = H_2(Q_{id}, U, usk \cdot U, e(U, Cert_{id, \tau}))$$

$$= H_2(Q_{id}, U, r \cdot upk, e(P_{pub}, Q_{id})^r).$$

4   Security and Efficiency Analysis

Under the hardness of the CDH problem and the Gap-BDH problem, we have proved our CBE scheme is IND-CNE-CCA2 secure in the random oracle model. The following theorem is our result about the security of our scheme.

Theorem 1. *Suppose that H_1, H_2 are random oracles and the symmetric encryption scheme* SE *is IND-SE-CCA2 secure, then the above CBE scheme is IND-CBE-CCA2 secure under the hardness of the CDH problem and the Gap-BDH problem.*

Proof. We will write the proof of this theorem in the full version of this paper.

We now make an efficiency comparison between our scheme and the existing CBE schemes. In the computation cost comparison, we consider three major operations: Pairing (p), Multiplication (m), and Exponentiation (e). Among these operations, the pairing operation is considered as the heaviest time-consuming one in spite of the recent advances in the implementation technique in [3]. As usual, all symmetric operations are ignored. Moreover, we denote the signing algorithm and the verification algorithm in the signature scheme by (*Sign*, *Vfy*). In the communication cost comparison, ciphertext expansion represents the length difference between the ciphertext and the plaintext. The length of a string X is denoted by |X|. We denote the public commitment string and the de-commitment string in an encapsulation scheme by *com* and *dec* respectively, the message authentication code by *mac*, and the verification key and the signature in a one-time signature scheme by *vk* and σ respectively. Ciphertext expansion represents the difference between the ciphertext length and the message length. In [12] and [18], l should be at least 160 in order to obtain a reasonable security. Considering the pre-computation, the detailed performances of all the CBE schemes are listed in Table 1.

Table 1. Efficiency comparison

Scheme	Computation Cost		Communication Cost		
	Encryption	Decryption	Ciphertext Expansion	Public Key	Certificate
Gentry03 [12]	$2p+1m+1e$	$1p+1m$	$|G_1|+l$	$|G_1|$	$|G_1|$
MR06 [19]	$4m+2e$	$3p+3m$	$3|G_1|+|dec|+|com|+|mac|$	$2|G_1|$	$2|G_1|$
GMR08 [11]	$5m+2e+Sign$	$3p+3m+Vfy$	$3|G_1|+|vk|+|\sigma|$	$2|G_1|$	$2|G_1|$
LZ [16]	$2m+7e$	$2p+1m+2e$	$2|G_2|+|G_1|$	$6|G_1|$	$3|G_1|+3|Z_q|$
LLX 09[18]	$2m+2e$	$1p+1m+1e$	$|G_1|+l$	$|G_2|$	$|G_1|$
Our Scheme	$2m+1e$	$1p+1m$	$|G_1|$	$|G_1|$	$|G_1|$

From the table, we can see that our scheme has better performances on both the computation efficiency and the communication bandwidth. What is worth mentioning is that our scheme introduces non redundancies in ciphertext and has short public keys and short certificates. Therefore, it is more suitable for the bandwidth limited network.

5   Conclusion

In this paper, we present a new CBE scheme which is IND-CBE-CCA2 secure under the hardness of the CDH problem and the Gap-BDH problem in the random oracle model. Our scheme does not require computing any pairings in the encryption algorithm and requires computing only one pairing in the decryption algorithm. Furthermore, our scheme introduces non redundancies in ciphertext and has short public keys and short certificates. When compared with the previous CBE schemes, our CBE scheme has obvious advantage on both the computation efficiency and the communication bandwidth.

References

1. Al-Riyami, S.S., Paterson, K.G.: Certificateless Public Key Cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003)
2. Al-Riyami, S.S., Paterson, K.G.: CBE from CL-PKE: A Generic Construction and Efficient Schemes. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 398–415. Springer, Heidelberg (2005)
3. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient Algorithms for Pairing-based Cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–368. Springer, Heidelberg (2002)
4. Boneh, D., Boyen, X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
5. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
6. Chen, L., Cheng, Z.: Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 442–459. Springer, Heidelberg (2005)
7. Dodis, Y., Katz, J.: Chosen-Ciphertext Security of Multiple Encryption. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 188–209. Springer, Heidelberg (2005)
8. Fujisaki, E., Okamoto, T.: Secure Integration of Asymmetric and Symmetric Encryption Schemes. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg (1999)
9. Fujisaki, E., Okamoto, T.: How to Enhance the Security of Public-Key Encryption at Minimum Cost. In: Imai, H., Zheng, Y. (eds.) PKC 1999. LNCS, vol. 1560, pp. 53–68. Springer, Heidelberg (1999)
10. Galindo, D., Morillo, P., Ràfols, C.: Breaking Yum and Lee Generic Constructions of Certificate-Less and Certificate-Based Encryption Schemes. In: Atzeni, A.S., Lioy, A. (eds.) EuroPKI 2006. LNCS, vol. 4043, pp. 81–91. Springer, Heidelberg (2006)
11. Galindo, D., Morillo, P., Ràfols, C.: Improved Certificate-based Encryption in the Standard Model. Journal of Systems and Software 81(7), 1218–1226 (2008)
12. Gentry, C.: Certificate-based Encryption and the Certificate Revocation Problem. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 272–293. Springer, Heidelberg (2003)
13. Gentry, C.: Practical Identity-based Encryption without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)

14. Kang, B.G., Park, J.H.: Is It Possible to Have CBE from CL-PKE? Cryptology ePrint Archive, Report 2005/431 (2005), `http://eprint.iacr.org/`
15. Libert, B., Quisquater, J.J.: Identity Based Encryption without Redundancy. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 285–300. Springer, Heidelberg (2005)
16. Liu, J.K., Zhou, J.: Efficient Certificate-based Encryption in the Standard Model. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) SCN 2008. LNCS, vol. 5229, pp. 144–155. Springer, Heidelberg (2008)
17. Lu, Y., Li, J.G., Xiao, J.M.: Generic Construction of Certificate-Based Encryption. In: 9th International Conference for Young Computer Scientists, pp. 1518–1594. IEEE CS, New York (2008)
18. Lu, Y., Li, J.G., Xiao, J.M.: Constructing Efficient Certificate-based Encryption with Paring. Journal of Computers 4(1), 19–26 (2009)
19. Morillo, P., Ràfols, C.: Certificate-based Encryption without Random Oracles. Cryptology ePrint Archive, Report 2006/12 (2006), `http://eprint.iacr.org/`
20. Okamoto, T., Pointcheval, D.: The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes. In: Kim, K.-c. (ed.) PKC 2001. LNCS, vol. 1992, pp. 104–111. Springer, Heidelberg (2001)
21. Park, J.H., Lee, D.H.: On the Security of Status Certificate-based Encryption Scheme. IEICE Trans. Fundamentals E90-A(1), 303–304 (2007)
22. Sakai, R., Kasahara, M.: ID Based Cryptosystems with Pairing on Elliptic Curve. Cryptology ePrint Archive, Report 2003/054 (2003), `http://eprint.iacr.org/`
23. Waters, B.: Efficient Identity-based Encryption without Random Oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
24. Yum, D.H., Lee, P.J.: Identity-Based Cryptography in Public Key Management. In: Katsikas, S.K., Gritzalis, S., López, J. (eds.) EuroPKI 2004. LNCS, vol. 3093, pp. 71–84. Springer, Heidelberg (2004)
25. Yum, D.H., Lee, P.J.: Separable Implicit Certificate Revocation. In: Park, C.-s., Chee, S. (eds.) ICISC 2004. LNCS, vol. 3506, pp. 121–136. Springer, Heidelberg (2005)

Efficient Forward-Secure Identity-Based Encryption Scheme in the Standard Model

Yang Lu

College of Computer and Information Engineering,
Hohai University
Nanjing City, Jiangsu Province, China
`luyangnsd@163.com`

Abstract. The paradigm of forward security provides a promising approach to deal with the secret key exposure. It guarantees that the compromise of current secret keys does not compromise past secret keys and past communications. Therefore, forward security can minimize the resulting damage caused by the secret key exposure. In this paper, we propose a new forward-secure identity-based encryption (FS-IBE) scheme which is forward-secure against adaptive chosen-ciphertext attacks under in the standard model. In the proposed scheme, some of the main efficiency parameters are independent on the total number of time periods. Compared with the existing FS-IBE scheme, our scheme is much more efficient.

Keywords: Forward security, key exposure, identity-based encryption, standard model.

1   Introduction

In traditional public key cryptography, private keys are generated randomly with no connection to users' identities. Therefore, a Public Key Infrastructure (PKI) is used to provide an assurance to the users about the relationship between a public key and the identity of the holder of the corresponding private key by certificates. However, the need for PKI supporting certificates is considered as the main difficulty in the deployment and management of traditional public key cryptography. To simplify the management of the public key certificates, Shamir [12] introduced the notion of identity-based cryptography (IBC) in 1984. In IBC, the public key of each user is derived directly from certain aspects of its identity, such as an IP address or an e-mail address, and the corresponding private key is generated by a trusted third party called Private Key Generator (PKG). Rather than obtaining the disparate public keys and the corresponding certificates of its intended recipients separately as is done in traditional public key cryptography, a message sender who knows the identities of its recipients needs only to obtain the public parameters of the PKG. Therefore, the main practical benefit of IBC lies in great reduction of need for public key certificates and certificate authorities. However, it was an open problem to construct an efficient identity-based encryption (IBE) scheme until almost two decades after Shamir posed the initial open question in [12]. In 2001, Boneh and Franklin [5] presented the first practical and

provably secure IBE scheme using the bilinear pairings on elliptic curves. Despite its only recent invention, IBE has been used extensively in practice, and is currently in the process of getting standardized.

The paradigm of forward security provides a promising approach to deal with the key exposure. The central idea of forward security is that the compromise of current secret keys does not compromise past secret keys. The notion of forward security was first proposed in the context of key-exchange protocols by Günther [11] and later by Diffie, et al. [8]. In forward-secure key-exchange protocols, compromise of long-term secret keys does not compromise past session keys. A forward-secure key-exchange protocol naturally gives rise to an interactive forward-secure encryption scheme in which the two communication parties interact to generate a shared key which is erased immediately after being used to encrypt a single message. The notion of non-interactive forward security was first proposed by Anderson [1] and later formalized in the context of signature by Bellare and Miner [2]. In the model formalized by Bellare and Miner, the lifetime of the system is divided into N time periods labeled $0,\ldots, N$-1, and secret keys are evolved at regular time periods with the time of the system. The device begins by storing secret key SK_0. At the beginning of each time period i, the device applies some key-evolving algorithm to the previous secret key SK_{i-1} in order to derive the secret key SK_i which is used in the time period i, and then deletes the previous secret key SK_{i-1}. Notice that if being in a public-key cryptosystem, the public keys are never updated and remains fixed while the private keys are evolved with the time. A forward-secure cryptosystem guarantees that an adversary who learns the secret key SK_i for a time period i will be unable to break the security of the system for all time periods prior to i.

As pointed out by Yao, et al. [13], the standard notion of IBE security is vulnerable to the secret key exposure. Therefore, forward-secure IBE (FS-IBE) schemes would be desirable. In [13], Yao, et al. proposed a forward-secure hierarchical identity-based encryption scheme in the random oracle model [7] by combining the forward-secure public key scheme proposed by Canetti, et al. [6] with the hierarchical identity-based encryption scheme proposed by Gentry and Silverberg [9]. We write this scheme to be YFDL04 scheme for short. In the YFDL04 scheme, the dependency of all the performance parameters on the total number of time periods is poly-logarithmic. Suppose that N is the total number of distinct time periods, then the first-level of this scheme results in ciphertext/public key/private key of size $O(log_2N)$ and key generation/key update/encryption/decryption of time $O(log_2N)$. Obviously, the YFDL04 scheme is quite inefficient for large values of N. In this paper, we construct a quite efficient FS-IBE scheme which is secure in the standard model. In our scheme, some of main efficiency parameters are independent on the total number of time periods. What is worth mentioning is that the ciphertext in our scheme consists of only four or five group elements and the decryption requires only three or four pairing operations. Compared with the first-level of the YFDL04 scheme, our FS-IBE scheme is much more efficient.

The rest paper is organized as follows: In Section 2 we briefly review the definition of bilinear map and describe the hardness assumption on which the security of our scheme is based. In Section 3 we give the definitions of FS-IBE and its security. In Section 4 we present a FS-IBE scheme which is provably secure in the standard model. In Section 5, we make an efficiency comparison between our scheme and the first-level of the YFDL04 scheme. In Section 6, we conclude our paper.

2   Bilinear Map and Hardness Assumption

Let p be a large prime number, G_1 and G_2 denote two multiplicative cyclic groups of the same order p. A mapping $e: G_1 \times G_1 \rightarrow G_2$ is called a bilinear map if it satisfies the following properties:

- Bilinearity: $e(u^a, v^b) = e(u, v)^{ab}$ for all $u, v \in G_1$ and $a, b \in Z_p^*$.
- Non-degeneracy: $e(g, g) \neq 1$ for a random generator $g \in G_1$.
- Computablity: $e(u, v)$ can be efficiently computed for all $u, v \in G_1$.

The security of our scheme is based on a complexity assumption called the truncated decision q-augmented bilinear Diffie-Hellman exponent (q-ABDHE) assumption proposed by Gentry in [10]. Let $q = q(k)$ be a polynomial. The truncated decision q-ABDHE problem is defined as follows: Given $(g, g^\alpha, \ldots, g^{\alpha^q}, g', g'^{\alpha^{q+2}})$ $\in G_1^{q+3}$ and an element $T \in G_2$, where g and g' be generators of G and α be a random element in Z_p^*, decide whether $T = e(g, g')^{\alpha^{q+1}}$ or T is a random element of G_2. Let A be a probabilistic algorithm against the truncated decision q-ABDHE problem. The advantage of the algorithm A in solving the truncated decision q-ABDHE problem is defined to be

$$\left| \Pr\{ A(g, g^\alpha, \ldots, g^{\alpha^q}, g', g'^{\alpha^{q+2}}, e(g, g')^{\alpha^{q+1}}) = 1 \} \right.$$
$$\left. - \Pr\{ A(g, g^\alpha, \ldots, g^{\alpha^q}, g', g'^{\alpha^{q+2}}, T) = 1 \} \right|.$$

Definition 1. We say that the truncated decision (t, ε, q)-ABDHE assumption holds in (G_1, G_2) if no t-time algorithm has advantage at least ε over random guessing in solving the truncated decision q-ABDHE problem in (G_1, G_2).

3   Definitions of Forward-Secure Identity-Based Encryption

Our definitions of FS-IBE generalize the standard notions of IBE, similar to the way in [6] where the definitions of FS-PKE generalize the standard notions of PKE. Similar definitions of forward security for HIBE can be found in [13].

Definition 2. A forward-secure identity-based encryption (FS-IBE) scheme is a 5-tuple of PPT algorithms (*Setup*, *KeyGen*, *KeyUpd*, *Enc*, *Dec*) such that:

- *Setup* takes as input a security parameter 1^k and the total number of time periods N. It returns the system public parameters *params* and the PKG's master key *msk* that is kept secret. Usually, this algorithm is performed by a PKG.
- *KeyGen* takes as input *params*, *msk*, and a user's identity *id*. It returns the user's initial private key $SK_{id|0}$. Usually, this algorithm is also performed by a PKG.
- *KeyUpd* takes as input *params*, an index $i \in [0, N\text{-}1]$ of the current time period, and the associated private key $SK_{id|i}$. It returns a private key $SK_{id|i+1}$ for the time period $i+1$.

- *Enc* takes as input *params*, an identity *id*, an index $i \in [0, N)$ of the current time period, and a message *M*. It returns a ciphertext *C* for the time period *i*.
- *Dec* takes as input *params*, an index $i \in [0, N)$ of the current time period, a private key $SK_{id|i}$, and a ciphertext *C*. It returns a message *M* or $\perp$ if *C* is invalid.

Definition 3. A FS-IBE scheme is said to be $(t, q_k, q_d, \varepsilon)$-FS-ID-CCA secure if for any *t*-time adversary that makes at most q_k key extraction queries and at most q_d decryption queries has advantage at most ε in the following game:

- **Setup.** The challenger runs *Setup* to generate *params* and *msk*. It gives the adversary *params* and keeps *msk* to itself.
- **Phase 1.** The adversary issues a series of key extraction queries and decryption queries adaptively. The challenger responds as follows:

  - On key extraction query <*id*, *i*> where $i \in [0, N)$, the challenger runs algorithm *KeyGen* to generate the initial private key $SK_{id|0}$ for the identity *id*, then runs algorithm *KeyUpd* recursively to derive the private key $SK_{id|i}$ for the time period *i*. Finally, it returns the key $SK_{id|i}$ to the adversary.
  - On decryption query <*id*, *i*, *C*>, the challenger first generates the private key $SK_{id|i}$ as above, then runs *Dec* to decrypt *C* using $SK_{id|i}$ and returns the resulting plaintext to the adversary.

- **Challenge.** Once the adversary decides that Phase 1 is over, it outputs an identity id^*, a time period i^*, and two equal length plaintexts M_0 and M_1 on which it wishes to be challenged. The constraint is that no private key query has been issued for the identity id^* for any time period $0 \leq j \leq i^*$. The challenger chooses a random bit $b \in \{0, 1\}$, and sets $C^* = Enc(params, id^*, i^*, M_b)$. It sends C^* as the challenge ciphertext to the adversary.
- **Phase 2.** The adversary issues more private key queries and decryption queries. The constraint is that <id^*, *j*> where $0 \leq j \leq i^*$ is not a subject of the private key queries, and <id^*, i^*, C^*> is not a subject of the decryption queries.
- **Guess.** Finally, the adversary outputs a guess $b' \in \{0, 1\}$ and wins the game if $b = b'$. The advantage of the adversary is defined to be $|Pr[b = b'] - 1/2|$.

4   A New FS-IBE Scheme

In this section, we present a new FS-IBE scheme which is FS-ID-CCA secure in the standard model. Our scheme is constructed from the IBE scheme proposed by Gentry [10] and the HIBE scheme proposed by Boneh, Boyen and Goh [4].

To update the users' private keys, we take a labeled full binary tree as the key evolving-tree. To do so, we associate the time periods with all nodes of the binary tree. Assume that the total number of time periods $N \leq 2^{l+1}-1$, this binary tree has depth *l*. For an identity *id*, let $id|\omega^{(i)}$ denote the node associated with the time period $i \in [0, N)$, we associate the time periods with all nodes of the binary tree according to a pre-order traversal as follows:

- Set $id|\omega^{(0)}$ to be the root node of the tree (i.e., $id|\omega^{(0)} = id|\varepsilon$).
- If $id|\omega^{(i)}$ is an internal node then $id|\omega^{(i+1)} = id|\omega^{(i)}0$;
- Else if $id|\omega^{(i)}$ is a leaf node and $i < N$-1 then $id|\omega^{(i+1)} = id|\omega'1$, where ω' is the longest binary string such that $\omega'0$ a prefix of $\omega^{(i)}$.

Moreover, the private key $SK_{id|i}$ for a given time period i consists of the secret key for the node $id|\omega^{(i)}$ (which is acted as the decryption key in the time period i) and the secret keys for all right siblings of the nodes on the path from the root to the node $id|\omega^{(i)}$ (which are used to update the private key from $SK_{id|i}$ to $SK_{id|i+1}$ at the beginning of the time period $i+1$).

For simplification, we assume that the identities in our FS-IBE scheme are elements in Z_p^*. Of course, we can extend our scheme to identities over $\{0, 1\}^*$ by first hashing the identities into elements in Z_p^* using a collision resistant hash function $H: \{0, 1\}^* \to Z_p^*$. Let G_1 and G_2 be two groups of prime order p, and let $e: G_1 \times G_1 \to G_2$ be a bilinear map. Our scheme is described as follows:

Setup: The PKG selects a random generator $g \in G_1$ and a random element $\alpha \in Z_p^*$. It sets $g_1 = g^\alpha$. It furthermore randomly choose $g_2, h_1,\ldots,h_l \in G_1$ and a hash function H from a family of universal one-way hash functions. The system public parameters are $params = (N, g, g_1, g_2, h_1,\ldots,h_l, H)$ and the master key is $msk = \alpha$.

KeyGen: The PKG selects a random $r_{id} \in Z_p^*$ and sets $SK_{id|0} = (r_{id}, (g_2 g^{-r_{id}})^{\frac{id}{\alpha}})$ as the initial private key for the identity id.

To simplify the description of the **KeyUpd** algorithm, we define an additional algorithm as follows:

KeyExtract: On input $params$ and the secret key $sk_{id|\omega}$ associated with node $id|\omega$, this algorithm generates and outputs the secret key for nodes $id|\omega0$ and $id|\omega1$ as follows: If $id|\omega = id|\varepsilon$, this algorithm selects a random $s \in Z_p^*$ and outputs

$$sk_{id|0} = (r_{id}, (g_2 g^{-r_{id}})^{\frac{id}{\alpha}}, g_1^r, h_2^r, \ldots, h_l^r) \text{ and } sk_{id|1} = (r_{id}, (g_2 g^{-r_{id}})^{\frac{id}{\alpha}} \cdot h_1^r, g_1^r, h_2^r, \ldots, h_l^r).$$

Else, let $id|\omega = id|\omega_1\ldots\omega_k \in \{0,1\}^k$, it first parses $sk_{id|\omega}$ as $(a_0, a_1, a_2, b_{k+1}, \ldots, b_l)$, where

$$a_0 = r_{id}, a_1 = (g_2 g^{-r_{id}})^{\frac{id}{\alpha}} \cdot (\prod_{i=1}^{k} h_i^{\omega_i})^r, a_2 = g_1^r, b_{k+1} = h_{k+1}^r, \ldots, b_l = h_l^r.$$

It then selects a random $s \in Z_p^*$ and outputs

$$sk_{id|\omega\omega_{k+1}} = (a_0, a_1 \cdot b_{k+1}^{\omega_{k+1}} \cdot (\prod_{i=1}^{k+1} h_i^{\omega_i})^s, a_2 \cdot g_1^s, b_{k+2} \cdot h_{k+2}^s, \ldots, b_l \cdot h_l^s),$$

where $\omega_{k+1} \in \{0,1\}$. Let $r' = r + s$, it is easy to verify that

$$sk_{id|\omega\omega_{k+1}} = (r_{id}, (g_2 g^{-r_{id}})^{\frac{id}{\alpha}} \cdot (\prod_{i=1}^{k+1} h_i^{\omega_i})^{r'}, g_1^{r'}, h_{k+2}^{r'}, \ldots, h_l^{r'}).$$

Therefore, $sk_{id|\omega\omega_{k+1}}$ is a valid secret key for the node $id|\omega_1\ldots\omega_{k+1} \in \{0,1\}^{k+1}$.

KeyUpd: To derive the private key $SK_{id|i+1}$ for the time period $i+1$, this algorithm performs as follows: If the node $id|\omega^{(i)}$ according to the time period i is an internal node, then run **KeyExtract** to generate the secret keys $sk_{id|\omega^{(i)}0}$ and $sk_{id|\omega^{(i)}1}$ for the two child nodes of the node $id|\omega^{(i)}$, and output the private key $SK_{id|i+1} = \{sk_{id|\omega^{(i)}0}, sk_{id|\omega^{(i)}1}\} \cup (SK_{id|i} - \{sk_{id|\omega^{(i)}}\})$; Else if $id|\omega^{(i)}$ is a leaf node, then simply output $SK_{id|i+1} = SK_{id|i} - \{sk_{id|\omega^{(i)}}\}$.

Enc: To encrypt $M \in G_2$ using id in the time period i, if $i = 0$, the sender selects a random $t \in Z_p^*$ and computes the ciphertext

$$C = (c_1, c_2, c_3, c_4) = (M \cdot e(g, g_2)^{-id \cdot t}, e(g, g)^{id \cdot t}, g_1^t, (h_1 h_2^\beta)^t) \in G_2^2 \times G_1^2 ,$$

where $\beta = H(c_1, c_2, c_3)$. Else, let the node according to the time period i to be $id \mid \omega_1 ... \omega_k \in \{0,1\}^k$, this algorithm selects a random $t \in Z_p^*$ and computes the ciphertext

$$C = (c_1, c_2, c_3, c_4, c_5) = (M \cdot e(g, g_2)^{-id \cdot t}, e(g, g)^{id \cdot t}, g_1^t, (\prod_{i=1}^{k} h_i^{\omega_i})^t, (h_1 h_2^\beta)^t) \in G_2^2 \times G_1^3 ,$$

where $\beta = H(c_1, c_2, c_3, c_4)$. Notice that encryption does not require any paring computations once $e(g, g)$ and $e(g, g_2)$ have been pre-computed.

Dec: To decrypt the ciphertext C using $SK_{id|i}$, if $i = 0$, the receiver first parses C as (c_1, c_2, c_3, c_4) and $SK_{id|0}$ as (a_0, a_1) , then computes $\beta = H(c_1, c_2, c_3)$ and verifies whether $e(g_1, c_4) = e(c_3, h_1 h_2^\beta)$. If so, it outputs the plaintext

$$M = c_1 \cdot e(c_3, a_1) \cdot c_2^{a_0} .$$

Else, let the node according to the time period i to be $id \mid \omega^{(i)} = id \mid \omega_1 ... \omega_k \in \{0,1\}^k$, it first parses C as $(c_1, c_2, c_3, c_4, c_5)$ and $sk_{id|\omega^{(i)}}$ as $(a_0, a_1, a_2, b_{k+1}, ..., b_l)$, then computes $\beta = H(c_1, c_2, c_3, c_4)$ and verifies whether $e(g_1, c_5) = e(c_3, h_1 h_2^\beta)$. If so, it outputs the plaintext

$$M = c_1 \cdot e(c_3, a_1) \cdot c_2^{a_0} \cdot e(a_2, c_4)^{-1} .$$

The correctness of above scheme can be checked as follows:

(1) $e(g_1, c_4) = e(g_1, c_5') = e(g_1, (h_1 h_2^\beta)^t) = e(g_1^t, h_1 h_2^\beta) = e(c_3, h_1 h_2^\beta) = e(c_3', h_1 h_2^\beta)$.

(2) $c_1 \cdot e(c_3, a_1) \cdot c_2^{a_0} = M \cdot e(g, g_2)^{-id \cdot t} \cdot e(g_1^t, (g_2 g^{-r_{id}})^{\frac{id}{\alpha}}) \cdot (e(g, g)^{id \cdot t})^{r_{id}} = M$.

(3) $c_1 \cdot e(c_3, a_1) \cdot c_2^{a_0} \cdot e(a_2, c_4)^{-1}$

$$= \frac{M \cdot e(g, g_2)^{-id \cdot t} \cdot e(g_1^{t}, (g_2 g^{-r_{id}})^{\frac{id}{\alpha}} \cdot (\prod_{i=1}^{k} h_i^{\omega_i})^r) \cdot (e(g, g)^{id \cdot t})^{r_{id}}}{e(g_1^{r}, (\prod_{i=1}^{k} h_i^{\omega_i})^t)} = M .$$

We can prove that the above FS-IBE scheme is FS-ID-CCA secure in the standard model. The following theorem is our result about the security of the scheme.

Theorem 1. Let $q = q_k + 1$. Assume that the truncated decision (t, ε, q)-ABDHE assumption holds in (G_1, G_2). Then, the above FS-IBE scheme is $(t^{'}, \varepsilon, q_k, q_d)$-FS-ID-CCA secure for $t^{'} = t - O(t_{exp} \cdot q^2 \cdot l)$, where t_{exp} is the time required to compute the exponent in G_1.

Proof. We will write the proof of this theorem in the full version of this paper.

5   Efficiency Comparison

In Table 1, we make an efficiency comparison between our scheme and the first-level of the YFDL04 scheme [13].

Table 1. Efficiency comparison

Parameters	YFDL04 [13]	Ours
Key generation time	$O(\log_2 N)$	$O(1)$
Key update time	$O(\log_2 N)$	$O(1)$
Encryption time	$O(\log_2 N)$	$O(1) \sim O(\log_2 N)$
Decryption time	$O(\log_2 N)$	$O(1)$
Ciphertext length	$O(\log_2 N)$	$O(1)$
Public key length	$O(\log_2 N)$	$O(\log_2 N)$
Private key length	$O(\log_2 N)$	$O(\log_2 N)$

From the table, we can see that the time required for key generation, key update and decryption, and the length of ciphertext in our scheme are independent on the total number of time periods N. At the same time, the dependency of these performance parameters of the YFDL04 scheme on the total number of time periods N is poly-logarithmic. The ciphertext in our scheme consists of only four or five group elements and the decryption requires only three or four pairing operations. Furthermore, the security of our scheme is hold in the standard model while the security of the YFDL04 scheme is proved only in the random oracle model. Therefore, our FS-IBE scheme is much more efficient and practical than the first-level of the YFDL04 scheme.

6   Conclusion

In this paper, we proposed a new FS-IBE scheme which is secure in the standard model. In our scheme, some of main efficiency parameters are independent on the

total number of time periods. What is worth mentioning is that the ciphertext in our scheme consists of only four or five group elements and the decryption requires only three or four pairing operations. When compared with the existing scheme, our FS-IBE scheme is much more efficient and practical.

References

1. Anderson, R.: Two Remarks on Public Key Cryptology. In: Invited Lecture, 4th ACM Conference on Computer and Communications Security (1997),
   http://www.cl.cam.ac.uk/ftp/users/rja14/forwardsecure.pdf
2. Bellare, M., Miner, S.K.: A Forward-Secure Digital Signature Scheme. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 431–448. Springer, Heidelberg (1999)
3. Bellare, M., Rogaway, P.: Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In: 1st ACM Computer and Communications Security Conference, pp. 62–73. ACM, New York (1993)
4. Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical Identity Based Encryption with Constant Size Ciphertext. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)
5. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
6. Canetti, R., Halevi, S., Katz, J.: A Forward-Secure Public-Key Encryption Scheme. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 255–271. Springer, Heidelberg (2003)
7. Canetti, R., Goldreich, O., Halevi, S.: The Random Oracle Methodology, Revisited. Journal of the ACM 51(4), 557–594 (2004)
8. Diffie, W., Van-Oorschot, P.C., Weiner, M.J.: Authentication and Authenticated Key Exchanges. Des.,Codes, Cryptography 2(2), 107–125 (1992)
9. Gentry, C., Silverberg, A.: Hierarchical ID-based Cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002)
10. Gentry, C.: Practical Identity-Based Encryption without Random Oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
11. Günther, C.G.: An Identity-Based Key-Exchange Protocol. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 29–37. Springer, Heidelberg (1990)
12. Shamir, A.: Identity-Based Cryptosystems and Signature Schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
13. Yao, D., Fazio, N., Dodis, Y., Lysyanskaya, A.: ID-Based Encryption for Complex Hierarchies with Applications to Forward Security and Broadcast Encryption. In: 11th ACM Conference on Computer and Communications Security, pp. 354–363. ACM, New York (2004)

Kolmogorov and Linear Widths on Generalized Besov Classes in the Monte Carlo Setting*

Liqin Duan[1] and Peixin Ye[2,**]

[1] Institute of Mathematics, Hangzhou Dianzi University, Hangzhou 310018, China
[2] School of Mathematics, Nankai University, Tianjin 300071, China
yepx@nankai.edu.cn

Abstract. In this paper, we studied the Kolmogorov and the linear widths on the generalized Besov classes $B_{p,\theta}^{\Omega}$ in the norm of L_q in the Monte Carlo setting. Applying the discretization technique and some properties of pseudo-s-scale, we determined the exact asymptotic orders of the Kolmogorov and the linear widths for certain values of the parameters p, q, θ.

Keywords: Kolmogorov width, linear width, generalized Besov class, Monte Carlo methods.

1 Introduction

The theory of information-based complexity has created notions and tools to understand the efficiency issues both for deterministic and Monte Carlo methods. This way some comparison between the deterministic and the Monte Carlo settings becomes possible. What is the superiority of Monte Carlo methods compared with deterministic methods, i.e., can it be of help to involve chance, randomness into numerical processes, and if yes, in which situations is this advisable? The first results about the analysis of efficiency of randomized(Monte Carlo) methods were due to Bakhvalov [1] in 1959, while an intensive wider research started only after the theory of information-based complexity [2] was established. For the general background on the theory of information-based complexity, we can refer to Traub, Wasilkowski, Woʹzniakowski [2].

Recently many authors have investigated the complexity of problems on function approximation,quadrature formulae, approximate solutions of differential and integral equations [2–10] in the randomized setting. In particular, Novak [10], Mathʹe [8, 9] and Heinrich [5, 6] studied the approximation problems on the classical multivariate Sobolev space $W_p^r([0,1]^d)$ in the norm of $L_q([0,1]^d)$, $1 \le p$, $q \le \infty$ by different methods in the deterministic and the Monte Carlo settings.From the point of view of approximation efficiency, the randomized methods lead to considerably better rates than those of the deterministic ones in many cases. The detailed analysis can be found in Heinrich [5] and Mathʹe [9]. In [11, 12], we also studied the approximation problems on the Sobolev classes with bounded mixed derivative in the Monte Carlo setting.

---

* Project supported by the NSF of China(Grant No.10926056 and No.10971251).
** Corresponding author.

Q. Zhou (Ed.): ICTMF 2011, CCIS 164, pp. 70–76, 2011.
© Springer-Verlag Berlin Heidelberg 2011

It is well-known that the Besov classes of functions also play an important role in the approximation theory and other mathematical fields. For the approximation characteristics of the classes, many researchers have devoted their efforts to the classes and obtained many meaningful results. For more information, we can refer to [13–16] and the references therein. In 1994, N.N. Pustovoitov [17] introduced a function class $H_q^{\Omega}(T^d)$. He first used a standard function $\Omega(t)$, a prototype of which is $\Omega(t) = t^r := t_1^{r_1} \cdots t_d^{r_d}$ as a majorant function for the mixed modulus of smoothness of order l of functions $f \in L_q$ instead of the standard function t^r and obtained the estimates of best approximations of classes H_q^{Ω} with some special $\Omega(t_1, \ldots, t_d)$. In 1997, Wang heping [18] introduced the Besov classes $B_{p,\theta}^{\Omega}(T^d)$ by means of $\Omega(t)$, i.e., an extension of the Besov classes $S_{q,\theta}^r(T^d)$, which was introduced first by Amanov [19] and gave the asymptotic estimates for Kolmogorov n-widths of the classes under the condition $\Omega(t) = \omega(t_1 \ldots t_d)$, where $\omega(t) \in \Psi_l^*$ (i.e.,univariate function). In [20, 21], Stasyuk and Fedunyk studied the Kolmogorov and the linear widths of $B_{p,\theta}^{\Omega}(T^d)$ for some values of parameters p, q, θ, respectively. In addition, in [22] the author also considered the best m-term approximation on generalized Besov classes and gave the asymptotic estimates for some values parameters p, q, θ. However, the behavior of these approximate characteristics in the Monte Carlo setting is still open. At this point, it is suitable to indicate a fact which, in the author's opinion, is of interest in studying the problems of approximation of the classes $B_{p,\theta}^{\Omega}(T^d)$ in the Monte Carlo setting. In the present paper, we investigated the estimates exact in order for the Kolmogorov and the linear widths in the Monte Carlo setting.

2   Preliminary and Main Result

Let X, Y be Banach spaces. $L(X, Y)$ denotes the set of all bounded linear operators from X to Y. Let S be a continuous(possibly nonlinear) operator from a closed bounded subset X_0 of a Banach space X to a Banach space Y. Here, we assume that $X_0 = B_X$ is the unit ball of X, and S is an operator mapping the data to the exact solution of the problem. We seek to approximate S by mappings of the form $u = \varphi \circ N,$ where

$$N : X_0 \to R^n; \varphi : N(X_0) \to Y.$$

N and φ describe a numerical method. $\varphi(N(f))$ is the outcome of the numerical operations performed on $N(f)$ in order to obtain an approximation to $S(f)$. According to the properties of N and φ, we pay our attention to the following classes of methods.

For fixed $k \in \mathbb{N}$, a rule $u : X_0 \to Y$ of the form $u = \varphi \circ N$ is said to be a Kolmogorov method,if the information operator N is an arbitrary mapping from X_0 to R^k and φ extends to a linear mapping from R^k to Y and a linear method, if the information operator N is the restriction of a continuous linear mapping from X to R^k and φ extends to a linear mapping from R^k to Y.

Let $D_k(X_0,Y), A_k(X_0,Y)$ denote the sets of all Kolmogorov, linear methods which have cardinality equal to k, and put

$$D^n(X_0,Y) := \bigcup_{k=0}^{n} D_k(X_0,Y); \mathfrak{A}^n(X_0,Y) := \bigcup_{k=0}^{n} A_k(X_0,Y),$$

such that

$$D(X_0,Y) := \bigcup_{n\in N} D^n(X_0,Y); \mathfrak{A}(X_0,Y) := \bigcup_{n\in N} \mathfrak{A}^n(X_0,Y)$$

give rise to the respective classes of Kolmogorov and linear methods. Note that we will denote by $\mathfrak{M}(X_0,Y)$ any of the classes of Kolmogorov and linear methods in this paper.

Now we pass to the randomized setting, or Monte Carlo methods. As compared to deterministic procedures, the randomized methods, and hence also the approximation results, depend on chance, or on a random parameter. We assume that both X_0 and Y are equipped with their respective Borel σ-algebras $B(X_0)$ and $B(Y)$, i.e., the σ-algebras generated by the open sets.

Definition 1. Given a class of methods $\mathfrak{M}(X_0,Y)$, a triple $P_{\mathfrak{M}}([\Omega,F,P],u,k)$ is called an $\mathfrak{M}$-Monte Carlo method, if

(1) $[\Omega,F, P]$ is a probability space.
(2) $u:\Omega \to \mathfrak{M}(X_0,Y)$ is such that the mapping $\Phi: X_0\times\Omega \to Y$, defined by

$$\Phi(f,\omega) := (u(\omega))(f), f \in X_0, \omega \in \Omega,$$

is product measurable into Y and the set $\{(u(\omega))(f), f\in X_0, \omega\in\Omega\}$ is a separable subset in Y.
(3) The cardinality function $k : \Omega \to N$ is a measurable natural number, for which

$$u_\omega := u(\omega) \in \mathfrak{M}^{k(\omega)}(X_0,Y), \omega \in \Omega.$$

The Monte Carlo error is defined as

$$e(S,P_{\mathfrak{M}}) := \sup\{(\int_\Omega \| S(f) - u_\omega(f) \|_Y^2 dP(\omega))^{1/2}, f \in X_0\}.$$

The cardinality of a Monte Carlo method $P_{\mathfrak{M}}$ is defined through the cardinality function k as

$$\text{MC-card}(P_{\mathfrak{M}}) := \int_\Omega k(\omega)dP(\omega).$$

The n-th Monte Carlo error is defined as

$$e_n^{MC}(S,\mathfrak{M},X,Y) := \inf\{e(S,P_{\mathfrak{M}}), \ \text{MC-card}(P_{\mathfrak{M}}) \leq n-1\}.$$

If we take the specific class of methods as $\mathfrak{m}$ in the Monte Carlo setting, we can obtain the following pseudo-s-scales, respectively

$$d_n^{MC}(S,X,Y) := e_n^{MC}(S,D,X,Y); a_n^{MC}(S,X,Y) := e_n^{MC}(S,\mathfrak{A},X,Y).$$

Let R^d be the Euclidean space with dimension d. Denote by $L_q(T^d)$, $1 \leq q \leq \infty$, the Lebesgue space of q-th powers integrable functions defined on the d-dimensional

torus $T^d := [0, 2\pi)^d$, which are 2π-periodic with respect to each variable with the usual norm $\| \cdot \|_q$.

In what follows, we assume that functions $f(x)$ belong to the space

$$L_q^0(T^d) = \{ f : f \in L_q(T^d), \int_{-\pi}^{\pi} f(x)dx_j = 0, j = 1, \ldots, d \}.$$

For $f \in L_q^0(T^d)$, we set

$$\Omega^l(f,t)_q := \sup_{|h| \leq t} \| \Delta_h^l f(x) \|_{q,}$$

where $l \in Z_+$ is a fixed positive integer, $t = (t_1, \ldots, t_d) \geq 0$ (i.e., $t_j \geq 0$, $j = 1, \ldots, d$), $h = (h_1, \ldots, h_d)$, $|h| = (|h_1|, \ldots, |h_d|)$, and $|h| \leq t$ means $|h_j| \leq t_j$, $j = 1, \ldots, d$. At last,

$$\Delta_h^l f(x) := \Delta_{h_d,d}^l (\Delta_{h_{d-1},d-1}^l \cdots (\Delta_{h_1,1}^l f(x)) \cdots),$$

where

$$\Delta_{h_i,i}^l f(x) = \sum_{j=0}^l (-1)^{l-j} \binom{l}{j} f(x_1, \ldots, x_{i-1}, x_i + jh_i, x_{i+1}, \ldots, x_d), i = 1, \ldots, d.$$

As we know, $\Omega^l(f,t)_q$ is the order l modulus of smoothness in $L_q(T^d)$ norm (of mixed type). In order to give the definition of the generalized Besov spaces $B_{p,\theta}^\Omega(T^d)$, we need the following some definitions given by Wang heping in [18].

Definition 2. Let $\phi : R_+^d \to R_+ = [0, \infty)$ be a non-negative function defined on $R_+^d = \{ (x_1, \ldots, x_d) \mid x_j \geq 0, j = 1, \ldots, d \}$. We say that $\phi(t) \in \Phi_l^*$ if it satisfies

(1) $\phi(0) = 0, \phi(t) > 0$ for any $t \in R_+^d, t > 0$ (i.e., $t_j > 0$, $j = 1, \ldots, d$);

(2) $\phi(t)$ is continuous;

(3) $\phi(t)$ is almost increasing, i.e., for any two points $t, \tau \in R_+^d$ and $0 \leq t \leq \tau$ (i.e., $0 \leq t_j \leq \tau_j, j = 1, \ldots, d$), we have $\phi(t) \leq C\phi(\tau)$, where $C \geq 1$ is a constant independent of t;

(4) for any $n := (n_1, \ldots, n_d) \in Z_+^d$

$$\phi(n_1 t_1, \ldots, n_d t_d) \leq C \left(\prod_{j=1}^d n_j \right)^l \phi(t_1, \ldots, t_d),$$

where $l \geq 1$ is a fixed positive integer and $C > 0$ is a constant independent of n and t.

Definition 3. Let $\phi(t)$ be a non-negative function defined on R_+^d which satisfies conditions (1), (2) in Definition 2. We say that $\phi(t) \in S^*$ provided that there exists a vector $\alpha = (\alpha_1, \ldots, \alpha_d) > 0$ such that $\phi(t)t^{-\alpha}$ is almost increasing.

It is easy to see that in this definition we can always assume $0 < \alpha < 1$ (i.e., $0 < \alpha_j < 1, j = 1, \ldots, d$) without loss of generality. Throughout this paper, the capital letter C has different values in different places.

Definition 4. Let $\phi(t)$ be a non-negative function defined on R_+^d satisfying (1),(2) in Definition 2. We say that $\phi(t) \in S_l^*$ if there exist $\gamma = (\gamma_1, \ldots, \gamma_d)$ such that $0 < \gamma_j < l, j = 1, \ldots, d$ and a constant $C > 0$ such that for any two points $0 < t \le \tau$ it always holds

$$\phi(t)t^{\gamma - l \cdot 1} \ge C\phi(\tau)\tau^{\gamma - l \cdot 1}.$$

Denote $\Psi_l^* = \Psi^* = \Psi_l^* \cap S^* \cap S_l^*$. The generalized Besov spaces $B_{p,\theta}^{\Omega}(T^d)$ are defined as follows. Let $e_d := \{1, \ldots, d\}, e \subset e_d$. If $e = \{j_1, \ldots, j_m\}, j_1 < \ldots < j_m,$ then we write $t^e := (t_{j_1}, \ldots, t_{j_m}), (t^e, 1^{\hat{e}}) := (\bar{t}_1, \ldots, \bar{t}_d)$, where $\bar{t}_i = t_i$ for $i \in e$, $\bar{t}_i = 1$ for $i \in \hat{e} = e_d \setminus e$.

Definition 5. For $\Omega(t) \in \Psi_l^*$, we write $f \in B_{p,\theta}^{\Omega}(T^d)$ if it satisfies

(1) $f \in L_p^0(T^d)$;

(2) for any non-empty $e \subset e_d$,

$$\left\{ \int_0^{2\pi} \cdots \int_0^{2\pi} \left(\frac{\Omega^{l^e}(f, t^e)_p}{\Omega(t^e, 1^{\hat{e}})} \right)^{\theta} \prod_{j \in e} \frac{dt_j}{t_j} \right\}^{1/\theta} < \infty, 1 \le \theta < \infty,$$

and

$$\sup_{t^e > 0} \frac{\Omega^{l^e}(f, t^e)_p}{\Omega(t^e, 1^{\hat{e}})} < \infty, \theta = \infty,$$

where

$$\Omega^{l^e}(f, t^e)_p := \sup_{|h^e| \le t^e} \| \Delta_{h^e}^{l^e}(f, x) \|_p, h^e := (h_{j_1}, \ldots, h_{j_m}),$$

$$\Delta_{h^e}^{l^e}(f, x) = \Delta_{h_{j_m}, j_m}^{l} (\Delta_{h_{j_{m-1}}, j_{m-1}}^{l} \cdots \Delta_{h_{j_1}, j_1}^{l} f(\ldots, x_{j_1}, \ldots, x_{j_m}, \ldots) \ldots).$$

We define

$$\| f \|_{B_{p,\theta}^{\Omega}(T^d)} := \| f \|_p + \sum_{e \subset e_d} \left\{ \int_0^{2\pi} \int_0^{2\pi} \left(\sup_{t^e > 0} \frac{\Omega^{l^e}(f, t^e)_p}{\Omega(t^e, 1^{\hat{e}})} < \infty, \theta = \infty, \right)^{\theta} \prod_{j \in e} \frac{dt_j}{t_j} \right\}^{1/\theta}, 1 \le \theta < \infty,$$

and

$$\| f \|_{B_{p,\theta}^{\Omega}(T^d)} := \| f \|_p + \sum_{e \subset e_d} \sup_{t^e > 0} \frac{\Omega^{l^e}(f, t^e)_p}{\Omega(t^e, 1^{\hat{e}})} < \infty, \theta = \infty.$$

It was not difficult to verify that the generalized Besov spaces $B_{p,\theta}^{\Omega}(T^d)$ with the above norm are complete. In this paper, we mainly considered the case $\Omega(t) = \omega(t_1 \ldots t_d)$ where $\omega(t) \in \Psi_l^*$ for some α. For convenience, we suppressed the domain T^d in the notation below.

In this paper, we used the notations $\ll$ and $\sim$. For two sequence $\{a_n\}_{n \in N}$ and $\{b_n\}_{n \in N}$ of positive real numbers, we wrote $a_n \ll b_n$ provided that $a_n \le c b_n$ for certain $c > 0$. If furthermore, also $b_n \ll a_n$, then we wrote $a_n \sim b_n$.

Now we are in a position to state the main result of this paper.

Theorem 1. Let $\Omega(t) = \omega(t_1 \ldots t_d)$ where $\omega(t) \in \Psi_l^*$ for some α. Then for any natural numbers M and n such that $M \sim 2^n n^{d-1}$, we have

$$d_M^{MC}(I, B_{p,\theta}^{\Omega}, L_q) \sim a_M^{MC}(I, B_{p,\theta}^{\Omega}, L_q) \sim$$

$$\sim \begin{cases} \omega(2^{-n}) n^{(d-1)(1/2-1/\theta)}, & 1 < q \le 2 < p < \infty, 2 \le \theta \le \infty, \alpha > 0; \\ \omega(2^{-n}) n^{(d-1)(1/2-1/\theta)}, & 2 < q \le p < \infty, 2 \le \theta \le \infty, \alpha > 0; \\ \omega(2^{-n}) 2^{n(1/p-1/q)}, & 1 < p \le q \le 2, 1 \le \theta \le q, \alpha > 1/p - 1/q; \\ \omega(2^{-n}) 2^{n(1/p-1/2)} & 1 < p \le 2 \le q < \infty, 1 \le \theta \le 2, \alpha > 1/p; \\ \omega(2^{-n}) n^{(d-1)(1/2-1/\theta)}, & 2 \le p \le q < \infty, 2 \le \theta \le \infty, \alpha > 1/2. \end{cases}$$

For the proof of Theorm 1, by Maiorov's discretization technique, we can obtain the main result along the same line as in the work by Fang and the author [11]. Here we omit the its details. Comparing Theorem 1 with the deterministic corresponding approximation characters obtained by Wang [18], Stasyuk[20] and Fedunyk[21], we can observe that for linear width Monte Carlo methods lead to considerably better rates than deterministic methods for $p < q$ and $2 \le q < \infty$.

References

1. Bakhvalov, N.S.: On the approximate computation of multiple integrals. Vestnik Moskov Univ.Ser. Mat. Mekh. Astr. Fiz. Khim 4, 3–18 (1959)
2. Traub, J.F., Wasilkowski, G.W., Woźniakowski, H.: Information-based Complexity. Academic Press, New York (1988)
3. Fang, G.S., Ye, P.X.: Integration Error for Multivariate Functions From Anisotropic Classes. J. Complexity 19, 610–627 (2003)
4. Fang, G.S., Ye, P.X.: Complexity of deterministic and randomized methods for multivariate integration problem for the class $H_p^{\Lambda}(I^d)$. IMA Journal of Numerical Analysis 25, 473–485 (2005)
5. Heinrich, S.: Lower Bounds for the Complexity of Monte Carlo Function Approximation. J. Complexity 8, 277–300 (1992)

6. Heinrich, S.: Random approximation in numerical analysis. In: Bierstedt, K.D., Bonet, J., Horvath, J., et al. (eds.) Functional Analysis: Proceedings of the Essen Conference. Lect. Notes in Pure and Appl. Math, vol. 150, pp. 123–171. Chapman and Hall/CRC, Boca Raton (1994)
7. Heinrich, S.: Monte Carlo approximation of weakly singular integral operators. J. Complexity 22, 192–219 (2006)
8. Math′e, P.: Random approximation of Sobolev embedding. J. Complexity 7, 261–281 (1991)
9. Math′e, P.: Approximation Theory of Stochastic Numerical Methods. Habilitationsschrift, Fachbereich Mathematik, Freie Universit¨at Berlin (1994)
10. Novak, E.: Deterministic and stochastic error bounds in numerical analysis. Lecture Notes in Mathematics, vol. 1349. Springer, Berlin (1988)
11. Fang, G.S., Duan, L.Q.: The complexity of function approximation on Sobolev spaces with bounded mixed derivative by linear Monte Carlo methods. J. Complexity 24, 398–409 (2008)
12. Fang, G.S., Duan, L.Q.: The information-based complexity of approximation problem by adaptive-Monte Carlo methods. Science in China A: Mathematics 51, 1679–1689 (2008)
13. Nikolskii, S.M.: Approximation of Functions of Several Variables and Imbeddings Theorems. Springer, Berlin (1975)
14. Romanyuk, A.S.: On estimate of the Kolmogorov widths of the classes $B_{p,\theta}^r$ in the space Lq. Ukr.Math. J. 53, 1189–1196 (2001)
15. Romanyuk, A.S.: Linear widths of the Besov classes of periodic functions of many variables.II. Ukr.Math. J. 53, 965–977 (2001)
16. Romanyuk, A.S.: Approximation of classes $B_{p,\theta}^r$ by linear methods and best approximations. Ukr.Math. J. 54, 825–838 (2002)
17. Pustovoitov, N.N.: Representation and approximation of multivariate periodic functions with a given mixed modulus of smoothness. Analysis Math. 20, 35–48 (1994)
18. Sun, Y.S., Wang, H.P.: Representation and approximation of multivariate periodic functions with bounded mixed moduli of smoothness. In: Proc. Steklov Inst. Math., vol. 219, pp. 350–371 (1997)
19. Amanov, T.I.: Representation and imbedding theorems for the function spaces $S_{p,\theta}^r B(R^n), S_{p,\theta}^{*r} B(0 \le x_j \le 2\pi, j = 1, \ldots, n)$. Trudy Mat. Inst. Akad. Nauk SSSR 77, 5–34 (1965)
20. Stasyuk, S.A.: Best approximations and Kolmogorov and trigonometric widths of the classes $B_{p,\theta}^\Omega (T^d)$ of periodic functions of many variables. Ukr. Math. J. 56, 1849–1863 (2004)
21. Fedunyk, O.V.: Linear widths of the classes $B_{p,\theta}^\Omega (T^d)$ of periodic functions of many variables in the space Lq. Ukr. Math. J. 58, 103–117 (2006)
22. Duan, L.Q.: The best m-term approximations on generalized Besov classes $MB_{q,\theta}^\Omega$ with regard to orthogonal dictionaries. J. Approx. Theory 162, 1964–1981 (2010)
23. Pinkus, A.: N-widths in Approximation Theory. Springer, New York (1985)

Initial Boundary Value Problem
for a Generalized Zakharov Equations[*]

Shujun You and Xiaoqi Ning

Department of Mathematics, Huaihua University,
Huaihua 418008, Hunan, P.R. China
`ysj980@yahoo.com.cn, nxq06@yahoo.cn`

Abstract. In this paper the authors consider the existence of the solution to the initial boundary value problem for a class of generalized Zakharov equations and prove the global existence of the generalized solution to the problem by a priori integral estimates and Galerkin method.

Keywords: Zakharov equations, generalized Zakharov equations, Initial boundary value problem, Generalized solution.

1 Introduction

The Zakharov equations, derived by Zakharov in 1972 [1], describes the propagation of Langmuir waves in an unmagnetized plasma. The usual Zakharov system defined in space time $\mathbb{R}^{d+1}$ is given by

$$iE_t + \Delta E = nE, \tag{1.1}$$

$$n_{tt} - \Delta n = \Delta \mid E \mid^2, \tag{1.2}$$

where $E : \mathbb{R}^{1+d} \to \mathbb{C}^d$ is the slowly varying amplitude of the high-frequency electric field, and $n : \mathbb{R}^{1+d} \to \mathbb{R}$ denotes the fluctuation of the ion-density from its equilibrium.

In the past decades, the Zakharov system was studied by many authors [2-7]. In [4], B. Guo, J. Zhang and X. Pu established globally in time existence and uniqueness of smooth solution for a generalized Zakharov equation in two dimensional case for small initial data, and proved global existence of smooth solution in one spatial dimension without any small assumption for initial data. Linares F. and Matheus C.[5] obtained global well-posedness results for the initial-value problem associated to the ID Zakharov-Rubenchik system, and the results are sharp in some situations by proving ill-posedness results otherwise. In [6], Linares F. and Saut JC. proved that the Cauchy problem for the three-dimensional Zakharov-Kuznetsov equation is locally well-posed for data in $H^s(\mathbb{R}^3), s > \frac{9}{8}$. If $0 < p < 4$, the existence and uniqueness of the

global classical solution for a generalized Zakharov equation were obtained in [7]. The nonlinear Schrodinger limit of the Zakharov equation was discussed in [8-9].

In this paper, we are interested in studying the following generalized Zakharov systems.

$$iE_t + E_{xx} - nEg'(|x|^2) = 0, \tag{1.3}$$

$$n_t + \varphi_{xx} = 0, \quad x \in (0, a) \tag{1.4}$$

$$\varphi_t + \beta\varphi + n + g(|E|^2) = 0, \quad \beta \geq 0 \tag{1.5}$$

$$E_x - \alpha_1 E|_{x=0} = 0, E_x + \alpha_2 E|_{x=a} = 0, \quad \alpha_1, \alpha_2 \geq 0, t \geq 0 \tag{1.6}$$

$$n|_{x=0} = n|_{x=a} = \varphi|_{x=0} = \varphi|_{x=a} = 0, \quad t \geq 0 \tag{1.7}$$

$$E|_{t=0} = E_0(x), n|_{t=0} = n_0(x), \varphi|_{t=0} = \varphi_0(x), \quad x \in (0, a) \tag{1.8}$$

We mainly consider the existence of the Generalized solution to the system.

For the sake of convenience of the following contexts, we set some notations. For $1 \leq q \leq \infty$, we denote $L^q(0, a)$ the space of all q times integrable functions in $(0, a)$ equipped with norm $\|\cdot\|_{L^q(0,a)}$ or simply $\|\cdot\|_{L^q}$ and $H^{s,p}(0, a)$ the Sobolev space with norm $\|\cdot\|_{H^{s,p}(0,a)}$. If $p = 2$, we write $H^s(0, a)$ instead of $H^{s,2}(0, a)$. Let $(f, g) = \int_0^a f(x) \cdot \overline{g(x)} dx$, where $\overline{g(x)}$ denotes the complex conjugate function of $g(x)$. General constant C depends on initial value data. Now we state the main results of the paper.

Theorem 1. Suppose that

(1) $g(s) \in C^1, s \in [0, \infty)$, and $|g(s)| \leq As^{\frac{1-\delta}{2} - \frac{\delta}{2}} + B$. $A, B > 0$, $\delta > 0$;

(2) $E_0(x) \in H^1(0, a), n_0(x) \in L^2(0, a), \varphi_0(x) \in H^1(0, a)$.

Then there exists a global generalized solution of the initial boundary value problem (1.3)-(1.8),

$$E(x, t) \in L^\infty(0, T; H^1(0, a)) \bigcap W_\infty^1(0, T; H^{-1}(0, a)) \bigcap C^{(\frac{1}{2}, \frac{1}{4})}(Q)$$

$$n(x, t) \in L^\infty(0, T; L^2(0, a)) \bigcap W_\infty^1(0, T; H^{-1}(0, a))$$

$$\varphi(x, t) \in L^\infty(0, T; H^1(0, a)) \bigcap W_\infty^1(0, T; L^2(0, a)) \bigcap C^{(\frac{1}{2}, \frac{1}{2})}(Q)$$

The paper is organized as follows: In section 2, we make a priori estimates of the problem (1.3)-(1.8). In section 3, we obtain the existence of the global Generalized solution of the problem (1.3)-(1.8) by Galerkin method.

2   A Priori Estimations of Problem (1.3)-(1.8)

Lemma 1. Suppose that $E_0(x) \in L^2(0, a), g(s) \in C^1$. Then forthe solution of problem (1.3)-(1.8) we have

$$\| \ E(\cdot,t)\|^2_{L^2(0,a)} = \| \ E_0(x)\|^2_{L^2(0,a)} .$$

Proof. Taking the inner product of (1.3) and E, it follows that

$$(iE_t + E_{xx} - nEg'(|E|^2), E) = 0, \tag{2.1}$$

since

$$\operatorname{Im}(iE_t, E) = \frac{1}{2}\frac{d}{dt}\| \ E\|^2_{L^2} , \quad \operatorname{Im}(-nEg'(|E|^2), E) = 0 ,$$

$$\operatorname{Im}(E_{xx}, E) = \operatorname{Im}\left(E_x \overline{E} \,|_0^a - \int_0^a E_x \overline{E}_x dx \right)$$

$$= \operatorname{Im}\left(E_x(a,t)\overline{E}(a,t) - E_x(0,t)\overline{E}(0,t) \right)$$

$$= \operatorname{Im}\left(-\alpha_2 \,|\, E(a,t)|^2 - \alpha_1 \,|\, E(0,t)|^2 \right) = 0$$

hence from (2.1) we get

$$\frac{d}{dt}\| \ E(\cdot,t)\|^2_{L^2} = 0 ,$$

i.e.

$$|\ E(\cdot,t)\|^2_{L^2} = \| \ E_0(x)\|^2_{L^2} .$$

Lemma 2. (Sobolev's estimations) Assume that $u \in L^q(\Omega)$, $D^m u \in L^r(\Omega)$, $1 \le q$, $r \le \infty$, $0 \le j \le m$, $\Omega \subseteq \mathbf{R}^n$, we have the estimations

$$|\ D^j u\|_{L^p(\Omega)} \le C\| \ D^m u\|^\alpha_{L^r(\Omega)}\| \ u\|^{1-\alpha}_{L^q(\Omega)} ,$$

Where C is a positive constant, $0 \le \frac{j}{m} \le \alpha \le 1$,

$$\frac{1}{p} = \frac{j}{n} + \alpha\left(\frac{1}{r} - \frac{m}{n}\right) + (1-\alpha)\frac{1}{q} .$$

Lemma 3. Suppose that the conditions of Lemma 1 are satisfied, and assume that

(1) $|g(s)| \le As^{\frac{3}{2}-\frac{\delta}{2}} + B, \quad A, B > 0, \delta > 0$.
(2) $E_0(x) \in H^1(0,a)$, $n_0(x) \in L^2(0,a)$, $\varphi_0(x) \in H^1(0,a)$.

Then we have

$$\| \ E\|_{H^1(0,a)\times L^\infty(0,T)} + \| \ n\|_{L^2(0,a)\times L^\infty(0,T)} + \| \ \varphi\|_{H^1(0,a)\times L^\infty(0,T)} \le C_1.$$

Proof. Taking the inner products of (1.3) and E_t,
it follows that

$$\left(iE_t + E_{xx} - nEg'(|E|^2), E_t\right) = 0 \tag{2.2}$$

Since

$$\operatorname{Re}\left(iE_t, \ E_t\right) = 0 ,$$

$$\mathrm{Re}(E_{xx}, E_t) = \mathrm{Re}\left(E_x\bar{E}_t\mid_0^a - \int_0^a E_x\bar{E}_{xt}dx\right)$$

$$= \mathrm{Re}\left(E_x(a,t)\bar{E}_t(a,t) - E_x(0,t)\bar{E}_t(0,t)\right) - \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\parallel E_x\parallel_{L^2}^2$$

$$= -\frac{1}{2}\left(\alpha_2\frac{\mathrm{d}}{\mathrm{d}t}\mid E(a,t)\mid^2 + \alpha_1\mid E(0,t)\mid^2 + \frac{\mathrm{d}}{\mathrm{d}t}\parallel E_x\parallel_{L^2}^2\right)$$

$$\mathrm{Re}(-nEg'(\mid E\mid^2), E_t) = -\frac{1}{2}\int_0^a g'(\mid E\mid^2)n\mid E\mid_t^2\,dx = -\frac{1}{2}\int_0^a n\frac{\mathrm{d}}{\mathrm{d}t}g(\mid E\mid^2)dx$$

$$= -\frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\int_0^a ng(\mid E\mid^2)dx + \frac{1}{2}\int_0^a n_t g(\mid E\mid^2)dx$$

$$= -\frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\int_0^a ng(\mid E\mid^2)dx + \frac{1}{2}\int_0^a n_t(-\varphi_t - \beta\varphi - n)dx$$

$$= -\frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\int_0^a ng(\mid E\mid^2)dx + \frac{1}{2}\int_0^a \varphi_{xx}\varphi_t dx + \frac{\beta}{2}\int_0^a \varphi_{xx}\varphi dx - \frac{1}{2}\int_0^a n_t n\,dx$$

$$= -\frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\int_0^a ng(\mid E\mid^2)dx - \frac{1}{4}\frac{\mathrm{d}}{\mathrm{d}t}\parallel \varphi_x\parallel_{L^2}^2 - \frac{\beta}{4}\parallel \varphi_x\parallel_{L^2}^2 - \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\parallel n\parallel_{L^2}^2$$

then we deduce from (2.2)

$$\frac{\mathrm{d}}{\mathrm{d}t}\left[\alpha_2\mid E(a,t)\mid^2 + \alpha_1\mid E(0,t)\mid^2 + \parallel E_x\parallel_{L^2}^2 + \int_0^a ng(\mid E\mid^2)dx + \frac{1}{2}\parallel \varphi_x\parallel_{L^2}^2 + \parallel n\parallel_{L^2}^2\right] + \frac{\beta}{2}\parallel \varphi_x\parallel_{L^2}^2 = 0. \qquad (2.3)$$

Letting

$$w(t) = \alpha_2\mid E(a,t)\mid^2 + \alpha_1\mid E(0,t)\mid^2 + \parallel E_x\parallel_{L^2}^2 + \int_0^a ng(\mid E\mid^2)dx + \frac{1}{2}\parallel \varphi_x\parallel_{L^2}^2 + \parallel n\parallel_{L^2}^2,$$

and noticing (2.3) we obtain

$$w(t) \le w(0). \qquad (2.4)$$

On the other hand

$$\left|\int_0^a ng(\mid E\mid^2)dx\right| \le \frac{1}{4}\parallel n\parallel_{L^2}^2 + \left\|g(\mid E\mid^2)\right\|$$

$$\le \frac{1}{4}\parallel n\parallel_{L^2}^2 + 2A\parallel E\parallel_{\frac{6-2\delta}{6-2\delta}}^{\frac{6-2\delta}{6-2\delta}} + 2B^2a$$

$$\le \frac{1}{4}\parallel n\parallel_{L^2}^2 + \frac{1}{2}\parallel E_x\parallel_{L^2}^2 + C.$$

Hence from (2.4) we get

$$\parallel E_x\parallel_{L^2}^2 + \parallel \varphi_x\parallel_{L^2}^2 + \parallel n\parallel_{L^2}^2 \le \mathrm{const.}$$

Taking the inner products of (1.5) and φ, it follows that

$$\left(\varphi_t + \beta\varphi + n + g(\mid E\mid^2), \varphi\right) = 0. \qquad (2.5)$$

Since

$$(\varphi_t, \varphi) = \frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\|\varphi\|_{L^2}^2, \quad (\beta\varphi,\varphi) = \beta\|\varphi\|_{L^2}^2,$$

$$\left|(n,\varphi)\right| \leq \|n\|_{L^2}\|\varphi\|_{L^2} \leq (\beta+1)\|\varphi\|_{L^2}^2 + C\|n\|_{L^2}^2 \leq (\beta+1)\|\varphi\|_{L^2}^2 + C,$$

$$\left|\left(g(|E|^2),\varphi\right)\right| \leq \left\|g(|E|^2)\right\|_{L^2}\|\varphi\|_{L^2} \leq \|\varphi\|_{L^2}^2 + C.$$

thus we deduce from (2.5)

$$\frac{\mathrm{d}}{\mathrm{d}t}\|\varphi\|_{L^2}^2 \leq C\|\varphi\|_{L^2}^2 + 1$$

By using Gronwall inequality we obtain

$$\|\varphi\|_{L^2}^2 \leq \text{const.}$$

Lemma 4. Suppose that the conditions of Lemma 3 are satisfied. Then we have

$$\|E\|_{L^\infty(0,T;H^{-1}(0,a))} + \|n\|_{L^\infty(0,T;H^{-1}(0,a))} + \|\varphi\|_{L^\infty(0,T;L^2(0,a))} \leq C_2,$$

$$\|E\|_{C^{(\frac{1}{2},\frac{1}{4})}(Q)} + \|\varphi\|_{C^{(\frac{1}{2},\frac{1}{2})}(Q)} \leq C_3,$$

where $Q = (0,T)\times(0,a)$.

Proof. Taking the inner products of (1.3)-(1.5) and v, it follows that

$$\left(iE_t + E_{xx} - nEg'(|x|^2),v\right) = 0, \tag{2.6}$$

$$\left(n_t + \varphi_{xx}v\right) = 0, \tag{2.7}$$

$$\left(\varphi_t + \beta\varphi + n + g(|E|^2),v\right) = 0. \tag{2.8}$$

Where $\forall v \in H_0^1(0,a)$.

We obtain from (2.6)

$$\begin{aligned}\left|(E_t,v)\right| &\leq \left|(E_x,v_x)\right| + \left|\left(nEg'(|E|^2),v\right)\right| \\ &\leq \|E_x\|_{L^2}\|v_x\|_{L^2} + \left\|g'(|E|^2)\right\|_{L^\infty}\|n\|_{L^2}\|v\|_{L^2} \\ &\leq C\|v\|_{H_0^1(0,a)}.\end{aligned} \tag{2.9}$$

From (2.7), there is

$$\left|(n_t,v)\right| = \left|(\varphi_{xx},v)\right| = \left|(\varphi_x,v_x)\right| \leq \|\varphi_x\|_{L^2}\|v_x\|_{L^2} \leq \|v\|_{H_0^1(0,a)}. \tag{2.10}$$

We deduce from (2.8)

$$\begin{aligned}\left|(\varphi_t,v)\right| &\leq \left|(\beta\varphi,v)\right| + \left|(n,v)\right| + \left|\left(g(|E|^2),v\right)\right| \\ &\leq \beta\|\varphi\|_{L^2}\|v\|_{L^2} + \|n\|_{L^2}\|v\|_{L^2} + \left\|g(|E|^2)\right\|_{L^2}\|v\|_{L^2} \\ &\leq C\|v\|_{L^2}.\end{aligned} \tag{2.11}$$

Therefore, from (2.9),(2.10) and (2.11), it follows that

$$\| E\|_{L^\infty(0,T;H^{-1}(0,a))} + \| n\|_{L^\infty(0,T;H^{-1}(0,a))} + \| \varphi\|_{L^\infty(0,T;L^2(0,a))} \le C_2.$$

Let

$$w(x,t) = \int_0^a E(\xi,t)\mathrm{d}x,$$

for(1.3),we have

$$\| w\|_{L^2} \le \| E_x(\cdot,t)\|_{L^2} + \| E_x(0,t)\|_{L^2} + \| g'(|E|^2)E\|_{L^\infty} \mathrm{d} \| n\|_{L^2}$$

$$\le C + \sqrt{a}\alpha_1 | E(0,t)|$$

$$\le C + C \| E_x\|_{L^2} \le \text{Const.}$$

From $w_{xx} = E_x$,we have that $w(x,t)$ is bounded uniformly in $L^\infty(0,T;H^2(0,a)) \cap W_\infty^{(1)}(0,T;L^2(0,a))$. Hence

$$\left| E(x,t_2) - E(x,t_1)\right| = | w_x(x,t_2) - w_x(x,t_1) |$$

$$\le C \| w(x,t_2) - w(x,t_1)\|_{L^2}^{\frac{1}{4}} \| w(x,t_2) - w(x,t_1)\|_{H^2}^{\frac{3}{4}}$$

$$\le C | t_2 - t_1 |^{\frac{1}{4}} \sup_{0\le t\le T}\| w_t(\cdot,t)\|_{L^2}^{\frac{1}{4}} \sup_{0\le t\le T}\| w(\cdot,t)\|_{H^2}^{\frac{3}{4}} \qquad (2.12)$$

$$\le C | t_2 - t_1 |^{\frac{1}{4}}$$

On the other hand, if $x_2 \ge x_1$, we get

$$| E(x_2,t) - E(x_1,t) | = \left| \int_{x_1}^{x_2} E_x(x,t)\mathrm{d}x \right|$$

$$\le \left(\int_{x_1}^{x_2} |E_x(x,t)|^2 \, \mathrm{d}x \right)^{\frac{1}{2}} \left(\int_{x_1}^{x_2} 1\mathrm{d}x \right)^{\frac{1}{2}}$$

$$\le \| E_x(x,t)\|_{L^2} | x_2 - x_1 |^{\frac{1}{2}} \qquad (2.13)$$

$$\le C | x_2 - x_1 |^{\frac{1}{2}},$$

and the same result as above are valid for $x_2 < x_1$.

Then we deduce from (2.12) and (2.13)

$$E(x,t) \in C^{(\frac{1}{2},\frac{1}{4})}(Q).$$

Moreover,

$$| \varphi(x,t_2) - \varphi(x,t_1) | \le C \| \varphi(x,t_2) - \varphi(x,t_1)\|_{H'(0,a)}^{\frac{1}{2}} \| \varphi(x,t_2) - \varphi(x,t_1)\|_{L^2}^{\frac{1}{2}} \frac{1}{2}$$

$$\le C \sup_{0\le t\le T}\| \varphi(x,t)\|_{H'}^{\frac{1}{2}} \sup_{0\le t\le T}\| \varphi_t(x,t)\|_{L^2}^{\frac{1}{2}} | t_2 - t_1 |^{\frac{1}{2}} \qquad (2.14)$$

$$\le C | t_2 - t_1 |^{\frac{1}{2}}$$

the same argument used to obtain (2.13) now shows that

$$| \varphi(x_2,t) - \varphi(x_1,t) |= \left| \int_{x_1}^{x_2} \varphi_x(x,t)\mathrm{d}x \right|$$

$$\leq \| \varphi_x \|_{L^2} | x_2 - x_1 |^{\frac{1}{2}} \tag{2.15}$$

$$\leq C | x_2 - x_1 |^{\frac{1}{2}}$$

It follows from (2.14) and (2.15) that

$$\varphi(x,t) \in C^{(\frac{1}{2},\frac{1}{2})}(Q).$$

3 The Existence of Global Generalized Solution for Problem (1.3)-(1.8)

By using Galerkin method and the priori integral estimates in section 2 we have

Theorem 1. Suppose that

(1) $g(s) \in C^1, s \in [0,\infty)$, and $| g(s) |\leq As^{\frac{1-\delta}{2-\frac{\delta}{2}}} + B.A, B > 0, \delta > 0$;

(2) $E_0(x) \in H^1(0,a), n_0(x) \in L^2(0,a), \varphi_0(x) \in H^1(0,a)$.

Then there exists a global generalized solution of the initial boundary value problem (1.3)-(1.8),

$$E(x,t) \in L^\infty(0,T;H^1(0,a)) \bigcap W_\infty^1(0,T;H^{-1}(0,a)) \bigcap C^{(\frac{1}{2},\frac{1}{4})}(Q),$$

$$n(x,t) \in L^\infty(0,T;L^2(0,a)) \bigcap W_\infty^1(0,T;H^{-1}(0,a)),$$

$$\varphi(x,t) \in L^\infty(0,T;H^1(0,a)) \bigcap W_\infty^1(0,T;L^2(0,a)) \bigcap C^{(\frac{1}{2},\frac{1}{2})}(Q).$$

References

1. Zakharov, V.E.: Collapse of Langmuir waves. Sov. Phys. JETP 35, 908–914 (1972)
2. Holmer, J.: Local ill-posedness of the 1D Zakharov system. Electron. J. Differential Equations 24, 1–24 (2007)
3. Pecher, H.: An improved local well-posedness result for the one-dimensional Zakharov system. J. Math. Anal. Appl. 342, 1440–1454 (2008)
4. Guo, B., Zhang, J., Pu, X.: On the existence and uniqueness of smooth solution for a generalized Zakharov equation. J. Math. Anal. Appl. 365, 238–253 (2010)
5. Linares, F., Matheus, C.: Well Posedness for the 1D Zakharov-Rubenchik system. Advances in Differential Equations 14, 261–288 (2009)
6. Linares, F., Saut, J.C.: The Cauchy problem for the 3D Zakharov-Kuznetsov equation. Discrete and Continuous Dynamical Systems 24, 547–565 (2009)
7. You, S.: The posedness of the periodic initial value problem for generalized Zakharov equations. Nonlinear Analysis: Theory, Methods & Applications 71, 3571–3584 (2009)
8. Masmoudi, N., Nakanishi, K.: From the Klein-Gordon-Zakharov system to the nonlinear Schroinger equation. J. Hyperbolic Differ. Equ. 2(4), 975–1008 (2005)
9. Masmoudi, N., Nakanishi, K.: Energy convergence for singular limits of Zakharov type systems. Invent. Math. 172, 535–583 (2008)

Application and Research of Virtual Reality Technique on the Safety of Transportation of Dangerous Goods

Li Qi-Zhong

North China Institute of Science & Technology,
Yanjiao Beijing-East, 101601

Abstract. Transportation of dangerous materials is highly risky and difficult in management. Once accident happens, it would cause great loss in lives and properties, and bring serious social impact. The safety is the lifeline of railways transportation, and human is the most important factor. With the application of computer, information and network technique, it was adopted the means of Virtual Reality（VR）to simulating the work of railway transportation of dangerous materials. This means was provided with the trait as reality, safe, economy and speediness, so it had important practical value.

Keywords: dangerous goods, Railway transportation, Safety, Virtual Reality, simulation.

1　Introduction

We transport dangerous chemicals nearly 160 million tons every year by railway. There are 2187 Dangerous Goods handling stations which include 330 stations for only dangerous goods, 98 stations for only dangerous goods container, 64 stations for only virulent. There are nine categories, more than 8000 kinds of dangerous goods transportation with flammable, explosive, toxic, radioactive, corrosive and other features. We assume the transportation of dangerous chemicals for these enterprises such as petroleum and chemical, military and national defense, aerospace, building materials, medicine, scientific research and education system.

Because the dangerous goods is different from ordinary, it has its own special requirements in equipment and technology management, transport organization, security protection and accident rescue, etc. so the practitioners of dangerous goods transportation management will be needed higher requirements.

Considering the difficulty and dangerous of the actual operation of dangerous goods, we lead virtual reality technology into the transportation of dangerous goods management and the training of its practitioners, it will have a great advantage. We can simulate the dangerous goods by computer, and operate them through the data glove, we can also simulate a dangerous situation to deal with them, and we also use the VR system for training through the distance network. Therefore, it has the characteristics such as less investment, safe and reliable, repeatable by using the VR technology to simulate of transportation of dangerous goods management and training.
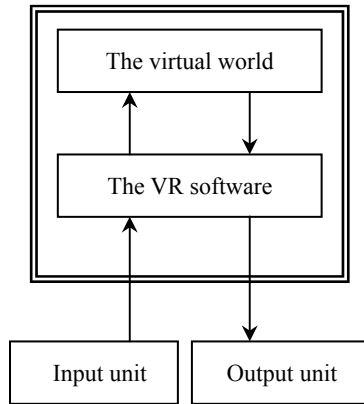
Fig. 1. Constitution of the VR system

2   Brief Introduction of VR

The VR(Virtual Reality) is a high-tech which developed at the end of 1980s, it has collected many essential technologies such as the computer graphics, multimedia technical, the artificial intelligence, the man-machine connection technology, the sensor technology, the highly parallel real-time computation technology, person's behavior study research and so on. It is the newest and ultimate layer of the simulation technology; it is one front science of the world now. [1]

The VR technology's definition may summarize as one kind of artificial simulated environment which produces by the computer, and the environment is the three-dimensional space which constitutes by the computer, or establishes verisimilitude "the simulated environment" in the computer by realistic environment. It lets the user absorbed in this environment by many kinds of special equipment, and causes the user to produce one kind of feeling of immersing in the simulated environment on the sense of vision, hearing, touch, taste and so many kinds of sense of organs. Compares with the traditional man-machine interactive technology, the VR has three most prominent characteristics: interaction, immersion and conception. And the interaction means the participant achieving the object's operated degree and the natural degree of the feedback of the simulated environment by using special equipment and the humanity's natural skill. The immersion means the real degree of the participant's feeling of existing in the simulated environment just like a protagonist. The conception means the application of VR technology is enables to solve the practical question in the project, the medicine, the military and so on. [2] It maybe makes people get sensitive and rational cognizance from the simulated environment. And it may deepen concept, generate fresh idea and conception, seek, explore and accept the information on its own instead of passive acknowledgment.

A typical VR system mainly includes five constituents: the virtual world, the computer, VR software, the input unit and the output unit (as fig.1 shows). The

approximately process of interacting with the virtual world is: the user firstly activates input device such as data helmet, data glove, and microphone and so on for providing input signal to the computer. Then VR software receives input signal which sends by the tracking device and sensor to explain, updates the database of the simulated environment, adjusts the scene of current simulated environment, and makes the three dimensional picture under this new viewpoint and other information such as sound, touch, feedback of strength and so on to be transmitted immediately for the corresponding output unit such as the helmet monitor, earphone, data glove and so on in order to make the user promptly obtain the simulated effect on many kinds sense of organs.

3 The Research of the Application of VR in the Railway Safe Transportation of Dangerous Goods

3.1 Brief Application of VR

Railway safe transportation of dangerous goods in VR is using current computer technology, information and network technology. By using VR methods, we can simulate and emulate the on-site operations of transportation of dangerous goods. It is based VR, comprehensively use multimedia such as graphics, images, animations and sound to simulate the actual situation. Combined with the remote control technology, people can work by staying away from dangerous workplaces. The system is known as a virtual remote operating system. Through the system, the operator can use the traditional mechanical equipment to operate away from the job site.

3.2 System Architecture

Generally, a virtual remote operating system is divided into four parts: man-machine interface systems, image processing and calibration systems, on-site operating system, virtual simulation system.

The image processing system and the virtual simulation system is the key part of the remote operating system, and it is the main work of the system design. There are many ways to get a virtual three-dimensional image from the current methods which people mastering. For the virtual remote operating system, the key part of image processing and virtual simulation is how to get synchronized with the on-site changes in a virtual environment. Namely, it is a question of solving the communication and control delay of the virtual environment and job-site.

To solve the problem, the system uses the organic integration of "virtual" and "reality" to achieve synchronized results. The specific method is: through the model to establish a framework for virtual simulation environment, using live video images and simulation environment for video integration and synthesis of a virtual simulation environment. The virtual simulation environment will give a real-time feedback to the operator under the control instructions, while the remote operation machinery will have same and Synchronization action under the control instructions, repeating the results of simulation environment, and feedback the results into the virtual environment to reduce the synchronization error.

3.3   The Program of the System Implementation

Virtual remote operating system is not only a complex system but also involve a large number of new technical theories. So it is necessary to emulate the program of the system's design, to research and explore the technical theories, such as virtual environments, remote control, man-machine interface.

According to the characteristics of the railway freight yard, we can determine the composition of virtual simulation system experiment as follows:

(1) Job field. We can produce the model railroad freight yard in proportion. The model consists of sites, buildings, goods, operating machinery, etc. The operating machinery is the focus of the experiment simulation. We select the forklift as the operating machinery, because the forklift is a very typical material of handling machinery, while its movements and actions is relatively simple, and easy to control.

(2) Computer hardware. It include three-dimensional graphics processing system and human-computer interaction devices, such as 3D accelerator card, head-mounted display, space ball, data glove, mouse, keyboard, control and communications interfaces.

(3) Software environment. Use World Toolkit (WTK) as a simulation engine for the whole system, and use Visual C++ to develop the integrated simulation environment and control procedures.

3.4   Establishment of Virtual Simulation Scenarios

3.4.1   Modeling the Operating Mechanical

(1) Geometric mode

From the point of view of the structure is relatively simple and has the typical representation, forklift was a more appropriate operating machinery. The typical forklift consists of four parts: the body, working device, driving device and the power. Working device includes door, forks, tilt cylinders, lifting cylinders, chain pulley blocks and drive devices. The driving devices include chassis, wheels, transmission, etc. When it is working the driving device to complete the function of walking and transportation, the work unit implements the task of handling and stacking. According to the need of simulation and control, simplify the structure of forklift. All kinds of power plants use the motor drive, and set drive motor on the wheels, doors and fork respectively. Through the control of motor, it completes the driving, steering, extract, and stacking and other moves.

We use ordinary three-dimensional modeling software to establish the model of forklift, and transform it into the file format, such as ".wrl" file which can be recognized by the simulation software WTK.

(2) Kinematical model

The body, doors and fork of a forklift compose a chain of movement by the order of succession. The spatial location of each component not only with relate to its own movement, but also to the "dependency" components and the spatial location of the body. In order to describe the interdependence and interaction of the movement relation

of the components, we use the global coordinates, the body coordinates and the possession coordinates to describe the movement of forklift. As shown in Figure 2, its coordinates are: body coordinate system x0y0z0, possessed coordinates x1y1z1 (doors), possessed coordinates x2y2z2 (fork), the global coordinate system xyz.
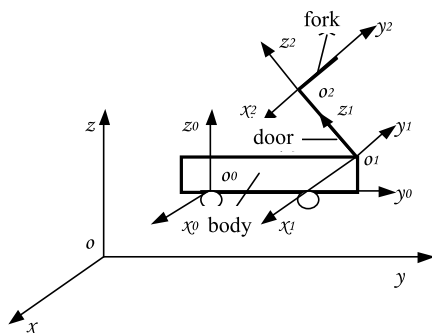
Fig. 2. The coordinate system of forklift model

According to the definition of the coordinate system between the forklift models, combined with the relative motion relationship of components, we can deduce the graphics transformation matrix of components when they are moving. And we can deduce the relationship between the drive motor rotation of wheels, doors, car fork and graphics transform.

3.4.2   Virtual Scene Modeling Based on WTK

(1) Introduction of WTK

WTK (World Toolkit) is a virtual environment application development toolkit which provided by the Sense8 company of the United States. Through a plug-in platform, they provide users with a complete three-dimensional virtual environment for interactive development platform. WTK provides users with more than 1000 library functions which include device drivers and compiled the C language. And the function can be directly called by C/C++ program. At the same time, WTK can provide users with high-level application development interface by the underlying OpenGL graphics functions. In C/C++ language integrated environment, users can easily take WTK as external library and directly embed in their own applications, to develop three-dimensional virtual environment application.

(2) Construction of WTK virtual environment

The way of constructing the virtual environment with WTK is: in C++ software development platform, call WTK related function, use the object's geometric model to composite a scene graph by the relationship between each scene. And add texture and light on the scene and so on. Then they are unified managed by simulation management program and acting under all kinds of operating instructions of users.

WTK organize the virtual environment in accordance with object-oriented, its main classes include: Universe, Geometry, Object, Polygon, Vertex, Path, Sensor, Viewpoint, Light, Node, Portal, Animation and so on. From the class hierarchy view, Universe is the most senior class and its function is equivalent to a container which can accommodate a variety of objects to form a variety of scene.

The virtual environment which created by WTK is constituted by one or more Universe, while the various kinds objects and nodes which provided by WTK is constituted by a certain hierarchy relation. Thus, the focus of virtual environment modeling under WTK platform is how to establish the scene which based on WTK and meet the user's needs. In WTK, the basic unit of the scene is the Node, each scene graph is a collection of a number of points of order, and its structure is equivalent to a top-down inverted trees. The node which constitute a scene graph include: Geometry Node, Light Node, Fog Node, Transform Node, Group Node and so on., they describe the entire virtual environment together.

When we establish the 3D geometry model of the virtual object, we can use the three-dimensional modeling capabilities of WTK. We can also use other three-dimensional modeling software. WTK supports multiple file formats input.

(3) Construction and assembly of the virtual environment scene tree

Railway freight yard scene is composed with fixed objects moving objects. Fixed objects include: freight yard background, terrain, ground buildings and other fixed facilities. Moving objects include: operating machinery (forklifts), the goods to be handling and other operating machinery. Through the WTK organization in the scene and the characteristics of the railway freight yard, we establish the structure of the scene, as shown in Figure 3.
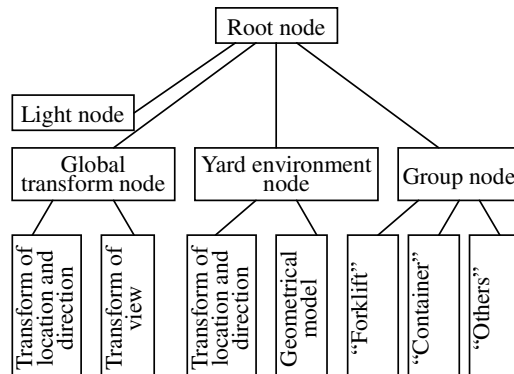

Fig. 3. The virtual simulation scene of railway job field

In the scene graph in Figure 3, the group node can be connected to multiple group nodes. We can also establish the inheritance child nodes by hierarchical model. The group node "forklift" can be created multi-level child node. The child nodes have their

own controlled independence movement, while they also inherit the motion characteristics of the parent node. Thus, in the simulation environment, we can complete various control of the job machinery and its moving parts.

(4)The assembly of scene graph

It may load geometry file of each object in the scene by the WTK function WTnode_load or WTmovenode_load. And the scene tree loads the scene sub-tree with the composition of the scene. The parent node is appointed to adopt the loading methods in the parameters of the function. Assembling all objects in the scene, we can get a complete scene graph finally. As core equipment and control objects in simulation, the forklift can be seen as an independent object in the scene graph when it link with other parts of the scene. But it is also a mobile node which is composed with a large number of moving parts and structural parts. In order to ensure the virtual forklift truck moving synchronized with the actual, we must strictly to calculate the transformation matrix when loading the geometry nodes to do forklift assembly. And determine the correct position of the components in the space.

3.5   The Conclusion of Application and Research

The site of the operation for the virtual simulation experiment is a 1000mm × 1000mm bench, and the simulation is a simple on-site rail operations. The yard include forklifts, obstructions, goods, construction and other physical model, they are produced scaled. The initial position of all objects in the yard is correspondence with the virtual scene. Through determining the speed of the forklift truck model's wheel drive motor, door drive motor, fork drive motor and the actual one's speed, we can get correspondence between the virtual motor and the actual, and make the forklift truck models and the actual have synchronized movements.

In the course of simulation, we can use the space ball as space navigation tool of view, and track people's horizons. The operator see the three-dimensional simulation images on a computer screen through head-mounted display to obtain the experimental information of the operating table, use the keyboard and data glove to control the movement and loading and unloading operations.

4   Conclusions

The virtual reality modeling and simulation of rail transport of dangerous goods of is the concrete application of virtual reality technology, it simulates a audio-visual space for the rail transport of dangerous goods safety. It can make the user learning and training efficient in the virtual environment. At the same time, users can remotely train in different locations, breaking the constraints of previous training time and space. The development and putting into use of the system will give benefit to management of dangerous goods and the training for field operations staff, thus to improve the level of railway transport safety.

References

[1] Wang, C.: The theory, realization and application of the virtual environment (virtual reality) technical, pp. 55–60. Tsinghua University publishing house, Beijing (1996)

[2] Matijaseric. A Networked VE for Mobile Robotics Approaches. Tech-Report of University of Southwestern Louisiana, USA, 20-40 (1999)

[3] Li, J., Zhang, J., Zhang, J.: The virtual reality system of coal mining working surface which based on PC. Journal of Taiyuan University of Technology 34(1), 37–38, 42 (2003) (in Chinese)

[4] Li, Q.: The simulation and research of construction progress about a factory based on VR. Handan: Hebei Engineering College, 33–65 (2005) (in Chinese)

[5] Lan, Z., Li, Q., Xu, J.: The present situation and analysis of the application of virtual reality technology. Coal Science Technology in the Coal Mine Safety 34(11), 56–59 (2006) (in Chinese)

A GPU-RSVM Based Intrusion Detection Classifier

Xueqin Zhang[1], Chen Zhao[1], Jiyi Wu[2], and Chao Song[1]

[1] School of Information Science and Engineering,
East China University of Science and Technology, Shanghai, China
`zxq@ecust.edu.cn`
[2] Hangzhou Key Lab of E-Bussiness and Information Security, Hangzhou Normal
University, Zhejiang 310036, China

Abstract. Recently support vector machines based intrusion detection methods are increasingly being researched because it can detect unknown attacks. But solving a support vector machine problem is a typical quadratic optimization problem, which is influenced by the number of training samples. Due to GPU's high performance in parallel computing, this paper proposes a Euclidean distance based reduction algorithm developed on GPU platform, which is called GPU-RSVM, to eliminate samples that have less effect on building SVM classifier. Experiment results show that the time of reduction process can decrease significantly. With optimal reduction ratio, the overall performance of the intrusion detection classifier based on the proposed GPU-RSVM algorithm is better than that based on LIBSVM algorithm.

Keywords: Intrusion Detection System, Support Vector Machines, data reduction, GPU.

1 Introduction

With the increase of network and computer security events, intrusion detection system (IDS) becomes an important part in security detecting system. According to the difference of detection technology, IDS can be classified into misuse detection and anomaly detection [1]. Machine learning-based intrusion detection approaches belong to the latter one. Since it can identify both known and unknown attack activities, it has been widely researched in recent years.

Support vector machines (SVMs), proposed by Vladimir.N, is an approach of machine learning and has been seen as a powerful tool for solving intrusion detection classification problems in the latest few years. Huang HP proposed a SVM based intrusion detection system and found it could achieve better performance than ANN (Artificial Neural Network) based IDS [2]. Yu J applied MIB and SVM to implement effectively detection on traffic flooding attack [3]. Song used clustering and one-class unsupervised SVM for intrusion detection, and experiments result proved its method can detect unknown attacks effectively [4].

But solving SVM problem would require calculating a quadratic programming (QP) problem whose memory and time complexity requirement increases as a

function of l^2, where l is the number of samples [5]. Consequently, for large-scale network intrusion detection problem, when l increases, the computation consuming of using SVM would be too costly to practise.

In this paper, a Euclidean distance based reduction algorithm is proposed to speed up SVM training, and GPU (Graphics Processing Unit) is utilized to reduce the time complexity in samples reduction period. The paper is organized as follows. In section 2, SVM theory and the reduction algorithm is preliminarily described. In section 3, the GPU-based reduction algorithm is introduced. In section 4, experiment results on KDD'99 intrusion detection dataset are described. Finally, conclusions are given in section 5.

2   Related Background

2.1   Support Vector Machine

Given training sample $(x_1, y_1), \ldots, (x_1, y_1)$, $x \in R^d$, $y_1 \in \{+1, -1\}$, l is the number of training sample, d is the dimension of the sample feature, $\mathbf{x} = \{x_1, x_2, \ldots, x_d\}$, y_1 is the class label.

According to the SVM theory [6],[7], there is an optimal hyperplane (decision boundary), which classify two-class samples with maximum distance, see Fig.1.
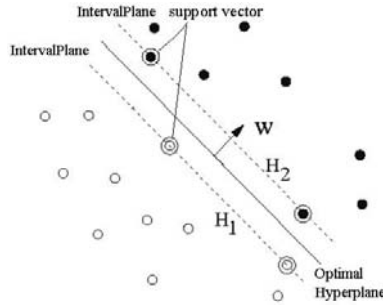
Fig. 1. Optimal hyperplane and support vectors of SVM

In order to obtain this hyperplane, according to Wolfe dual theory, SVM solves the following quadratic optimization problem:

$$\texttt{max} \quad W(\alpha) = \sum_{i=1}^{l} \alpha_i - \frac{1}{2} \sum_{i,j=1}^{l} \alpha_i \alpha_j y_i y_j K(x_i, x_j) \tag{1}$$

$$\texttt{s.t.} \quad \sum_{i=1}^{l} y_i \alpha_i = 0, \ 0 \leq \alpha_i \leq C, \ i = 1, 2, \cdots, l$$

Where C is a penalty coefficient, α_i are the Lagrange multipliers. According to the Karush-Kuhn-Tucker (KKT) conditions, the samples that yield corresponding $\alpha_k > 0$ are called support vectors (SVs). Support vectors, which

are near the optimal hyperplane, locate on the class boundary of each class. In Fig.1, SVs are those samples which are surrounded by hollow circular. The support vector machine classifier is determined by the set of support vectors. $K(x_i, x_j) = \phi(x_i) \cdot \phi(x_j)$ is the kernel function. The common kernels are linear kernel, polynomial kernel, and radial basis function (RBF) kernels.

By solving the quadratic optimization problem, the decision function is:

$$f(x) = \mathrm{sgn}\left\{ \sum_{i=1}^{l} \alpha_i^* y_i K(x_i, x) + b^* \right\} \tag{2}$$

In formula (2), α_i^* and b^* are optimal parameters.

2.2 Eucledean Distance Based Reduced Algorithm

According to the theory of support vector machine, optimal hyperplane is only decided by support vectors. The samples which are far from the optimal hyperplane can be deleted without degrading the classification effect. In this paper, a simple reduction algorithm for linear or similarly linear separable case is proposed, which is based on two facts:

1. if one sample is near the centroid of its own class, then the sample can be deleted. This kind of samples are called periapsises.
2. if one sample is far from the centroid of another class, then the sample can be deleted. This kind of samples are called apoapsises.

To find the periapsises and apoapsises, the reduction algorithm includes three main steps, calculating the centroid of each class, calculating the distance between samples and centroids, sorting the samples by the distance.

In this algorithm, the centroid of positive class is defined as $x^+ = \frac{1}{l_1} \sum_{i=1}^{l_1} x_i$ and the centroid of negative class is defined as $x^- = \frac{1}{l_2} \sum_{j=1}^{l_2} x_j$. Here, l_1, l_2 is the number of positive samples and negative samples respectively. The distance d_+^* from the sample x^* in positive class to the centroid x^+ is:

$$d_+^* = \| x^* - x^+ \| = \sqrt{(x_1^* - x_1^+)^2 + (x_2^* - x_2^+)^2 + \ldots + (x_m^* - x_m^+)^2} \tag{3}$$

and the distance d_-^* from sample x^* in positive class to the centroid x^- is:

$$d_-^* = \| x^* - x^- \| = \sqrt{(x_1^* - x_1^-)^2 + (x_2^* - x_2^-)^2 + \ldots + (x_m^* - x_m^-)^2} \tag{4}$$

In formula (3) and (4), m is the dimension of the sample. The distance d_+', d_-' from some sample x' in negative class to the centroid x^+ and x^- can be calculated in the same way.

When getting the distance between samples and centroids, sorting the positive and negative samples by the distances d_+^*, d_-^*, d_+' and d_-' respectively in

ascending order to generate four monotonous data sequences $s_+^*, s_-^*, s_+^{'}$ and $s_-^{'}$. Then the first ε percent samples (periapsises) in sequence $s_+^*, s_-^{'}$ and the last θ percent samples (apoapsises) in sequence $s_-^*, s_+^{'}$ are the samples that could be deleted respectively. Here, ε and θ are the reduction coefficients. Assuming parameter γ is the sum of ε and θ. At last, there are total γ percent samples that are eliminated. The remaining $(1 - \gamma)$ percent samples are used to construct the reduced SVM training dataset.

3   Intrusion Detection Classifier Based on GPU-RSVM

3.1   The GPU Based Reduction Algorithm

In 1999, NVIDIA introduced its first GPU as a specialized accelerator for 3D graphic. With the development of CUDA (Compute Unified Device Architecture), GPU began to be widely used for general-purpose computations, such as gene squence [8], modecular dynamics [9], fluid dynamics [10].

In CUDA programing model, CPU is called host and GPU is device or co-processor. CPU is in charge of dealing with the strong logic events and serial computation, while GPU focuses on highly threaded parallel processing tasks. CPU and GPU have their own memory space respectively: host memory and device memory. Device memory includes global memory, shared memory, local memory, and also has two additional read-only memory spaces: constant and texture memory [11]. The program executes on the GPU is called kernel. One kernel function takes block as execution unit. Each block includes many threads. Kernel executes sequential program concurrently on a set of parallel threads under SIMT (Single Instruction Multiple Threads) mode. When CUDA kernels are invoked, CUDA threads may access data from multiple memory spaces.
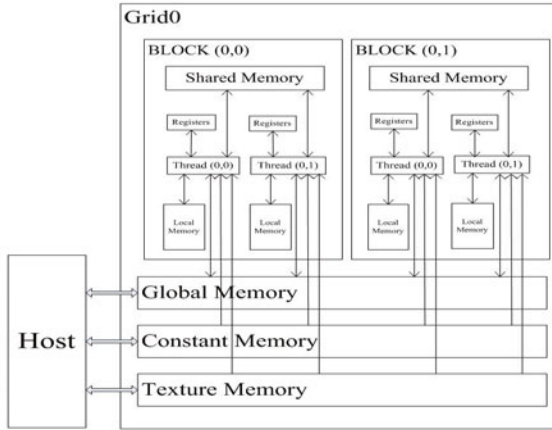

Fig. 2. Memory Hierarchies of GPU

In the reduction algorithm described above, there are a lot of addition, substraction and multiplication operations between matrixes. With CUDA threads, these operations can be executed in parallel.

1) Distance calculation. The distance calculation between samples mainly includes three kernel programs on GPU. The `centroid_compute`() kernel is used to calculate the centroid of two-class samples respectively. Second, the `vector_compute`() kernel is developed to compute the difference and square between the elements of vectors, such as $(x_i^* - x_i^+)^2$. And the `sum_reduction`() kernel is designed to accumulate these values. In order to get high accuracy, the system single-precision floating-point functions `__fadd_rn`() and `__fmul_rn`() are used in these kernels.

2) Sorting Operation. Bitonic sorting method is adopted to select the periapsises and apoapsises [12]. Bitonic sort is an unusual sorting algorithm designed specially for parallel machines. The detail of bitonic sorting method is in[13].

When designing kernel program, it is very important to assign device memories reasonably. For example, the centroid of two-class samples are used in each time of distance calculating, so they should be assigned into the constant memory because the data transfer speed of constant memory is much faster than global memory. Also, in `sum_reduction`() and `bitonic_sort`() kernel, since kernel threads need to access memory frequently to do accumulation and comparison operation, the data in computing should be loaded into shared memory firstly till the distance calculation and bitonic sorting is done. Then these data should be transferred to global memory for further analysis.

3.2   GPU-RSVM Intrusion Detection Classification Algorithm

The GPU based reduction SVM algorithm (GPU-RSVM) includes three parts: SVM training data reduction, SVM based intrusion detection classification model training and intrusion detection testing. In this proposed algorithm, SVM pattern recognization method is applied to build intrusion detection classifier and detect unknown attacks. The reduced SVM algorithm is proposed to decrease the amount of SVM training samples to resolve complexity of time and space in SVM modeling process without sacrificing detecting accuracy. The reduction algorithm is implemented on GPU parallel to save the time in reduction process.

4   Experiments and Results

4.1   Dataset Description

A real world data set taken from the KDD'99 (1999 knowledge discovery and data mining conference) intrusion detection standard dataset was used in experiment [14]. In this dataset, there are about 5 million network connection records that including normal network connection record and four categories attack record: DoS, R2L,U2L and Probing.

Because the size of original dataset is huge, two subsets of the original data set, known as the '10percent' dataset in KDD'99, were selected as the training dataset

'D41' and testing dataset 'T41'. Each of the dataset contains approximately 50000 records. The data are labeled as attack or normal. In these two datasets, the normal records and attack records are mixed randomly.

4.2   Experiments and Analysis

In this section, three groups of experiments are executed. All experiments run on a stand-alone personal computer with Pentium Dual-Core CPU running at 2.79GHz, 2G main memory and an NVIDIA GeForce GTS250 GPU which has 16 multiprocessors, 128 cores and 512MB of RAM.

1) Experiment 1. In experiment 1, the reduction algorithm runs on GPU and CPU respectively to compare their reduction speed. Four subsets with different size, including 1000, 5000, 20000, 49407, are taken from 'D41' respectively. With the same reduction coefficients $\varepsilon = 0.2$, $\theta = 0.2$, the cost time of reduction operation on different datasets are shown in Fig.3.
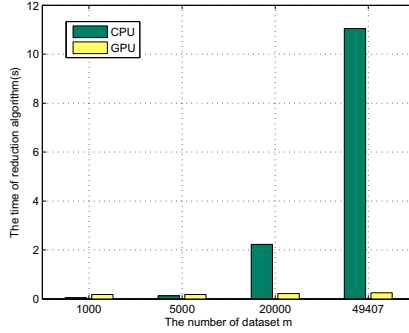
Fig. 3. The time of reduction implemented on CPU vs. GPU

From the Fig.3, when the number of sample is 1000, 5000, 20000 and 49407, the speedup ratio of GPU to CPU is 0.03, 0.73, 10.14 and 40 respectively. And with the increase of amount of samples, the speedup ratio increases sharply. The reason is that GPU communicates with CPU using PCI-E bus. Limited by the I/O bandwidth, the data transfer between GPU and CPU usually is the bottleneck in GPU+CPU collaborative work model. When the calculation density is low, the I/O transfer time between GPU and CPU is longer than the computing time. But with the increase of calculation density, the time consuming in computing become longer and will cover the I/O transfer time. So GPU is suitable for parallel computing with large amount of samples.

2) Experiment 2. Experiment 2 focuses on seeking the optimal reduction coefficients θ and ε of the intrusion detection dataset "D41". To find the optimal pair of coefficients, we change one coefficient and fix another coefficient, and use classification accuracy of SVM classifier as evaluation index. LIBSVM [15] is

(a) $Kernel : RBF$ (b) $Kernel : Linear$
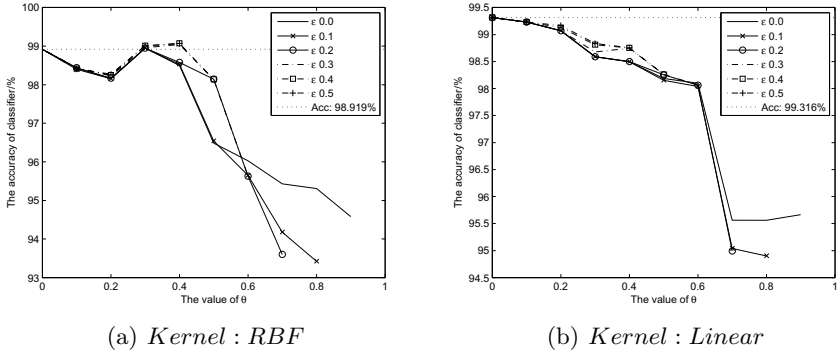
Fig. 4. The accuracy of classifier in different ε and θ

adopted as SVM training and testing tool in this experiment. In training period, default parameters are taken. The reduction ratio-dependent accuracy curves are shown in Fig.4.

From the Fig.4, it shows, in RBF kernel, the classification accuracy on the original dataset 'D41' is 98.92%. When taking ε=0.45 and θ=0.4 (it means there is only 15 percents samples of 'D41' remaining), the classifier gets the highest accuracy 99.07%. But the classification accuracy drops sharply if the number of eliminated points continues decreasing. In linear kernel, the classification accuracy on the original dataset 'D41' is the highest. With the increase of θ, the classification accuracy is inclined to decrease. But the shape of these curves with different ε is almost coincident, it means that ε is a non-sensitive parameter for linear kernel. Considering the decrease of 1% in classification accuracy is acceptable, $\varepsilon = 0.45$ and $\theta = 0.4$ are taken as the optimal parameter pair.

3) Experiment 3. This group of experiments are conducted to compare the performance of intrusion detection classifiers trained by GPU-RSVM and LIB-SVM in terms of the training time, testing time, prediction accuracy, number of support vectors, false negative rate (FNR) and false positive rate (FPR).

According to the results of experiment 2, when applying RBF kernel to train SVM model, the optimal reduction coefficients θ is 0.4 and ε is 0.45. In this case, the cost time of sample reduction is 265.68ms on GPU and 8564.23ms on CPU. The speedup ratio of GPU to CPU is 32. The number of eliminated samples is 41995 and 7412 samples are reserved. When applying linear kernel to train SVM model, the reduction coefficients θ is 0.4 and ε is 0.5. The cost time of sample reduction is 247.32ms on GPU and 9234.72ms on CPU. The speedup ratio of GPU to CPU is 37. The number of eliminated samples is 41995 and 4941 samples are reserved.

After the reduction operation, the SVM intrusion detection classifiers are trained on reduced dataset and original dataset respectively. In training process, default parameters are used. The dataset "T41" is taken as testing dataset in testing process. The experiment result is shown in Table.1.

Table 1. The performance comparison between GPU-RSVM and LIBSVM

	GPU-RSVM		LIBSVM	
Kernel	RBF	LINEAR	RBF	LINEAR
Training Time(s)	4.141	1.875	34.625	25.047
Testing Time(s)	19.218	10.653	21.688	14.125
Number of SVs	854	461	975	671
Accuracy(%)	99.07	98.76	98.92	99.32
FPR(%)	0.41	0.08	0.67	0.42
FNR(%)	0.52	1.16	0.41	0.27

From the Table 1, whether in RBF or linear kernel, the training and testing time of GPU-RSVM is shorter than that of LIBSVM. In RBF kernel, the overall speedup ratio is 8.28 in training process (including the reduction time) and 1.13 in testing process, the prediction accuracy increases. In linear classifier, the overall speedup ratio is 13.36 in training process (including the reduction time) and 1.33 in testing process, the prediction accuracy decreases, but less than 1%.

5   Conclusion

In order to build SVM based network intrusion detection classifier fast, a reduced SVM algorithm (GPU-RSVM) is proposed. This reduction algorithm is implemented on GPU platform. With GPU's highly parallel computation capability, the cost time of reduction process decreases greatly. By deleting the periapsises and apoapsises in the original SVM training dataset, the size of the training dataset can shrink effectively. In this way, the training and testing time become shorter, while the prediction accuracy hasn't obviously declined in general.

The future work will focus on parallelizing the SVM algorithm on GPU to speed up the whole modeling process.

References

1. Vapnik, V.N.: An overview of statistical learning theory. J. IEEE transactions on Neural Networks 10, 988–1000 (1999)
2. Huang, H.P., Yang, F.C., et al.: Intrusion Detection Based on Active Networks. J. Information Science and Engineering 25, 843–859 (2005)
3. Yu, J., Lee, H., et al.: Traffic flooding attack detection with SNMP MIB using SVM. J. Computer Communications 31, 4212–4219 (2008)
4. Song, J., Takakura, H., et al.: Unsupervised Anomaly Detection Based on Clustering and Multiple One-Class SVM. J. IEICE Transactions on Communications E92-B, 1981–1990 (2009)
5. Kim, D.S., Nguyen, H.-N., Park, J.S.: Genetic algorithm to improve SVM based-network intrusion detection system. In: 19th International Conference on Advanced Information Networking and Applications, pp. 155–158. IEEE Press, Taiwan (2005)
6. Cortes, C., Vapnik, V.: Support Vector Networks. J. Machine learning 20, 273–297 (1995)

7. Burges, C.J.C.: A tutorial on support vector machines for pattern recognition. J. Data Mining and Knowledge Discovery 2(2), 121–167 (1998)
8. Qiong, Z., Yingsha, Z.: Hierarchical clustering of gene expression profiles with graphics hardware acceleration. J. Pattern Recognition Letters 27, 676–681 (2006)
9. Anderson, J.A., Lorenz, C.D., Travesset, A.: General Purpose Molecular Dynamics Simulations Fully Implemented on Graphics Processing Units. J. Computational Physics 227, 5342–5359 (2008)
10. Garland, M., Le Grand, S., Nickolls, J., Anderson, J., Hardwick, J., Morton, S., Phillips, E., Yao, Z., Volkov, V.: Parallel Computing Experiences with CUDA. J. IEEE Micro. 28, 13–27 (2008)
11. CUDA C Programming Guide,
    http://developer.nvidia.com/object/cuda_3_2_downloads.html
12. Batcher, K.: Sorting networks and their applications. In: Proc. AFIPS Spring Joint Computer Conference, pp. 307–314. ACM Press, New York (1968)
13. Bitonic   Sorting,   http://facultyfp.salisbury.edu/taanastasio/COSC490/
    Fall03/Lectures/Sorting/bitonic.pdf
14. KDDCUP 1999 dataset,
    http://kdd.ics.uci.edu/dataset/kddcup99/kddcup99.htm
15. LIBSVM - A Library for Support Vector Machines,
    http://www.csie.ntu.edu.tw/~cjlin/libsvm/

Low Complexity Decoding Algorithm for Nonbinary LDPC Codes

Xue-Fei Yang[1], Wei Li[2], and Lian Huang[3]

[1] Naval Arm Academy, Beijing, 100161, China
[2] Naval Arm Office, Beijing, 100161, China
[3] Office of Naval Delegate in Wuhu, 241000, China

Abstract. Low complexity decoding algorithm is proposed to reduce the complexity of decoding algorithm for nonbinary quasi-cyclic LDPC codes. The algorithm uses methods of logarithm domain and look-up table based on the FFT-QSPA algorithm, avoiding multiplication and division calculations. These calculations make the hardware compute slowly. As a result, the algorithm makes the hardware easier to realize. The parity check matrices with quasi-cyclic form are constructed based on the finite fields, which are benefit for linear encoding based on the feedback shift registers. The letter presents a scheme combined with the constitution, coding and decoding of nonbinary quasi-cyclic LDPC codes with low complexity. The simulation shows that nonbinary quasi-cyclic LDPC codes achieve significant coding gains over RS codes with lower complexity and better performance.

Keywords: nonbinary LDPC codes, FFT-QSPA, quasi-cyclic codes, finite field.

1   Introduction

Nonbinary LDPC code is discovered by Davey and Mackay in 1998. They also brought forward the quasi sum-product decoding algorithm (QSPA)[1]. Their research indicate that the nonbinary LDPC code has superior capability than binary LDPC code, especially in middle short code(code length less than 1000), but with high decoding complexity. To reduce the complexity of decoding algorithm, FFT-QSPA is proposed by Davey and Mackay in 2000, which using FFT algorithm based on QSPA, with complexity of $o(q \log q)$. This letter focus on low complexity decoding algorithm for nonbinary LDPC codes, a scheme combine construction-coding-decoding is presented, that quasi-cyclic structured check matrix to bring coding superiority. Only simple cycle-shift register accumulate(CSRAA)union to carry through coding, the complexity is direct ration to the check bit. FFT-QSPA is used for decoding eclectic of capability and complexity.

   The letter arranged as follows: The second part present methods to construct nonbinary LDPC codes with finite field; the third part present the low complexity Decoding algorithm and analyze the complexity; the forth part present the simulate result and analysis; the fifth part summarize the letter and point out the next step to deepen the research.

2   Construct of Quasi-Cycle Nonbinary LDPC Code

The construct of nonbinary LDPC code focus on the design and construct of the check matrix.Suppose α is the primitive of GF(q), then $\alpha^{-\infty} = 0$, $\alpha^0 = 1$, α, ..., α^{q-2} are al the elements of GF(q)field. Location vector of nonzero element α^i ($0 \leq i \leq q-2$) is $\mathbf{z}(\alpha^i) = (z_0, z_1, \ldots, z_{q-2})$, $z_i = \alpha^i$, other $q-2$ elements are 0.

In GF(q) field, a basic matrix $\mathbf{W}$ is needed:

$$\mathbf{W} = \begin{bmatrix} \mathbf{w}_0 \\ \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_{m-1} \end{bmatrix} = \begin{bmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,n-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{m-1,0} & w_{m-1,1} & \cdots & w_{m-1,n-1} \end{bmatrix} \tag{1}$$

$\mathbf{W}$ has to satisfy the α-row restriction 1 and 2:1. For $0 \leq i < m$, $0 \leq k, l < q-1$ and $k \neq l$, $\alpha^k \mathbf{w}_i$ and $\alpha^l \mathbf{w}_i$ are at least different in at least $n-1$ positions; 2. For $0 \leq i, j < m$, $i \neq j$, and $0 \leq k, l < q-1$, $\alpha^k \mathbf{w}_i$ and $\alpha^l \mathbf{w}_j$ are different in at least $n-1$ positions. $\mathbf{A}_{i,j}$ is construct through the horizon expand and vertical expand of every element $w_{i,j}$:

$$\mathbf{A}_{i,j} = \begin{bmatrix} \mathbf{z}(w_{i,j}) \\ \mathbf{z}(\alpha w_{i,j}) \\ \vdots \\ \mathbf{z}(\alpha^{q-2} w_{i,j}) \end{bmatrix} \tag{2}$$

$m(q-1) \times n(q-1)$ dimension check matrix $\mathbf{H}$ is constructed:

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}_{0,0} & \mathbf{A}_{0,1} & \cdots & \mathbf{A}_{0,n-1} \\ \mathbf{A}_{1,0} & \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{m-1,0} & \mathbf{A}_{m-1,1} & \cdots & \mathbf{A}_{m-1,n-1} \end{bmatrix} \tag{3}$$

Consider the add group, suppose α is the primitive of GF(q) field, construct the base matrix $\mathbf{W}$:

$$\mathbf{W}^{(1)} = \begin{bmatrix} \alpha^0 - 1 & \alpha - 1 & \cdots & \alpha^{q-2} - 1 \\ \alpha^{q-2} - 1 & \alpha^0 - 1 & \cdots & \alpha^{q-1} - 1 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha - 1 & \alpha^2 - 1 & \cdots & \alpha^0 - 1 \end{bmatrix} \tag{4}$$

3 Low Complexity Decoding Algorithm

3.1 The Basic Concepts and Initialization Process

In the chart 1, nonbinary LDPC decoding gene chart contains variable node(cob on the top), check node(cob on the floor), permutation node and reset node.
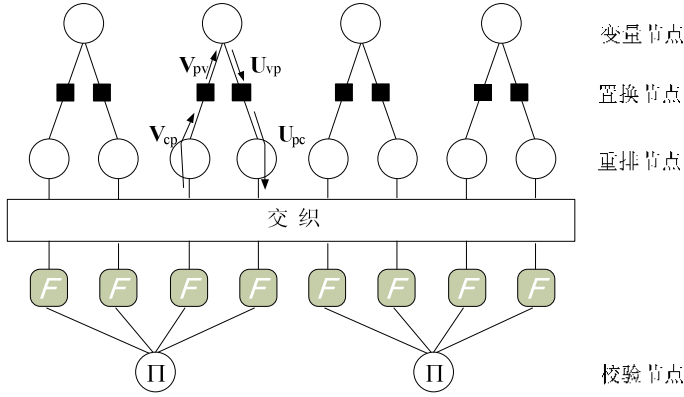
Fig. 1. Nonbinary LDPC decoding gene

Define the variable as follows: $\{\mathbf{V}_{pv}\}_{v=1,\ldots,d_v}$ represent the variable node enter the degree d_v node, $\{\mathbf{U}_{vp}\}_{v=1,\ldots,d_v}$ represent the variable node come out from the degree d_v node. The suffix pv represents the vector transfer from permutation node to reset node, vp represent the reverse; Also $\{\mathbf{U}_{pc}\}_{c=1,\ldots,d_c}$ represent the vector enter the degree d_c check node, $\{\mathbf{V}_{cp}\}_{c=1,\ldots,d_c}$ represent the belief enter in the check node.

We assume the (N, K) nonbinary LDPC code transferring on AWGN channel, using high rank modulate[10] (q scale, $q = 2^b$), mapping the code serial($c_1^1 c_1^2 \ldots c_1^b c_2^1 c_2^2 \ldots c_2^b \ldots c_N^1 c_N^2 \ldots c_N^b$)to $(s_1, s_2, \ldots, s_N)$. The received array after demodulated is:

$$y_i = s_i + v_i = (s_{i,c} + js_{i,s}) + (v_{i,c} + jv_{i,s}) = y_{i,c} + jy_{i,s}, i = 1, \ldots, N \qquad (5)$$

$v_{i,c}$ and $v_{i,s}$ are two independent gauss white noise.

$s^{(a)}$ represent constellation plot the a th symbol, suppose $s^{(a)} = s_c^{(a)} + js_s^{(a)}$, due to Bayes formula, the beforehand verify probability is:

$$P(y_i \mid s_i) = \frac{1}{k_i} \cdot \frac{\exp(-\dfrac{(y_{i,c} - s_{i,c})^2 + (y_{i,s} - s_{i,s})^2}{2\sigma^2})}{\displaystyle\sum_{a=0}^{q-1} \exp(-\dfrac{(y_{i,c} - s_c^{(a)})^2 + (y_{i,s} - s_s^{(a)})^2}{2\sigma^2})} \quad i = 0, \ldots, N-1 \qquad (6)$$

$k_i = P(s_i)/2\pi\sigma^2 P(y_i)$ is a constant.

When adopting BPSK modulate, mapping mode is $s_i = 2c_i - 1$ ($i = 1, \ldots, N$), the initialize probability is:

$$P(y_i \mid c_i = 0) = 1/[1 + \exp(2y_i / \sigma^2)]$$
$$P(y_i \mid c_i = 1) = 1/[1 + \exp(-2y_i / \sigma^2)] \qquad (7)$$

3.2   Low complexity FFT-QSPA Algorithm

Adopting BPSK modulate,calculate the probability according to the receive channel y_i, then initialization probability is gained:

$$L_i = p(y_i \mid \mathbf{c}_i = \mathbf{a}) = p(y_i \mid [c_{i1} \cdots c_{iq}] = [a_1 \cdots a_q]) = \prod_{k=1}^{q} p(y_i \mid c_i = a_k) \qquad (8)$$

$$i = 0, \ldots, N-1$$

a_k is k th bit of binary form of $\mathbf{a}$,believe degree $\mathbf{L} = (L_1, L_2, \ldots, L_N)$.

Because we adopt the logarithm field to calculate, so all the believe degree turn to logarithm. To conquer the limit of q, using the Fourier transfom to transfer the calculation to the frequency field, convolution turn to multiplicative operation. Then use the logarithm field turn the multiply algorithm to additive algorithm, depress the hardware operation time. All the operation of exponent and logarithm use the look-up table to reduce the operation complexity.

Suppose $\mathbf{U}[i_1, \ldots, i_p]$ as p dimension vector, and $(i_1, \ldots, i_p) \in \{0,1\}^p$. The FFT operation rule of $\mathbf{U}[i_1, \ldots, i_p]$ in GF(2^p) if formula(8):

$$\mathbf{W} = \mathcal{F}(\mathbf{U}) = \mathbf{U} \times_1 \mathbf{F} \times_2 \mathbf{F} \ldots \times_p \mathbf{F} \qquad (9)$$

Tensor multiplication $\mathbf{Z} = \mathbf{U} \times_k \mathbf{F}$ is defined as formula (9):

$$\mathbf{Z}[i_1,\ldots,i_{k-1},0,i_{k+1},\ldots,i_p] = \frac{1}{\sqrt{2}}(\mathbf{U}[i_1,\ldots,i_{k-1},0,i_{k+1},\ldots,i_p] + \mathbf{U}[i_1,\ldots,i_{k-1},1,i_{k+1},\ldots,i_p])$$
$$\mathbf{Z}[i_1,\ldots,i_{k-1},1,i_{k+1},\ldots,i_p] = \frac{1}{\sqrt{2}}(\mathbf{U}[i_1,\ldots,i_{k-1},0,i_{k+1},\ldots,i_p] - \mathbf{U}[i_1,\ldots,i_{k-1},1,i_{k+1},\ldots,i_p])$$
(10)

$(i_1 \ldots i_{k-1}, i_{k+1} \ldots i_p) \in \{0,1\}^{p-1}$ 。

The detailed steps are as follows:

Step 1:initialization

Suppose $\mathbf{U}_{vp} = \mathbf{L}$, factors in $\mathbf{L}$ calculated in terms of formula(7);

Step2:Update the check node

(S1):Shift step

$$vec(\mathbf{U}_{pc}) = \mathbf{P}_{h(x)} vec(\mathbf{U}_{vp})$$
(11)

$\mathbf{P}_{h(x)}$ is actually cycle shift all the factors,the reverse shift denoted by $\mathbf{P}_{h(x)}^{-1}$;

(S2):Reset

Rearrange the believe degree as ascending order according to the $a \in \mathrm{GF}(q)$;

(S3): FFT

$$\mathbf{V}_{tp} = \mathcal{F}^{-1}(\exp(\sum_{v=1,v\neq t}^{d_c}(\log(\mathcal{F}(\mathbf{U}_{pv}))))), \quad t = 1,\cdots,d_c \; ;$$
(12)

Step 3:Update the variable node

$$\mathbf{U}_{tp} = \exp(\log(\mathbf{L}) + \sum_{v=1,v\neq t}^{d_c} \log(\mathbf{V}_{pv})) \quad t = 1,\cdots,d_c \; ;$$
(13)

Step 4:Try decoding :Hard-judge

$$\hat{\mathbf{c}}_n = \arg\max_{GF(q)}(\log(\mathbf{L}) + \sum_{v=1}^{d_c} \log(\mathbf{V}_{pv})), \quad t = 1,\cdots,d_c \; ;$$
(14)

If $\mathbf{z} = \hat{\mathbf{c}} \cdot \mathbf{H}^T = \mathbf{0}$, then decoding correctly; or repeat step 2\3\4 until the most iterative time.

3.3   Complexity Analyses

The decoding of nnbinary LDPC code use the iterative decoding mode, the operation complexity focus on the check node, the operations on variable node affect little to the whole. Using QSPA algorithm to decode LDPC code in GF(q) field, the operation complexity of check node is $o(q^2)$. When calculating in FFT, check node turn to multiply operation, the complexity descending to $o(q \log q)$. Then method of log domain and lookup table make the multiplication turn to addition, the complexity descending again and easier to realization for hardware. For the sake of balance complexity and decoding performance, the letter present an algorithm for low complexity nonbinary LDPC codedecoding, based on look-up table, which barring multiplication and easier for hardware completement. For (N, K) regular GF(q)-LDPCcode, every step of every iterative process list as follow:

Table 1. Operation quantity of every iterative

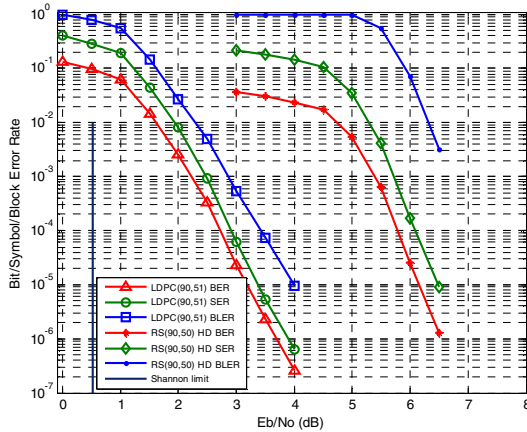| Step	Additive operation
2	$Nd_v q(d_c - 1 + 2\log_2 q)$
3	$Nd_v q(d_v + 1)$
4	$Nd_v q(d_v + 2) + (N - K)(2d_c - 1)$
Total	$Nd_v q(2 + d_c + 2d_v + 2\log_2 q) + (N - K)(2d_c - 1)$

Fig. 2. Performance curve of (90,51) GF(2^4)-LDPC code and (90,50)RS code

4   Simulation and Analyse

The simulation is carried based on AWGN channel, the sender use BPSK modulation, the constructed nonbinary LDPC code compared with RS code as the rate and length

is equivalent. Nonbinary LDPC codes use the decoding algorithm this letter presented. The max iterative time is 50, RS code use the hard-judge algorithm. Construct the check matrix $\mathbf{H}$ in GF(2^4) with finite approach, choose d_v =3 and d_c =6,the null space of $\mathbf{H}$ present(90,51)QC-LDPC code with rate 0.57 and least distance 4.

In figure 2, when BER=10^{-5}, (90,51)GF(2^4)-LDPC code gain 3dB coding plus than (90,50)RS code. when BER=10^{-2}, (90,51)GF(2^4)-LDPC code gain 2.79dB coding plus than (90,50)RS code.

Conclusion can be made from figure 2 that nonbinary LDPC code is superior than RS code at the same code rate and the same bit length.

Table 2. Operation times of every iteration

LDPC iterative times	(90,51) LDPC	(90,50)RS
5	86,400	2,073,600
50	864,000	2,073,600

When using FFT-QSPA decoding algorithm, conclusion can be made from table 1 that operation times of every iteration is $o(Nd_v q^m \log q^m)$. Table 2 present the decoding operation times of nonbinary LDPC code and RS code. When iterated for 5 times, the operation times of every iteration of (90,50)RS code is 24 times that of (90,51) LDPC code, when iterated for 50 times, the operation times for every iteration of (90,50)RS code is 2.4 times that of (90,51) LDPC code. So the complexity has a relation to construct of check matrix $\mathbf{H}$, N and d_v is also the factor restrict the complexity. The low complexity decoding algorithm is gained on the consider of complexity of decoding but also has to consider the construct of the check matrix.

5   Summarize

The decoding complexity of decoding of nonbinary LDPC code is an important factor restricts the complication. For the sake of reducing the complexity of decoding of nonbinary quasi-cyclic low density parity check(QC-LDPC)code, the construct of the quasi-cyclic check matrix is based on finite geometry and finite field. These methods can be realized by linear coding of nonbinary LDPC. The simulation prove that the nonbinary QC-LDPC code construct with the method this letter present has not only a significant performance over RS code with same parameter, but also reducing the complexity a lot.

References

1. Davey, M.C., Mackay, D.J.C.: Low-density parity check codes over GF(q). J. IEEE Commun. Lett. 2(6), 165–167 (1998)
2. Song, H., Cruz, J.R.: Reduced-complexity decoding of Q-ary LDPC codes for magnetic recording. J. IEEE Trans. Magn. 39(3), 1081–1087 (2003)

3. Declercq, D., Fossorier, M.: Decoding algorithms for nonbinary LDPC codes over GF(q). J. IEEE Trans. Commun. 55(4), 633–643 (2007)
4. Zeng, L., Lan, L., Tai, Y.Y., et al.: Construction of Nonbinary Quasi-Cyclic LDPC Codes:A Finite Field Approach. J. IEEE Trans. Commun. 56(4), 545–554 (2008)
5. Song, S., Zhou, B., Lin, S., et al.: A Unified Approach to the Construction of Binary and Nonbinary Quasi-Cyclic LDPC Codes Based on Finite Fields. J. IEEE Trans. Commun. 57(1), 84–93 (2009)
6. Zhou, B., Kang, J., Tai, Y.Y., Lin, S.: High Performance Non-Binary Quasi-Cyclic LDPC Codes on Euclidean Geometries. J. IEEE Trans. Commun. 57(5), 1298–1311 (2009)
7. Kou, Y., Lin, S., Fossorier, M.P.C.: Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results. J. IEEE Trans. Inform. Theory 47(7), 2711–2735 (2001)
8. Dou, G., Gao, J., Liu, B.: Fast algorithm of coding and decoding of quasi-cyclic LDPC code and the DSP implement (04), 323–327 (2008)

Efficient Query Protocol for Database's Privacy

Xianping Yuan[*], Hong Zhong[**], Hongsheng Huang[***], and Lei Yi[****]

Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education,
Anhui University, Hefei Anhui, P.R. China 230039;
School of Computer Science and Technology, Anhui University,
Hefei Anhui, P.R. China 230039
`yuanxp0123@yahoo.cn`, `zhonghahu@sohu.com`,
`huanghongsheng81@sina.com`, `abcyilei@126.com`

Abstract. To protect two party privacy of database's query, known solutions are encrypt the entire database and thus the encryption cost is excessively high. To resolve this problem, we construct a new efficient solution to database's query in semi-honest mode, Based on the assumption of combination commutative encryption and the oblivious transfer protocol. The protocol can safely and efficiently finished database's secure query lack of third-party participation. Furthermore, the correctness, the security and the computational complexity of this scheme are as well analyzed. The results of analysis show that compared with known solutions, the proposed scheme has much less computational complexity.

Keywords: secure multi-party computation, secure query, commutative encryption, privacy preserving.

1   Introduction

Database security question not only has extensive applications in secure multi-party computation [1], but also plays a very important role in many practical applications. For example, a customer wants to apply for endowment insurance at an insurance company. In order to prevent the applicant, the insurance business must find out whether the circ database has already existed his insurance information, or others. During the inquiry process, the server may maliciously modify the policy-holder's information. At the same time server also do not want the inquirer to know other irrelevant the information of policy-holder in the database. Therefore in the database query, on the one hand if the user can get the results of his query only and don't know any other records; On the other hand, The owner of the database do not know which the record the user inquires, such inquiry is called the secure query[2]. Security query is

---

[*] Master, the main research areas: Network and Information Security.
[**] Professor, Master Instructor, the main research areas: Information Security, Distributed Computing.
[***] Graduate Student, the main research areas: Network and Information Security.
[****] Master, the main research areas: Network and Information Security.

widespread in commercial competition, military cooperation and etc. Therefore, under the condition of preserving privacy, how to query database is became more and more important.

Rakesh Agrawal gives an effective resolution to security retrieval scheme [2]. In this scheme, two participates respectively encrypted their plaintexts, then sent their ciphertext to each other, after that they re-encrypted the ciphertext, last they both get two sets ciphertext results. Without third party, they realized the secure query. But the deficiency of the scheme is overmuch encryption calculation.

Based on Equijoin protocol, a scheme was proposed in Literature [3], which encryption cost is too much. So it was hard to adapt to the large database queries. In 2009, Yuan proposed the method for a sensitive information retrieval. Based on exchange encryption assumptions; it achieved the sensitive information query in semi-honest mode. Due to the third party may be incredible, such scheme brought a new hidden danger.

Aiming at the problems above, based on exchange cryptographic function and oblivious transfer protocol, we puts forward a new database secure query protocol, which does not needs the third party. It meets definition of the secure query.

2   Preliminaries

2.1   Commutative Encryption

The commutative encryption is a pair of combination of encryption function of which form like $f(g(v)) = g(f(v))$ [4,5]. Through encrypting v, two participates will not decrypt $f(g(v))$ without mutual cooperation. Supposed F is a commutative encryption function, which satisfies $f : Key\ F \times Dom\ F \rightarrow Dom\ F$, The following properties:

(1) For all e, $e' \in key\ F$, which satisfies $f_e \circ f_{e'} = f_{e'} \circ f_e$, that is, F is interchangeable.
(2) For each $f_e : Dom\ F \rightarrow Dom\ F$, f is bijective function.
(3) For a given e, inverse function is computable in polynomial time.
(4) Distribution of $(x, f_e(x), y, f_e(y))$ and distribution of $(x, f_e(x), y, z)$ are indistinguishable, of which $x, y, z \in_r Dom\ F$ and $e \in_R Key$.

2.2   Oblivious Transfer-OT

Alice and Bob are two parts in this protocol. The definition of OT_n^k is that a sender Alice inputs n messages $\{m_1, m_2, \cdots, m_n\}$, and a receiver Bob gets k messages out of n. At the same time Alice doesn't know which k messages Bob has got.

Inputs: Alice   inputs   n   messages $\{m_1, m_2, \cdots, m_n\}$ and   Bob k messages $\{\lambda_1, \lambda_2, \cdots, \lambda_k\}$.

Outputs: Bob gets k messages $\{m_{i_1}, m_{i_2}, \cdots, m_{i_k}\}$.

3   The Scheme

Suppose that Alice and Bob are two participants. The model of secure query protocol shows below (see Figure 1).
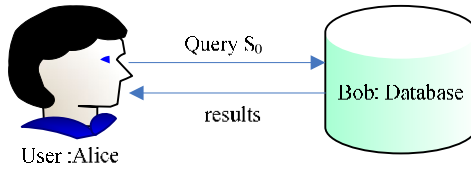
Fig. 1. Secure Query

Alice is a user and she has a condition v, where v is a value of the property V. Bob has a table from database (see Table 1). There are two sets, one is V= { $v_1, v_2, \cdots, v_n$ } and the other is { $ext(v_1), ext(v_2), \cdots, ext(v_n)$ }. Alice would like to know whether the property V of the relational table equal to v. If there is, it returns the results v corresponding to the record; if not, returns nothing.

Table 1. Relational Table

	Attribute A	Attribute V	Attribute B
$ext(v_1)$	a_1	v_1	b_1
$ext(v_2)$	a_2	v_2	b_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$ext(v_n)$	a_n	v_n	b_n

The proposed protocol:

Inputs: Alice inputs a property *v*, and Bob a table from database.
Outputs: Alice gets some records of which properties V equal to *v*.

Security:

At the end of this protocol, Alice knows what she wants to know. Bob knows nothing what Alice gets.

The detailed description of the protocol:

There are have Alice and Bob to participate the communication in the protocol is proposed, and is based on semi-honest mode. Alice selects the public/private keys(pk_a , sk_a), Bob selects the public key pk_b .Open the public key and private key is kept confidential, E() is the commutative encryption function.

The execution of the protocol is as follows:

Steps 1: Alice Encryption: $E_{pk_a}(v)$;

Alice $\rightarrow$ Bob: $E_{pk_a}(v)$

Steps 2: Bob Encryption: $E_{pk_b}(E_{pk_a}(v))$ and

For $i=1$ to n {

Bob Encryption: $E_{pk_b}(v_i)$

}

Bob $\rightarrow$ Alice: $E_{pk_b}(E_{pk_a}(v)), E_{pk_b}(v_1), E_{pk_b}(v_2), \cdots, E_{pk_b}(v_n)$

Steps 3: Alice Decryption:

$$D_{sk_a}(E_{pk_b}(E_{pk_a}(v))) = E_{pk_b}(v)$$

For $i=1$ to n {

If $E_{pk_b}(v) = E_{pk_b}(v_i)$

Then $v=v_i$

Alice gets i

}

Alice may be gets the set{ $i_1, i_2, \cdots, i_k$ }   ($1 \le i_k \le n$)

Steps 4: Bob selects a random records sets is { $r(1), r(2), \cdots, r(n)$ },One random

record $r(i) = (a'_i, v'_i, b'_i)$,as show in table 1.

For $i=1$ to n {

Bob calculates :

$$rext(i) = ext(v_i) \oplus r(i) \; ;$$

as $rext(i) = (ra_i, rv_i, rb_i)$

Or as $ra_i = a_i \oplus a'_i$

$$rv_i = v_i \oplus v'_i$$

$$rb_i = b_i \oplus b'_i$$

}

Steps 5: Alice and Bob execute twice OT_n^k protocol together, the other OT_n^k

protocol:

Alice inputs { $i_1, i_2, \cdots, i_k$ }, Bob inputs { $rext(1), rext(2), \cdots, rext(n)$ }

Alice and Bob executes the OT_n^k protocol,

Alice obtains k data { $rext(i_1), rext(i_2), \cdots, rext(i_k)$ };

The another OT_n^k protocol:

Alice inputs { $i_1, i_2, \cdots, i_k$ }, Bob inputs { $r(1), r(2), \cdots, r(n)$ }

Alice and Bob executes the OT_n^k protocol,

Alice obtains { $r(i_1), r(i_2), \cdots, r(i_k)$ };

Steps 6: for $j = i_1$ to i_k {

Alice computes $ext(v_j) = rext(j) \oplus r(j)$

as $ext(v_j) = (a_j, v_j, b_j)$

Or as $a_j = ra_j \oplus a_j'$

$v_j = rv_j \oplus v_j'$

$b_j = rb_j \oplus b_j'$

}

The sets { $ext(v_{i_1}), ext(v_{i_2}), \cdots, ext(v_{i_k})$ } is the information that the user inquires.

After that, Alice only gets the record contains attribute values v, but don't know the other information of the relation table in database; Meanwhile, Bob also don't know what Alice gets.

4 The Performance Analysis of the Protocol

We analysis the correctness, the security and the complexity of protocol as follows.

4.1 Correctness

In our protocol, we used commutative encryption function to encrypt user query v and the attribute values v_i of the database relational table. Comparing cipher-text by encrypted with the query attribute values, and finally we can gets records information through executes two OT_n^k protocol.

We can see the user will be get the information that he want to query, so the query results of the protocol is correct.

4.2 Security

Theorem 1. The user's private information is not leaked.

Proof: Firstly, Alice encrypted property value *v* with the public key pk_a and sends it to Bob. Because the public key pk_a is public, the private key sk_a is secret, Bob can not decrypt, so he can not get any information about the values *v* .

Secondly, Alice and Bob executes two OT_n^k protocol together, the security of OT_n^k protocol means: After the end of the OT_n^k ,except the messages which he or she chooses, the receiver can not get any other messages. Meanwhile, the sender does not know what messages the receiver received.

As mention above, the user's private information is not leaked.

Theorem 2. The database's information is not leaked except the user's query information.

Proof: Firstly, Bob encrypt $E_{pk_a}(v)$ and the attribute value v_i with the public key pk_b ,and sends $E_{pk_b}(E_{pk_a}(v))$ and $E_{pk_b}(v_i)$ to Alice. Because the public key is public, the private key is secret, Alice can not decrypt, so can not get any other information about the value v_i .

Secondly, Alice and Bob execute two OT_n^k protocol together, The security of OT_n^k protocol is analyzed above.

As mention above, our protocol can protect the security of database, because the database's information is not leaked except the user's query information.

4.3   Complexity

Computation complexity analysis: The efficiency of OT_n^k in literature[6] is better than others, so our protocol is also efficient. If *n* is the number of database's records, *m* is the number of database's fields. Alice executes encryption operation once and decryption operation one times, Bob executes *n*+1 times encryption operation, so this protocol needs to *n*+3 times operation. Comparison with encrypted the whole database in the literature[3], our protocol only to encrypted attribute value that the user will query, and the costs of encryption is relatively small. Comparison of the complexity of computer as shown in Table 2.

Communication complexity analysis: In step1, Alice sends $E_{pk_a}(v)$ to Bob, they needs communicates one times.During step2, Bob sends $E_{pk_b}(E_{pk_a}(v))$, $E_{pk_b}(v_1)$, $E_{pk_b}(v_2)$,···, $E_{pk_b}(v_n)$ to Alice, therefore they need communicate once. In order to get 2*k* data, Alice and Bob collaborate to achieve two times OT_n^k in step5, They need to communicate 4 times each other. As mention above, the total times of communications are 6.

From the above analysis, we can see the protocol is secure and efficient.

Table 2. Comparison of computational complexity of the protocol

protocok	Computation complexity
Jing weiwei[3]	$mn+3n+3$
This paper	$n+3$

5   Conclusion

Based on cryptographic algorithms and OT_n^k, we designed a secure query protocol, which effectively solves the problem of the secure query from database without the third part. We analyzed the accuracy, security and complexity of the protocol. The results of analysis show that this protocol is secure and efficient. For further research, we will make efforts to achieve a more secure and more effective secure query protocol under the condition of a malicious model.

References

1. Yao, A.C.: Protocols for Secure Computations. In: Proceedings of the 23th Annual IEEE Symposium on Foundations of Computer Science, pp. 160–164 (1982)
2. Agrawal, R., Evfimievski, A., Srikant, R.: Information sharing across private database. In: ACM SIGMOD Int'l Conf. On Management of Data, San Diego, California (June 2003)
3. Jing, W.-W., Huang, L.-S., Luo, Y.-L., et al.: Design and Realization of Secure Query Scheme. Chinese Journal of Computer Engineering 22(32), 144–145 (2006)
4. Yuan, Y., Liu, G.-H., Zhang, Y., Li, -Y., et al.: Sensitive Information Retrieval Method with Minimal Information Sharing. Chinese Journal of Computer Engineering 16(35), 39–41 (2009)
5. He, J., Li, L.-J., Li, X.-M., et al.: Secret Sharing Scheme Based on Commutative Encryption Function. Chinese Journal of Computer Engineering 9(36), 159–160 (2010)
6. Chu, C.-K., Tzeng, W.-G.: Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries. In: Vaudenay, S. (ed.) PKC 2005. LNCS, vol. 3386, pp. 172–183. Springer, Heidelberg (2005)

A Novel Model of Large-Scale Distributed and Hybrid Search and Location[*]

Jianying Chen

College of Computer Science & Technology, Southwest University for Nationalities,
Chengdu, China
`uestccjy@tom.com`

Abstract. To address the centralized index bottleneck of large scale distributed system, a hybrid overlay network with redundant super nodes is established. It includes a local hierarchical sub network composed of District/Site/Node and a super nodes network composed of peer-to-peer District nodes. Based on it, a corresponding hybrid search and location model is put forward. In this model, search and location in system is separated into two levels: the top level is among super nodes and the destination Districts can be located based on DHT (Distributed and Hash Table); another is intra-District and the destination Sites or Nodes can be located by employing back trace and index. Comparison and analysis illustrate that this model can achieve higher reliability, availability, load balancing and location efficiency than similar models in existence.

Keywords: large-scale distributed system, hybrid overlay network, search and location, back trace, DHT.

1   Introduction

The first and most important work of Large-Scale Distributed System (LSDS) is efficient search and location model design. The existent search or location models mainly focus on Grid[1], CDN[2] and P2P[3]. Most of them are implemented by establishing overlay network supporting efficient routing or improving existing search or location algorithms. By motivation of making use of advantages each other, more and more of LSDS adopt hybrid overlay network with super nodes. These systems always include two layers: the top layer is Super-Node P2P Network (SPN), which is composed of nodes with better performance and mainly responsible for resources indexing, message routing and transmitting; the next layer is composed of many Local Hierarchical Networks (LHNs) organized by the rest common nodes and managed by one super node respectively. The layer's number of LHN can be given beforehand or adjust in running time[4-7]. Meanwhile, LHNs thinking of topology or user search interesting can achieve further benefit of search and location efficiency[5,8]. However, the problem of system reliability and availability caused by single super

node design is evident. Moreover, the resources index transfer and network topology reconstruction become mostly factors on service performance of LSDS.

To share in index storage and management of super nodes, reduce access load and avoid single node failure, a hybrid overlay network based on District/Site/Node tri-layer LHN with redundant super nodes is established and a novel corresponding model named Large-Scale Distributed Hybrid Search and Location (LDHSL) is put forward. Comparison and analysis indicate that LSDS is more reliable, available as well as higher search and location efficiency.

2   The Hybrid Overlay Network Model

Figure 1 is the hybrid overlay network model based on tri-layers hierarchies District/Site/Node and peer to peer in Districts layer.
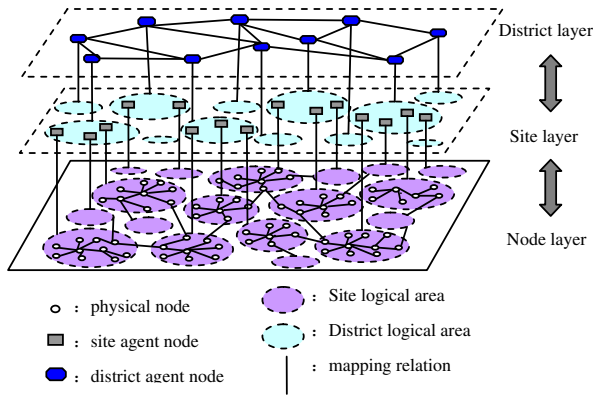
Fig. 1. The sketch map of hybrid overlay network

"District" and "Site" here are same as super and hypo-super node respectively. Thus, the District layer is SPN and all nodes belong to each District can make up of tri-layer hierarchical LHN. This model can commendably solve the scale problem of LSDS. For instance, even if a LSDS with 10^6 nodes and the biggest capacity of each District and Site is 50 as well as the average load of each node is 50%, then the nodes of SPN is only 1600. Consequently, the search and location can be handled even in SPN layer.In order to describe expediently, we differentiate the tri-layer nodes as follows:

Resource Storage Node (RSN): nodes in Node layer and mainly take charge to store resources, manage and publish local resources' index. RSN is also the entrance of search. When it receives a search query, it becomes the search agent (SA) of the query. Some RSN with close relation can organize a Sit.

Site Agent Node (SAN): node configured specially or selected from RSN according to their integrated performance (such as online time, network bandwidth, etc.). It mainly manage and publish resources in local Site. Many SAN with close relation can organize one District.

District Agent Node (DAN): node configured specially or selected from SAN according to their integrated performance. It mainly manages nodes and resources in its District. At the same time, it must manage and maintain the index distribution in DANs, transmit query message and route in DAN layer.

3   Search and Location Model Based on Large-Scale Distributed System

Based on figure 1, the search and location model is composed of two layers: one is in LHN witch is based on design of "back trace + index", the other one is SPN witch is based on DHT.

3.1   Search and Location Based on Back Trace and Index

3.1.1   Search and Location Based on Back Trace in Local District

A tri-layer solution space tree can be constructed by LHN. The search constraint is defined as a node with required resources and corresponding QoS. Search path advances according to "the initial RSN→its Site→its District→destination Site→destination RSN". This search will stop when one or more an appropriate nodes is met.

For example, the solution space tree shown in figure 2(a) has District A, Site B and C as well as RSN D, E, F, G and H. When a query comes, a RSN becomes Search Agent (SA) and the search begins from this SA. As shown in figure 2(b), the search path from node D must be one of the following four ways:

District layer

Site layer

Node layser

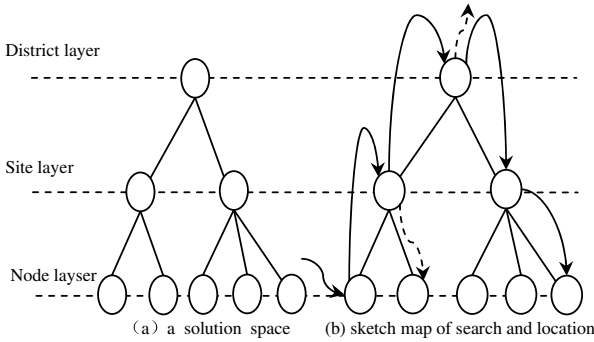(a) a solution space   (b) sketch map of search and location

Fig. 2. The sketch map of search in District based on back trace

a) D: the destination node is D;
b) D→B→E: the destination node is E in local Site;
c) D→B→A→other District: the destination node is not in local District and need search in the top layer SPN
d) D→B→A→C→H: the destination node is in local District and finally locate node H in Site C.

3.1.2   Location Mode Based on Hierarchical Index in Local District

Destination node in local District can be found by hierarchical index as figure 3. Each symbol is explained as follows:
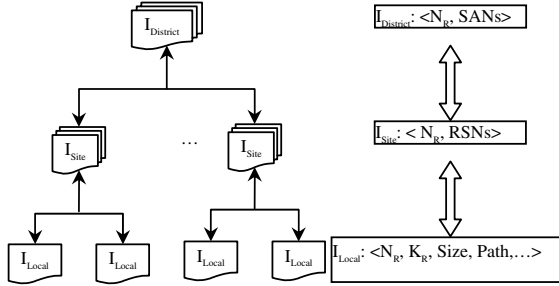

Fig. 3. Sketch map of location In local District based on hierarchical index

I_{Local}、I_{Site}和$I_{District}$: Respectively represent resources index of local RSN, RSN distribution in local Site and Site distribution in local District;

N_R (Resource Name): name or representation keywords of resource;

K_R (Resource Kind: the type of resource;

Size: the size of resource;

Path: the local path of resource;

RSNs: the RSN distribution of resources in local Site;

SANs: the SAN distribution of resources in local District;

…: other information, such as QoS information of node load, bandwidth, etc.

3.2   Search and Location in Districts Based on DHT

Our model is improved on Chord as follows:

a)   The Chord logical ring sort ascending by Hash value of District name and each District has a group of redundant DANs;

b)   MD5 is selected as Hash function and the distribution information in Districts of N_R is synchronized to redundant DANs according to Chord protocol;

c)   Add information of redundant DANs in routing table and the new routing table is Finger Table<Start, Interval, Successor, Backup-of -Successor>, in witch:

Start: Sort ascending D_x pointed in Finger Table computed. Here, x is computed as following formula:

x=(Hash(name of local District)+2^i) mod 2^{128}

Interval: The cyclic Hash interval, [(D_x+2^i) mod 2^{128}, (D_x+2^{i+1}) mod 2^{128}), used to index distribution and location in DANs

Successor: The successor District ID;

Backup-of-Successor: Set of redundant DANs in Successor, including node IP, loads and other necessary assistant location information.

d) Chord protocol is adopted in search course in Districts. At first, the corresponding District is selected according to hash mapping value of N_R, then the destination District with lightest loads can be found from Backup-of-Successor of this District.

e) District drops out only when all redundant DANs are failure and new DANs have not put forward.

3.3   Algorithm of Whole Search and Location

The whole search and location will be initiated by certain RSN when this RSN receives a query about N_R. The algorithm is described as follows:

Query in I_{Local} at first. If there is satisfied N_R, the path of N_R in local RSN will be returned, otherwise, the algorithm is ended;

Query in local I_{Site}. Transmit this query to the least loads RSN in local Site when N_R is existent and turn to step ① next;

Query in local $I_{District}$. Transmit this query to the least loads SAN in local District when N_R is existent and Turn to step ② next;

Locate the destination District of N_R based on DHT. If successful, transmit this query to destination District and algorithm ends. Otherwise, return NULL as search and location result. Algorithm ends.

4   Comparison and Analyses of Performance

This section, the advantages of LDHSL is illustrate by the following comparisons and analyses.

4.1   Routing Performance and Loads of SPN

As shown in table 1, two similar overlay networks based on index model, IS-P2P[4] and TAC[5], are selected to compare with our system.

Table 1. Comparison of routing performance and loads among IS-P2P, TAC and LDHSL

name of system	length of search path	sum of routing states	sum of average index	sum of average message
IS-Chord	$\log_2(N/M)$	$\log_2(N/M)$	$L \cdot N \cdot r/M$	$q \cdot N \cdot h/M$
IS-CAN	$d \cdot (N/M)^{1/d}$	$2 \cdot d$	$L \cdot N \cdot r/M$	$q \cdot N \cdot h/M$
IS-Pastry	$\log_b(N/M)$	$b \cdot \log_b(N/M)+b$	$L \cdot N \cdot r/M$	$q \cdot N \cdot h/M$
IS-Tapestry	$\log_b(N/M)$	$\log_b(N/M)$	$L \cdot N \cdot r/M$	$q \cdot N \cdot h/M$
TAC	$\log_2(N/M^2)+2$	$\log_2(N/M^2)$	$L \cdot N \cdot r/M$	$q \cdot N \cdot (1-\beta) \cdot h/M$
LDHSL	$\log_2(N/M^2)+2$	$\log_2[(N/M^2) \cdot R]$	$L \cdot N \cdot \sqrt{r}/M$	$q \cdot N \cdot (1-\beta)^2 \cdot h/M/R$

The meaning of parameter in table is as follows:

N: sum of nodes in system;
b: base of identifier;
M: ratio of nodes' sum from upper layer and lower layer;
L: total number of resources provided by each node;

d: spatial dimensions of IS-CAN;

r: the average redundancy number of resources in each layer (r≥1);

q: average query speed of each node;

R: the average redundancy number of DANs in LDHSL (1≤R≤M);

β: the average ratio of query handling in index nodes of each layer (0≤β≤1).

Results in table 1 illustrate that, in condition of N and M are same in every system:

a) The length of search path in LDHSL is equal to TAC but less than IS-Chord, witch is the shortest path system in IS-P2P. Therefore, routing performance can be improved only when capacity of node in LDHSL is more than 4.

b) The average sum of index in LDHSL node is $1/\sqrt{r}$ of IS-P2P and TAC. Because r≥1, this illustrate the costs on index storage of DAN is relatively smaller than the other system.

c) In condition of same length of search path, the message transmitting loads is smallest among three systems. It is only $(1-\beta)^2$/R of IS-2P and $(1-\beta)$/R of TAC in LDHSL Because the following expression:

$$(1-\beta)^2 \leq (1-\beta)/R \leq 1/R \leq 1$$

d) Because two expression as follows:

$$\log_2[(N/M^2) \cdot R] \geq \log_2(N/M^2)$$

$$\log[(N/M^2) \cdot R] = \log(N/M) \cdot (R/M) \leq \log(N/M)$$

It is evident that the sum of routing states is between TAC and IS-P2P. It is equal to TAC when R=1 and degenerates as IS-P2P.

From comparison and analyses above, the routing performance, index storage and network loads of LDHSL have more evident advantages than the two similar system.

4.2   Analyses on Load Balancing

The load balance of LDHSL is various:

a) The load balancing among Districts comes from the balance of Hash function MD5;

b) The load balancing of redundant DANs in one District comes from the loads information in Finger table. By loads information in this table, the search queries can be almost distributed evenly among all DANs in same District.

c) The load balancing of redundant SANs in one Site comes from the search and location algorithm. This is because the search agent always selects the SAN with the smallest load to transmit current query in the algorithm.

4.3   Analyses on Reliability and Availability

The redundant DANs reduce the probability of District failure and thus enhance the reliability and availability of search and location in SPN. Furthermore, search and location in District is based on back trace method and it can be handled at every hierarchical nodes. Thus, redundant DANs and SANs can efficiently guarantee the integrality of search on the solution space tree. Thereby, the high reliability and availability of search in District can be achieved.

5   Conclusion

To avoid the bottle neck of super nodes in large-scale distributed system efficiently, a novel hybrid overlay network with redundant super nodes is constructed and based on it, a hybrid search and location model based on "back trace and index" in local hierarchical network and DHT in top super nodes network is put forward and described in detail. In this model, large number of search and location query can be handled in local hierarchical network, only small amounts of query must transmit to top super nodes layer. Comparison and analyses with similar system illustrate the novel model can achieve higher routing efficiency, more reliable and available, better load balancing and lower network loads.

References

[1] Jiménez, Á.B., Lázaro, J.L., Dorronsoro, J.R.: Finding Optimal Model Parameters by Discrete Grid Search. Innovations in Hybrid Intelligent Systems Advances in Soft Computing 44/2007, 120–127 (2007)
[2] Mulerikkal, J.P., Khalil, I.: RMIT Univ., Melbourne. An Architecture for Distributed Content Delivery Network. In: 15th IEEE International Conference on Networks, pp. 359–364 (2007)
[3] Ghamri-Doudane, S., Agoulmine, N.: Enhanced DHT-based P2P Architecture for Effective Resource Discovery and Management. Journal of Network and Systems Management 15(3), 335–354
[4] Xia, Q.-Z., Xie, G.-G., Min, Y.-H., et al.: IS-P2P: Index-Based Structured P2P Networks. Chinese Journal of Computer 29(4), 602–610 (2006)
[5] Li, J.-F., Zhou, X.-M., Zhang, C.-X.: Peer-to-Peer Network Model with Three-tier Topology Based on Auto Clustering. Computer Science 36(2), 66–69 (2009)
[6] Feng, J.-X., Chen, G.-H., Xie, J.-Y.: Hierarchical and Ordered P2P Super2peer Topology Construction. Computer Science 36(10), 131–217 (2009)
[7] Trana, D.A., Nguyen, T.: Hierarchical multidimensional search in peer-to-peer networks. Computer Communications 31(2), 346–357 (2008)
[8] Li, Z., Mohapaira, P.: The impact of topology on overlay routing service. In: IEEE INFOCOM (2004),
     http://spirit.cs.ucdavis.edu/ pubs/conf/infocom04b.pdf

The Exploration of Mainstream VPN Technologies in Campus Network

Yao Bao, Wenjin Tian, and Zhiyuan Du

Hubei Meidcal University
Shiyan, Hubei, 442000, P.R.C
Boil1988@hotmail.com

Abstract. This article introduces the principle of IPSec VPN and SSL VPN, compares and analyzes the security, complexity and scalability of these two kinds of VPN technologies. Summarizes the advantages and disadvantages, points out their applicable fields. On this basis, we analyze the model that the users use the digital campus network while the campus network as application environment, and then we conclude that it is feasible to construct VPN which based on both SSL and IPSec protocols.

Keywords: SSL, IPSec, Smart Card, digital campus, MPLS.

1   Introduction

With the rapid development and popularization of the Internet, Digital Campus construction is in full swing, the colleges regard campus network as its basic communicational platform. As the campus scale expanding then it appears such problem: huge data flow, remote education, access network off-campus, in the entire traditional campus network already cannot meet the requirement of the developing universities. Now how to make data transmission more efficient, data exchange low-cost and resources more secure in the highly shared campus network environment. And also how to manage all the campuses in logical integration. There are so many campus network problems we should be faced. So in this case, the VPN becomes the first choice in campus network expansion and development. These problems should be faced in digital campus constructions. So in this case, the VPN in the digital campus is an important part of the construction.

2   VPN Technology

VPN (virtual private network) technology is the virtual private network technology, which connects remote branches, business partners and mobile officers, etc by an open public network resources and provides them end-to-end security data transmission, VPN can handle their own information through the public Internet as the same with leased line. So we can construct different kinds of VPN According to different application environment. Always VPN has three kinds of solutions: Access VPN, the enterprise Intranet VPN and Extranet VPN.

At present, there are three kinds of VPN technologies already used, which includes IPSec VPN, SSL VPN and MPLS VPN. These VPN technologies have their own characteristics and strengths. Now overseas manufacturers take more seriously in MPLS VPN and SSL VPN technology. But the IPSec VPN is still the most widespread used and matures technology.

2.1   IPSec VPN Technology

Because the IP packets are lacking in security, ITEF puts forward IPSec. IPSec (IP Security) is the standard that protects IP secure communication; it mainly authenticates and encrypts IP protocol group. IPSec encrypts and authenticates the data in the network layer, provides end-to-end network security plan such as access control, data source confirmation, the holistic confirmation of connectionless data, data content confidentiality, the replay protection as well as data stream confidentiality, etc.

The services IPSec provided is transparent and safe to upper protocol and application process, many kinds of protocols and application procedures may share the IP layer safe service and key management, so they do not need to design and realize their own safety mechanism, thus it can reduce expense of key consultation and lower security possibilities. Therefore IPSec is the most general method to provide security in Internet.

As a protocol family (series of interrelated protocols), IPSec composes of following components: Some protocols that protect packet stream; Protocols that establish Key exchange for packet stream.

The former contains two parts: Encapsulating Security Payload (ESP) and Authentication Header (AH). ESP provides Confidentiality for the original data, AH provides Authentication for packet stream and ensures information integrity.

IPSec VPN works similar to Packet Filter Firewall. When the CPE (Customer Premise Equipment) A receives an IP packet, it queries the SPD (security policy database) to decide whether forward the packet to the CPE B or not. It executes IPSec processing if required, this processing includes encrypting the data packets and encapsulating the packets into another ones. So that the packets are sent to CPE B through the network, when CPE B receives the data packets it requires decryption and decapsulation.

Of course in the processing procedure, if the newly generated packet is bigger than the MTU (Maximum Transfer Unit), it needs additional subcontractors and packages between the CPE A and CPE B.

2.2   SSL VPN

SSL is a protocol to solve the security of web-based application which proposed by Netscape, SSL protocol provides security of data-link between Web service (HTTP) and TCP / IP. It provides data encryption, server authentication and message integrity verification for TCP / IP links.

SSL includes two layers: SSL Record Protocol; It is built on a reliable transport protocol (such as TCP) to provide data encapsulation, compression, encryption and other basic support for upper protocols. SSL handshake protocol; It is built on SSL Record Protocol and used to authenticate the two sides, negotiate encryption algorithm, exchange encryption keys and so on before the start of the actual data transmission.

The workflow of SSL as below:

I. Server authentication phase:

i. Client sends a start message "Hello" to the server to start a new session connection;

ii. Server determines whether need to generate a new main key, if necessary, the server responses the information with new key inside to customer;

iii. Customer generates a main key based on information received from the server, and then return the key to server that encrypted by the public key;

iv. Server gets back the main key, and returns client authentication information with the main key in order to make client complete authenticating server.

II. User authentication phase: Until the server has passed through the client authentication, it is turn to authenticate client. The authentication server sends a question to customers, customer returns signature of the questions and their public keys to the server.

SSL VPN gateway is the agency during the communication. When users request to visit server, the information have not been directly to the application server but received by SSL VPN gateway. The data is first analyzed by the SSL VPN agency, then it executes identification, authentication and access control for security policy, and last it converts the data to proper protocols and sent it to application server.

2.3   Comparison of IPSec and SSL VPN

While in application, IPSec works in network layer, it protects all the data that transmits among correspondence. Usually IPSec VPN is suitable for all application procedure; it also makes remote users feel the same with local users when accessing local resources. But SSL locates at the socket layer, it has close relation with the application layer, which can only visit these resources that supported by SSL or the WEB browser. Therefore, its application filed is mainly consisted of e-mail system, file sharing and the Web application procedure.

While in security, IPSec VPN and SSL VPN strengthen its security through authentication and encryption. It has the direct relationship between IPSec VPN authentications and strategy of the network equipment, network parameter and equipment's IP address, etc. That's quite safe to the long-distance connection. In SSL VPN, the user may login in depending on its willing and judge the server certification by itself whether effective or not. IPSec VPN uses the more complex encryption algorithm, longer key than SSL VPN. But IPSec VPN generally only provides the encryption in gateway, no encryption between the application server and gateway. SSL VPN provides the end-to-end encryption.

While in extendibility, IPSec VPN is based on network layer, which has nothing to do with the application procedure. The enterprise could revise application procedure at its willing without modifying VPN. However, due to the very requirements of its clients, which makes it relatively trouble while adding new users. SSLVPN serves for the application layer, therefore changing application program means changing the interface of VPN, and moreover not all application programs may use the Web way to visit. If increasing a Web server as the proxy before many non-Web application procedures, it will cause Web server the overloaded. And last it will lead to system performance degradation.

While in the usage complexity, Because IPSec works in network layer, IPSec VPN clients for remote access is not easy to achieve, configure and maintain. For SSL VPN, it works among TCP and various application-layer protocols, and SSL also is embedded in web-browsers. So business based on B/S can directly use the browser to establish SSL VPN connection without installing clients.

3   Application of VPN Technology in the Campus Network

3.1   The Conception of Dital Campus

Digital Campus is based on campus network, relied on advanced management concepts, use advanced IT methods and tools, integrate existing teaching, research, management, life, service and other related resources and to achieve reunification, user management, resource management and access control; It is aimed at achieving efficient allocation of resources, full utilization of the school management and optimizing logistics services, and building a new mode of education, expanding the real dimensions of time and space in campus, providing online information exchange environment for students and teachers, creating e-school and educational resources, virtual communities and network services, digital and virtual university educational environment, and ultimately the overall educational process information, so as to improve teaching.

3.2   Problems and Solutions in Smart Card System of Digital Campus

As a part of digital campus, "The Smart card System" has already penetrated into many corners of university, this is the trend of university informationization and the symbol of university modern management.

Smart card system integrates its own function and computer network, then creates a integration among traditional relatively independent school roll administration, library, computer management, access control discrepancy, identity authentication, consumption and settlement etc, last realizes unified management and integrated resources. However, smart card system still exists some bottleneck problems, these problems are mainly:

Campus Information Island. The mergence and enrollment of University, make each school has established numerous campuses, these campuses are often trans-regional. While these campuses have not realized the inter-communication in network. This makes a card cannot spanned "tong" problem and students in different campuses have to use different smart cards. This is not only inconvenient, but also a waste of resources.

For some reason, Information transmitted in Smart card is not encrypted, so it's easy to be forged. In theory, the card itself is a strong password medium; it is not easy to be forged. However, coupled with the openness of campus network, an attacker can easily steal data and reproduce a legitimate smart card through vacant record cards, and it can cause losses to the card user.

Fortunately, in the above figures of the campus smart card business, we found that it is a good solution to use both IPSec and SSL VPN integration to solve the inherent problems.

Multiple smart cards sites connect through the IPSec VPN. We can access card management areas through the security certification, establishment of tunnel, encryption and other mechanisms of transmission. This mode builds mutual trust and the security of encrypted information between the transmission channels so as to achieve the effect of private network. At the same time, also enables application-layer access control filtering.

There are many different types of card reader terminals in campus, and some is based on the computer terminal platform, and some are dedicated reader devices. We can use SSL VPN to encrypt transmission for the computer terminal device. As long as they can use the browser's terminal equipment, we can use the SSL protocol to establish a secure, encrypted transmission channel. For the dedicated reader device, you can access the network using the PPTN, etc.

4   Summary

In solving the interconnection and the remote security access, both IPSEC VPN and SSL VPN have the respective good and bad points. Users will face these two problems in its own developing process, if using the sole VPN solution, it will exposure its own shortcomings gradually. So in this case, IP Sec VPN is deployed to be as general remote access solution and point-to-point collecting solution, with auxiliary SSL VPN deployed as remote access solution for Web visiting service. At the same time another VPN technology MPLS VPN has matured, it can be very simple to realize the horizontal and vertical visitations among school departments and does not require the configuration when adding a new node. So MPLS VPN technology has a very good set of maintainability and scalability. He is also more suitable for formatting complex and large-scale VPN networks. Although this kind of technology has not been popular in the current buildings, with the development of times, it will make a great contribution to the digital campus.

References

1. Krywaniuk, A.: Security properties of the IPSec protocol suite (2002)
2. Port Randomized VPN by Mobile Codes. IEEE (2004)
3. Lihong, He, C.: The comparison and application of mainstream VPN technology. Technology Forum (2010)
4. Qiu, J.: The Application of IPSec Based Technology in Campus Network (February 2010), http://www.cqvip.com/
5. Zhao, C., Lufei: Scratch the Surface of VPN technologies integration. GanSu Science and Technology (July 2010)
6. Yi, G., Fu, G., inZhou, X.: The Research and comparision of MPLS VPN, IPSec VPN and SSL VPN. Guizhou Science (June 2007)
7. Li, Q., Liu, X.: The Research of VPN in Enterprise network. Compeer Knowledge and Technology 1.6(19), 5232–5233 (2010)

A Novel ZigBee Keyboards with Mobile Ad Hoc Network

Wu Lei[*]

College of Inf., North China Univ. of Tech., Beijing, China, 100144
stone.wu@ncut.edu.cn

Abstract. This paper gives a solution of wireless keyboards with mobile Ad-hoc network (a mobile, multi-hop and autonomous decentralized system) without fixed infrastructure, which is a novel technology about establishing a mobile Ad-hoc network.

Keywords: ZigBee, Coordinator, Node, Ad-hoc network, USB, PS/2.

1 Brief

With development of radio communication, demands for portable devices are increasing day by day and wireless keyboards become a new trend. Especially, keyboards with mobile Ad-hoc network is interested by more and more young people when they play games.

2 The Wireless Architecture of Keyboard with Zigbee

The wireless keyboard normally consists of two parts: the ZigBee Keyboard Sender (Sender for short) and the ZigBee Keyboard Receiver (Receiver for short). The wireless scheme of keyboard with ZigBee is presented in Fig.1 the Receiver and the Sender are both built-in JN5121model (from Jennic company) based on ZigBee protocol.

Fig. 1. Block schematic of ZigBee Keyboard

3 The Scheme of Zigbee Keyboards with Mobile Ad-Hoc Network

With three Receivers (also called End Device or Node, here reference computer receiver built in ZigBee module) and corresponding three Senders (here reference keyboard with ZigBee module), we built a simple prototype of mobile Ad-hoc network,

---

[*] Associate Professor, Master Instructor, the main research & interests areas: Embedded system and technology, especially the application of Embedded, Zigbee system and technology, especially the application of Zigbee, wireless sensor network.

which can establish the truth of four schemes: one peer to one peer, one peer to multi-peer, multi-peer to one peer and multi-peer to multi-peer mobile Ad-hoc network, which is shown as in Fig. 2.
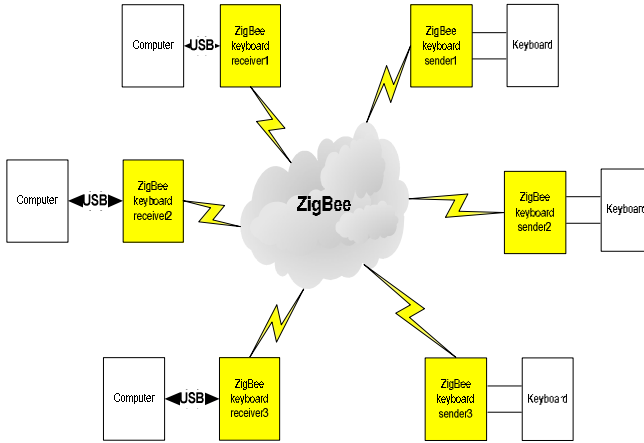

Fig. 2. Multi-peer to multi-peer scheme of keyboards with Ad-hoc keyboard network

4   The Way of ZigBee Binding

Binding mechanism is a key technology to build a mobile Ad-hoc network and also a kind of connection mechanism established among ZigBee nodes for fast and convenient exchange information. The binding mechanism is mainly realized through binding algorithm and binding table, which are mainly constituted by mobile Ad-hoc network address and the endpoint identity code.

There are two types of binding way. One is Direct binding, that binding table is preserved in Senders node, the other is indirect binding, that binding table is preserved in Coordinator node.

4.1   The Process of Direct Binding

1) First the sender endpoint (here called request point), is desired to transmit data, broadcast binding request to any other endpoint in the mobile Ad-hoc network.
2) Second an endpoint in mobile Ad-hoc network to respond the binding request by transmitting back message of ZigBee Device Profile (ZDP for short) only at the moment that the receiver endpoint discovered that this binding request data is matched with the receiver endpoint itself.
3) Third the request endpoint will store the receiver endpoint address in mobile Ad-hoc network and the identity code of receiver endpoint into the binding table only at the moment that the request endpoint discovered that the replied data of ZDP meets the requirement and is correctly.
4) If the other endpoints information has been stored in the binding table of the request endpoint, that means the direct binding is established among the request endpoint and

the another endpoints in the mobile Ad-hoc network, the request endpoint can directly mutually exchange data with each other endpoints by the binding table.

4.2   The Process of Indirect Binding

1) First the sender endpoint, is desired to transmit data, send binding request to Coordinator of the mobile Ad-hoc network.

2) Second Coordinator responds the binding request of the sender endpoint by transmitting back message of ZDP and stores the sender endpoint address in mobile Ad-hoc network and the identity code of Sender endpoint into the binding table.

3) The indirect binding is finished as soon as the request endpoint has correctly received reply message from Coordinator.

4) After indirect binding is established, each other endpoints in mobile Ad-hoc network can exchange data through Coordinator.

Wireless keyboard's Sender and Receiver built in ZigBee module make up the mobile Ad-hoc network, which network topology scheme is shown as Fig. 3.
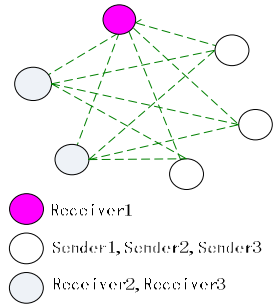

Fig. 3. Topology construction of the system

In Fig.3, Receiver1 plays the role of Coordinator and startups the network. Receiver2 and Receiver3 via USB interface to receive keyboard codes and exist as the role of the Router. Sender1, Sender2 and Sender3 connect with keyboard via PS/2 interface to send keyboard codes to binding Receiver and also plays the role of Router.

5   System Debug and Test Result

Debug and test by the following the three steps:

5.1   One Sender Transmit Vs. Multi-receivers Catch Information Respectively

Startup the Sender, message displayed on terminal of PC is as Fig.4 shown.

At startup, as the Fig.5 shown: the default receiver end is coordinator and the sender node is the Sender1.
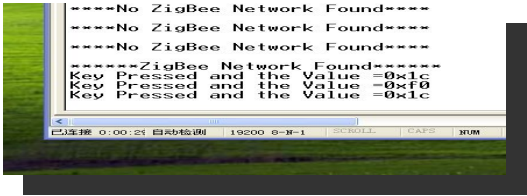
Fig. 4. Startup the Sender
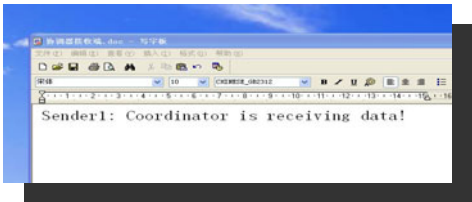
Fig. 5. At startup, sender1 transmit and coordinator receive

The first step is about only one Sender transmits data and the other multi-Receivers waits to be linked for getting information respectively.

The process of exchanging data between one peer to multi-peers is as following:

1)   Pressing the switch1, that means launch the Sender node 1 to send information and Receiver node 1 wait to be linked for getting information corresponding. The content on terminal of PC is shown as the Fig.6 and the situation of Sender node 1 send VS Receiver node 1 receive is shown as the Fig.7.
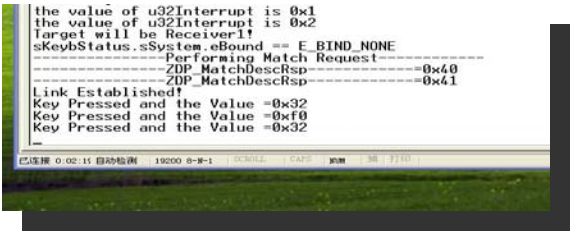
Fig. 6. Content on terminal of PC
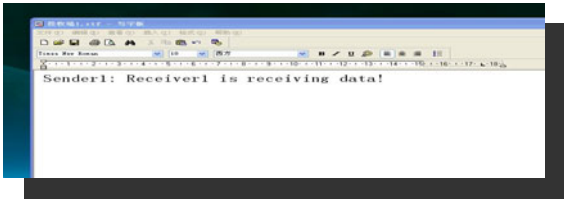
Fig. 7. Sender node 1 send VS Receiver node 1 receive

2) Pressing the same switch once again (the second time), that means launch the Sender node 1 to send and Receiver node 2 wait to be linked for getting information corresponding. The content on terminal of PC is shown as the Fig. 8 and the situation of Sender node 1 send VS Receiver node 2 receive is shown as the Fig. 9.

Fig. 8. Content on terminal of PC
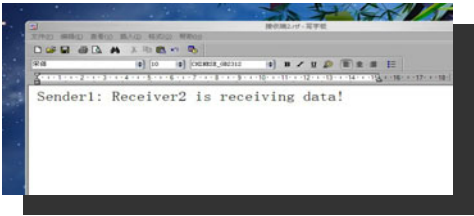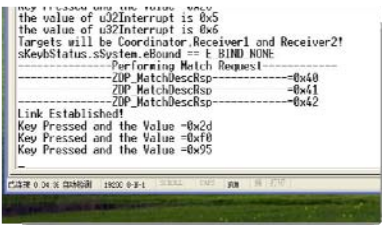
Fig. 9. Sender node 1 send VS Receiver node 2 receive

3) Pressing the same switch (the third time), that means launch the Sender node 1

Fig. 10. Content on terminal of PC

to send and Receiver node 3 (coordinator), Receiver node 1 and Receiver node 2 concurrent wait to be linked for getting information corresponding. The content on terminal of PC is shown as the Fig.10 and the situation of Sender node 1 send VS multi-Receivers nodes receive is shown as the Fig.11.
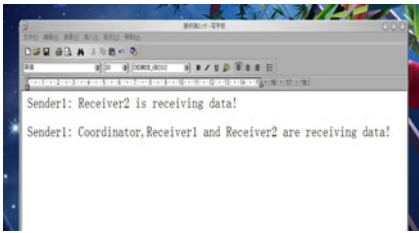
Fig. 11. Sender node 1 send VS multi-Receivers nodes receive

4)   Pressing the same switch (the fourth time), that means launch the Sender node 1 to send and Receiver node will be coordinator again is shown as the Fig.12., and next loop (is shown as the Fig.13) will be to start.

Fig. 12. Content on terminal of PC
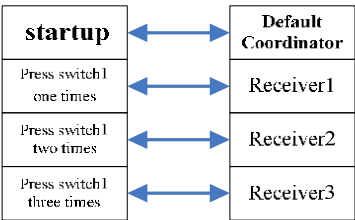
Fig. 13. Loop

In accordance with the above mentioned method, pressing number two switch with one time (two times, three times), that means launch the Sender node 2 to transmit dada, we need check the situation of Receiver node 1 (2, 3) to catch information respectively.

Within the same way, pressing the number three switch with one time (two times, three times), that means launch the Sender node 3 to transmit dada, we need check the situation of Receiver node 1 (2, 3) to catch information respectively.

And so on, a completing debug process about one Sender transmit VS multi-Receivers is reached.

5.2   Multi-senders Transmit Vs. One Receiver Catch Information Respectively

The second step is about multi-Senders transmit and only one Receiver wait to be linked for receiving information respectively is shown as the Fig.14. Under such circumstances of closing Receiver node 2 and Receiver node 3, we need only check the situation of Receiver node 1 gain data when pressing the switch 1, switch 2 and switch 3 concurrent. Similarly, check Receiver node 2 and Receiver node 3.

Fig. 14. Content on terminal of PC

5.3   Multi-senders Transmit Vs. Multi-receivers Catch Information Respectively

The third step is about while simultaneously pressing switch one, switch two and switch three, that means launch the Sender node 1, Sender node 2 and Sender node 3 simultaneously to send, Receiver node 1, Receiver node 2 and Receiver node 3 all wait to be linked for receiving information at random type is shown as the Fig.15.
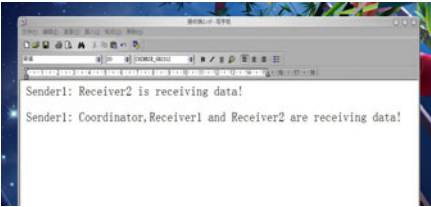
Fig. 15. Multi-Senders transmit VS multi-Receivers

Test is strictly by various settings and the results are satisfied after many months' executions.

References

1. ZigBee Application Development API Reference Manual JN-RM-2014 (December 10, 2006)
2. EZ-USB Xcelerator Development Kit. CYPRESS company

3. Wu, L.: The Realization of Keyboards with Mobile Ad-hoc Network. In: 2010 Second WRI Global Congress Systems, Wuhan, China, December 16-17, pp. 286–289. IEEE Computer Society, Los Alamitos (2010)
4. Ondrej, S., Zdenek, B., Petr, F., Ondrej, H.: ZigBee Technology and Device Design. In: Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, ICN/ICONS/MCL, April 23-29, p. 129 (2006)
5. Cox, D., Jovanov, E., Milenkovic, A.: Time synchronization for ZigBee networks. In: Proceedings of the Thirty-Seventh Southeastern Symposium on System Theory, SSST 2005, March 20-22, pp. 135–138 (2005)

An Open Platform for Earthquake Engineering Simulation in China

Ruizhi Wen, Bo Jin, Wei Chen, Xiangyu Jia, and Zhiyong Dai

Institute of Engineering Mechanics, China Earthquake Administration,
No.29 Xuefu Road, Harbin, 150080, China
`ruizhi@iem.net.cn`

Abstract. The architecture of an Open Platform for Earthquake Engineering Simulation (OPEES) is introduced. This project is sponsored by the Ministry of Finance, China, cost 30 million RMB during last five years. The various parts of the large platform are linked based on earthquake observation system, experiment systems, and theoretical research systems. The core equipment, 30 Teraflops parallel supercomputer and 200T storage array, are described. At last, 2 test cases, one seismic wave simulation and pseudo-dynamic test are used to verify the successful integration of OPEES.

Keywords: OPEES, Supercomputer, Storage, Test cases.

1   Introduction

In 2000, the U.S. National Science Foundation (NSF) invested more than 80 million U.S. dollars to integrate a network of cooperative experimental system (NEES). The NEES network infrastructure encompasses 1 management headquarter, 14 earthquake engineering and tsunami research facility sites located at universities across the U.S., available for testing on-site, in the field, or through telepresence and cyberinfrastructure operations ,the network connects, and the work of the experimental facilities, researchers, educators and students. Japan started to build the E-Defense since 2005 which is a full-size three-dimensional vibration destruction facility and is the largest in the world. The collaborative research between NEES and E-Defense focuses on tests and analyses to develop major experiments involving bridge columns and structures .This shaking table permits nearly full-size bridge models to be subjected to earthquakes as largely as any recorded one in Japan or in USA during the Kobe and Northridge earthquakes.

Since 2004, with the support of Chinese Natural Science Foundation, Institute of Engineering Mechanics, China Earthquake Administration (IEM/CEA), Tongji University, Hunan University and the other institutions had also launched basic researches for a collaborative network in experimental systems. China is one of the most countries hit by destructive earthquake and it is well known that large-scale experiments on Earthquake engineering is one of the most direct methods of verify the seismic capacity of various types of engineering structures.

In order to meet the challenge of high seismic activity in China, IEM/CEA proposed a project, Open Platform for Earthquake Engineering Simulation, to reduce

the impact of earthquake and to develop an active collaboration, a network center for plenty of researchers based on the development of information technology [1].

The goal of this project is effective integration of all kind of original earthquake related information and build an open platform which will serve for the earthquake engineering within China. This project has gotten sponsored from Ministry of Finance, China and the total fund is about 30 million RMB within 5 years. As the key involvers, this paper gives an introduction of the OPEES.

2   OPEES Architecture

The Open Platform for Earthquake Engineering Simulation(OPEES) was operated since 2004 and started to found in late April 2008. The Fig.1 shows there are three main components in the platform, the networked hardware environment, the numerical simulation and research, and the basic information repository. Architectural design explains the components within the open platform and how each component interacts with each other. This open platform will act as an operating system for earthquake engineering researches, trying to connect the facilities, data, information, knowledge and people together to this distributed networked platform. OPEES initiative will be a sample model for the networked hardware environment, and parallel computer which serves as the basis for the numerical simulation component, and data warehouse which can be expanded to serve as the basic information repository [2].

Under OPEES architecture, we design the hardware including the supercomputer and mega storage array. The OPEES Supercomputer consists of 384 nodes of HP ProLiant BL460c Blade Server,12 I/O node of HP Proliant DL380 G5and 8 management nodes of HP Proliant DL380 G5 and linked by Voltaire ISR 2012 Infiniband with 20T EMC CX3-80F Fibre Channel solution supporting HP blade servers. The theoretical CPU speed reaches 30 teraflops and have the ability to handle the earthquake engineering issue. The supercomputer also combines efficient compute power and high spatial density, with expanded memory for maximum performance.

Under OPEES architecture, we also design 3 layers software. The first layer is the Redhat Linux EL AS 4.0 U2 x6, a platform well-suited for a broad range of applications across the OPEES infrastructure and provides support for the new and existing applications. HP CMU is also installed as an efficient and robust tool for the management of Linux-based nodes in HPC clusters. The CMU simple graphic interface enables centralized console management, monitoring of cluster-wide and node-specific metrics, and software installation. And it is also easy for frequent changes to the software configuration across the cluster or on a subset of the cluster.

The second layer is the commercial parallel software which apply to the earthquake engineering simulation, such as ANSYS, ADINA and ABQUAS, and provides volume parallel capabilities to support multiple users, with complete flexibility to deploy the software wherever there are distributed resources. The parallel performance permits users to exploit the supercomputer systems using distributed parallel processing and offers parallel solver, which are improved iterative solver performance on many difficult large and complex earthquake engineering problems.

The third layer is the development and localization of series software to serve to physical remote control experiments and computational simulations, such as remote
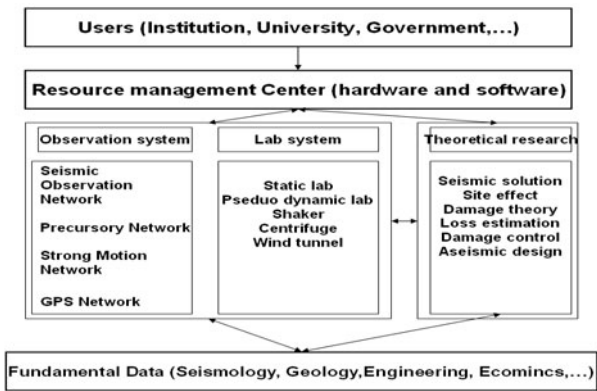
Fig. 1. OPEES components
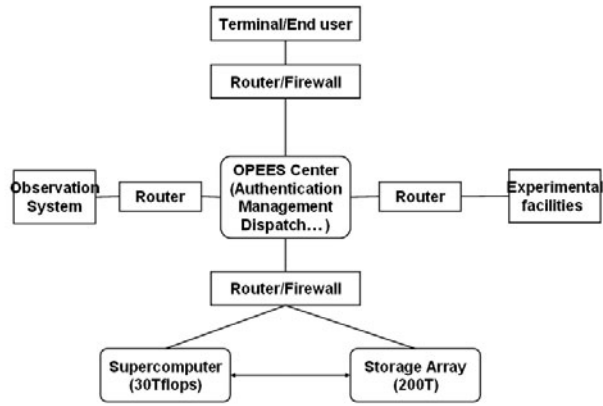
Fig. 2. OPEES hardware architecture

data collection, remote data storage, request management, real time data sharing, remote viewing and robotic control, etc. This prototype matches well with US NEES system so that the connection between China and US is available [3].

Fig. 3. 30 Teraflops supercomputer (left) and 200T storage (right)

3   Test Cases

Now the OPEES has the functionality of integrated data exchange, remote manipulation, high performance calculation, and multi-site collaboration within the networked environment. The following are two samples of the OPEES application.

3.1   Seismic Wave Propagation Simulation by Supercomputer

To model a cubic region 50km by 50km by 35km with 3 different material layers, and the simulations use 3240000 hexahedron finite elements with a spatial resolution 300m on a side, Fig. 5 and the material assumes the elastic rock layers .Due to the mesh size much less than the seismic wave length, wave propagation step is given 0.001s for 20s. Ricker wavelet used for control function as point seismic source and the epicenter is at the center of the cubic region. The central difference method is applied by the explicit algorithm. The CPU time costs for different CPU shows in Fig. 5 and implies the effective parallel computing .The visualization of the propagation simulation are in Fig.6 [4].
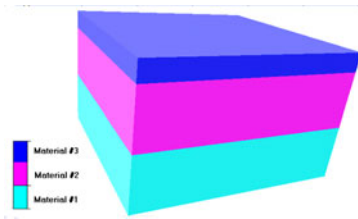
Fig. 4. Seismic wave simulation model   **Fig. 5.** CPU and time cost
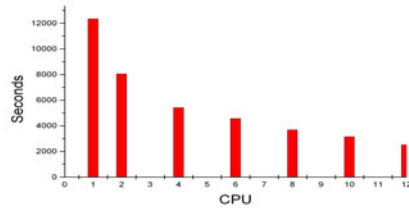
3.2   Pseudo-Dynamic Test between IEM and UIUC

This simple concrete frame in Fig. 7 applied for pseudo-dynamic test. In Fig. 8, the Multi-axial Full-scale Substructure Testing and Simulation (MUST-SIM) facility and the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign (UIUC) is linked by OPEES located in IEM/CEA, Fig.8.

The MUST-SIM and NCSA provides a total testing-analysis-visualization-display environment under complex loading and boundary conditions. When the IEM server receives a propose request, it validates the request, creates a new object to represent the proposed transaction and calls propose method. This method should return true if all site-specific conditions for accepting a proposed transaction are met, and false otherwise. For each pseudo-dynamic test, it needs 6 times data exchange, Fig.9. [5][6][7].
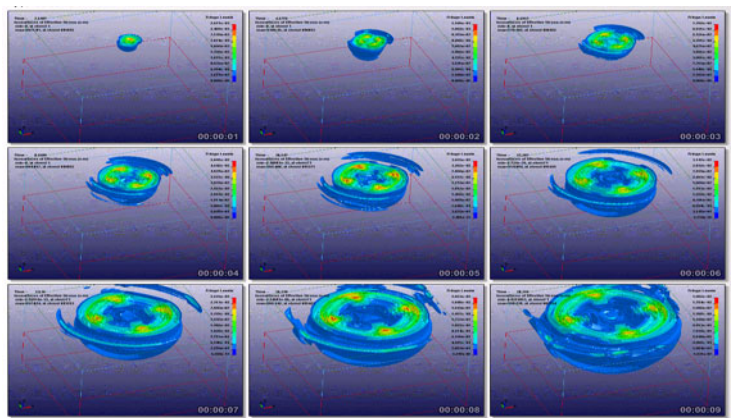
Fig. 6. Seismic wave propagation simulation by point source
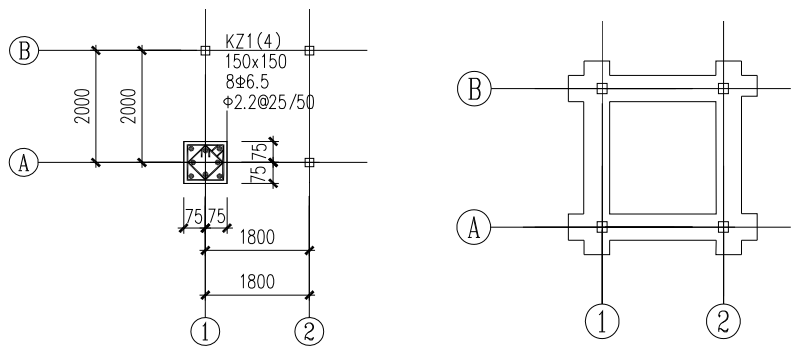
Fig. 7. Simple concrete frame model
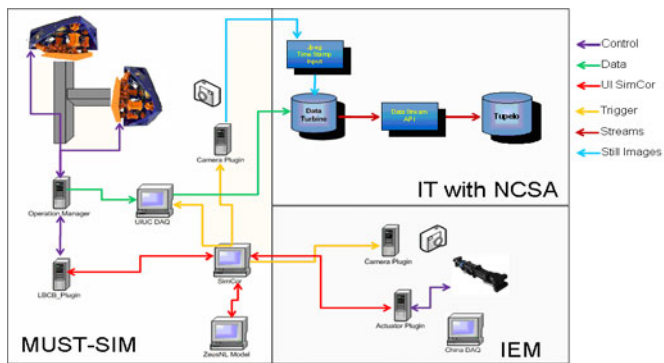
Fig. 8. Chart for pesduo-dynamic Test
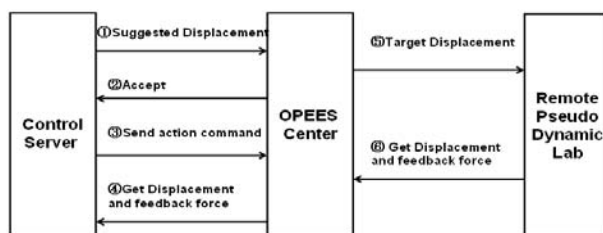
Fig. 9. Control command flowchart

4   Conclusion

In this paper, OPEES project has been introduced and the framework of this system has been tested and the results show the architecture could serve the earthquake engineering well. The infrastructure will soon link earthquake engineering sites across the country, provide data storage facilities and repositories, and offer access to high-performance computing applications used for conducting simulations. In the next 5-year plan, this center will also expand the services for earthquake early warning system, which is another key project for China earthquake mitigation.

References

1. Ru, J., Xiao, Y.: The American Plan of Network for Earthquake Engineering Simulation and the Idea of Realization of Long-distance Coordinative Structural Experiment in China. Journal Of Building Structures 23, 62–67 (2002)
2. Wang, Z.: An open platform for simulation of earthquake engineering damage. Journal Of Earthquake Engineering And Engineering Vibration 27, 1–6 (2007)
3. Wen, R.: China Network for Earthquake Engineering Simulation, IEM/CEA Report-0608001 (2010)
4. Liao, Z.: Introduction to Wave Motion Theories in Engineering. Science Press, Beijing (2002)
5. Pearlman, L., D'Arcy, M., Plaszczak, P., Kesselman, C.: NTCP Control Plugin.NEESgrid. NEESgrid TR-2003-16 (2003)
6. Nakashima, M., Kato, H., Takaoka, E.: Development of Real-Time Pseudo Dynamic Testing. Earthquake Engineering and Structural Dynamics 21, 79–92 (1999)
7. Networks for Earthquake Engineering simulation, http://www.nees.org

Synchronization Algorithm with APA Pilot Pulse Sequence for UWB Communication System

Huibin Xu[*] and Ying Wang[**]

Tongji University, Shanghai, China 200092
xuhuibin188@163.com, cwangying.cc@163.com

Abstract. Ultra wideband communications synchronization is an important and challening work because of its ultra short pulse shape and low-power transmissions. In this paper, the method of Using APA as a pilot sequences is proposed. The receiver utilizes the correlator which matches the pilot pulsed sequence, synchronization of receiver and transmitter can be attained by the peak value of the correlator. Theoretical analysis is consistent with simulation results. The synchronization performance of APA pilot sequences and random pilot sequences in AWGN and multipath channel is compared. Simulation results indicate that APA pilot sequences is superior to random pilot sequences in synchronization performance.

Keywords: synchronization, UWB, APA.

1   Introduction

UWB technology offers the potential for low-power transmissions, robustness to multi-path fading and excellent range resolution capabilities compared with its narrow band counterparts ,but one of the most challenging in the UWB realization is symbol synchronization. The coherent method is present in reference [2]. We know that timing error is sensitive in the UWB communication system from reference [3]. The receiver need the very accurate timing, if the receiver use the fixed template signal,which is difficult to achieve. The scheme of inserting the piolt pusle sequence in sender is proposed in reference [4], which is capable of matching the UWB signal without the phase of receiving signal,so UWB signal is captured. In this paper ,acquisition and time-synchronization algorithms for pilot pulsed sequence is analyzesd. Its idea is that the cross-correlation between receiving signals and templated signal is made. In this way, the output of correlator is changed by the similarity of receiving signal and template signal, the higher of similarity, the output of correlator is bigger. The receiver consider that the pilot singal appeared if the output of correlator exceeds a certain threshold, then the receiver estimate the peak of output of correlator and calculate the delay of the template signal, which is estimated for propagation delay. Ideally, the singal is not the influent by noise and distortion.so the value estimated keep the transmitter and receiver accurate synchronous.

In this paper, the synchronization of receiver and transmitter by choosing appropriate series as pilot sequence is mainly discussed. Pilot sequences must have the good correlation. According to this request, almost perfect sequence (APA) is a very good choice. So that, the algorithm of considering the APA series as pilot sequences is proposed.

2   Synchronization Algorithms for APA Pilot Sequence

2.1   Signal Model

Hypothesis: 2PPM - TH - UWB ultra-wideband system, its transmited signal can be expressed as:

$$S(t) = \sqrt{E_p} \sum_{j=-\infty}^{+\infty} p\left(t - jT_s - c_j T_c - d_j \varepsilon\right) \tag{1}$$

Where T_s is the pulse repetition time, $p(t)$ is the transmitted pulse, ε is the modulation index, c is the random bit value, T_c is the code cycle, d_j is information bits, E_p is single cycle pulse energy.

2.2   Receiver System Structure

Supposing $r_u(t)$ is the received signal bearing information by the receiver, which is polluted by the additive noise. Therefore , the received signals can be expressed as:
$r(t) = r_u(t) + n(t)$

In AWGN, $r_u(t)$ is signal that went by the delay and channel attenuation of transited signal $s(t)$. $r_u(t) = as(t - \tau)$,Where a is the channel gained , τ is the propagation delay.

In actual UWB communication system, for the receiver, τ is unknown..Receiver structure is shown in figure 1. $r(t)$ and $s(t)$ are the input of correlator, its output is expressed as:

$$R(\hat{\tau}) = \int r(t)s(t - \hat{\tau})dt$$

$$= \alpha \int s(t - \tau)s(t - \hat{\tau})dt + \int n(t)s(t - \hat{\tau})dt \tag{2}$$

From type (1) can be seen: Maximum relevance is obtained when $\hat{\tau} = \tau$. That is to say,

The corresponding time position , on which the maximum peak of $R(\hat{\tau})$ is appeared, is the accurate estimation of the propagation delay.

$$Max(R(\hat{\tau})) = R(\tau) \tag{3}$$
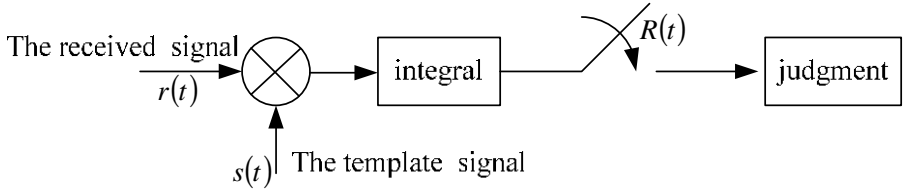
Fig. 1. Receiver structure

2.3   APA Sequence

Correlator is the core of the synchronization algorithms based on pilot pulse sequence. For type （2）have $\int n(t)s(t-\hat{\tau})dt$, the output of correlator is affected by SNR. As shown in figure 2 the output peak of correlator is very apparent and it is easy to capture the pilot pulse, when SNR is high. But detector can't accuratly identify the pilot pulse when SNR is lower. Therefore, the choice of appropriate pilot sequences is key. Its peak of the autocorrelation function is obtained on the origin and other peak is approximate 0. According to this request, APA sequence is a good choice.

（a）SNR=50dB   （b）SNR=0dB
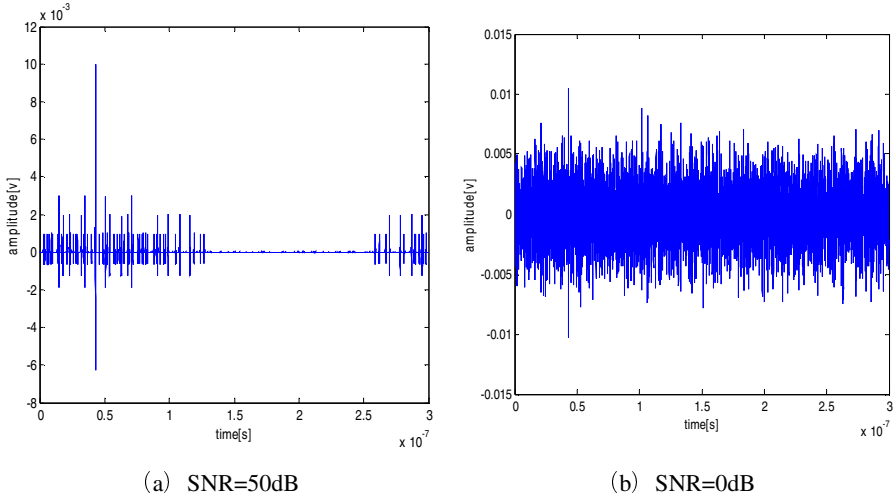
Fig. 2. The output of the random sequence correlator

The definition of the APA sequence is given in reference [5]. APA sequence is sequence that correlation coefficient of the all out-of-phase is alone ly a nonzero cycle sequence. e.g:

$$C_8 = [1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad -1 \quad -1]$$
$$C_{12} = [-1 \quad -1 \quad -1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1]$$

The correlation function C_8 of the APA sequence is expressed as:

$$R_8(\tau) = \sum_{i=1}^{8} C_8(i) C_8(i-\tau) = [8 \quad 0 \quad 0 \quad 0 \quad -4 \quad 0 \quad 0 \quad 0]$$

Obviously, the first peak is much higher than other value, which is very capable of capturing pilot pulse signal.

3 Simulation

In order to prove that APA sequence has better capture signal than random sequences, computer simulations is used. In simulation, the comparsion of 8-APA sequence with 8-random sequence is conducted.

The parameters of simulation are as follow: average power of transmitted signal Pow =- 30dBm; Impulse pulse duration Tm=0.5e-9s; Pulse form factor Tau=0.2e-9s; sampling frequency fc=1e11; Ts=8e-9s; the code-repetition number Ns=8; the maximum of jumped-time-code is Nh=8;cycle of the jumped-time-code is Np=8; code-time Tc=1e-9s; ε =0.5e-9s.
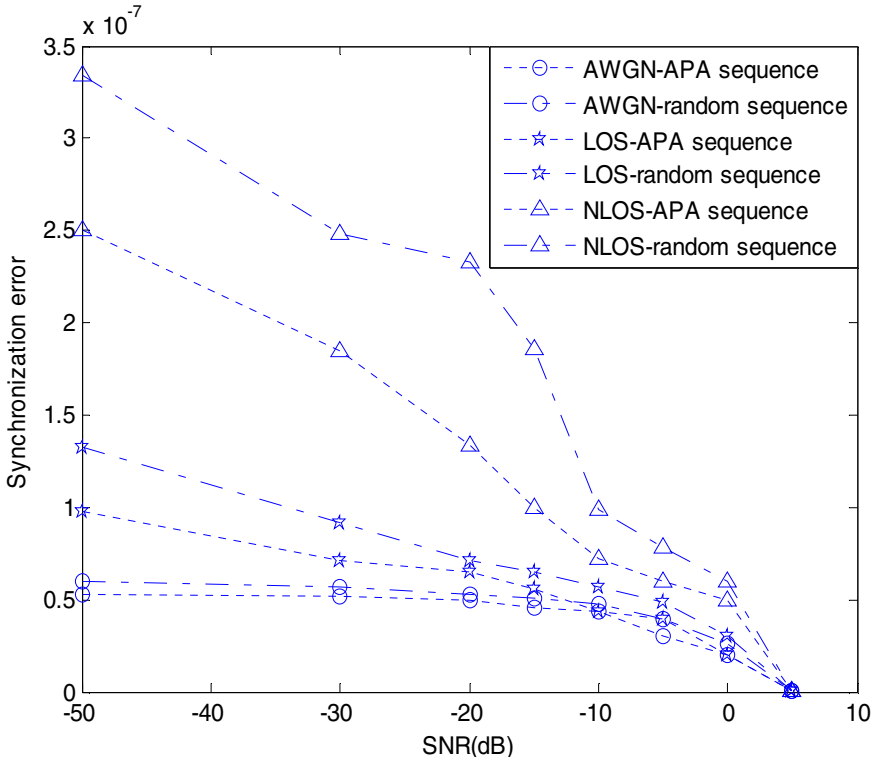
Fig. 3. The comparison of synchronization error between APA sequence and random sequence

AWGN, LOS, NLOS are tested in the simulation. Those channel parameters are from the channel model recommended by the IEEE.

As shown as the figure 3, APA sequence has better synchronize than random sequence for all the channel. For AWGN channel, They tend to be the same when SNR is less than -5dB, which resulted from the large of noise energy.

In LOS and NLOS channel, Synchronous precision obviously decreased for the influence of multipath distortion.

4   Conclusion

Through the simulation of synchronization algorithms for APA pilot pulse, the propose algorithms is feasible. Simulation results show that the proposal is practical for UWB system. The proposed algorithm is superior to the scheme based on the random sequence.

References

1. Win, M.Z., Scholtz, R.: Ultra-wide bandwidth time hopping spread-spectrum impulse radio for wireless multiple-access communications. IEEE Trans. on Comm. 48(4), 679–689 (2000)
2. Reggiani, L., Maggio, M.: Rapid search algorithms for code acquisition in UWB impulse radio communications. IEEE Journal on Selected Areas in Communications 23(5), 898–908 (2005)
3. Tian, Z., Giannakis, G.B.: BER sensitivity to mistiming in ultra-wideband impulse Radios-part I: nonrandom channels. IEEE Trans. on Signal Processing 53(4), 1550–1560 (2005)
4. Wang, J., Bi, G.G.: A new rapid acquisition scheme for DS-UWB systems. Circuits and Systems Journal 10(3), 120–123 (2005)
5. Wolfmann, J.: Almost perfect autocorrelation sequences. IEEE Transactions on Information Theory 38(4), 1414–1418 (1992)

The Key Management of Monitoring System for the Availability of Devastated Road[*]

Xiaoling Sun, Xuguang Sun, Zhong Li, Qiuge Yang, and Shanshan Li

Institute of Disaster Prevention, Yanjiao, Hebei, China, 065201
{sunxiaoling,sunxuguang,lizhong,
yangqiuge,lishanshan}@fzxy.edu.cn

Abstract. Earthquake damages roads and bridges, so the rescue of human and material can not be implemented in the first time to the devastated areas. In order to obtain the degree of destruction of roads and bridges, we need a real-time monitoring system. To ensure the safety and availability of the system, we need an effective key management scheme for the monitoring system for the availability of devastated road. In this paper, we proposed a new key management scheme combined with the polynomial-based key pre-distribution scheme and the Chinese Remainder Theorem based key distribution scheme. The new scheme can better support dynamically adding and deleting sensor node, can better save the storage space, computing power and communication energy of nodes. The new scheme is more suitable for the monitoring system for the availability of devastated road.

Keywords: sensor networks, key management, devastated road, monitoring system.

1 Introduction

Wireless sensor networks(WSN) collect the perceived target information within the coverage area through large numbers of nodes deployed in monitoring regional, then the information is transmitted to end-users after processed through multi-hop communication methods. For the nodes have the characteristics of random deployment and the dynamic changes of network topology, wireless sensor networks have broad application prospects in environmental monitoring, precision agriculture, national defense, military and commercial field. As the ordinary sensor nodes are limited by the energy, computing and storage capacity, communication bandwidth and transmission distance, they are vulnerable to security threats such as monitoring, capturing nodes, wormhole attacking. The content must be encrypted and authenticated to protect its safety communications. Key management becomes a very worthy of study.

At present, many scholars carried out relevant research on key management scheme for WSN. Eschenauer and Gligor[1] proposed a probabilistic key predistribution scheme for pairwise key establishment. The main idea was to let each sensor node randomly pick a set of keys from a key pool before deployment, so any two sensor nodes have a certain probability of sharing at least one common key. Chan [2] et al. further extended this idea and developed two key predistribution techniques: q-composite key predistribution and random pairwise keys scheme. The q-composite key predistribution also uses a key pool but requires two sensors compute a pairwise key from at least q predistributed keys they share. The random pairwise keys scheme randomly picks pairs of sensors and assigns each pair a unique random key. Du and Liu were partly based on Blom matrix [3] and polynomial model [4] to propose corresponding threshold solutions, these shemes effectively improved the ability of node to anti-capture under the case of increasing communications and computing. Zhu et al [5] proposed LEAP program to establish four types of communication key. Although the LEAP program achieved certain of the safety performance, but did not solve the problem of energy consumption for key updating.

2   Security Technology for Wireless Sensor Network

Since there is no considering of security during the design stage of protocol for sensor networks, there exists a variety of security risks of sensor networks. As the same with the traditional network, the research objective of sensor networks' security is to address the message confidentiality, integrity, message authentication, intrusion detection and access control et al. Used security technology are cryptographic algorithms, security protocols, authentication, secure routing, intrusion detection, access control.

2.1   Cryptography Algorithm

To prevent the transmission of confidential information, the most effective way is to establish an information encryption mechanism. The computing power and storage space of wireless sensor nodes are limited, so many existing cryptographic algorithms are difficult to use. At present, symmetric encryption algorithm is mainly used.

2.2   Security Protocol

For data confidentiality, data integrity, message authentication, data freshness and other security features, security protocol can be used to solve these problems. A. Perrig et al proposed sensor network security protocols SPINS, which contains two sub-protocols: SNEP and μTESLA. SNEP provides the basic security mechanisms: data confidentiality, data authentication and data fresh. μTESLA is sensor network broadcast authentication protocol.

2.3   Authentication Technology

The authentication technology of sensor network include authentication between entities, authentication within networks and users, broadcast authentication. And the

used authentication techniques are based on cryptography, based on message authentication codes, based on the authentication protocol. The key management of sensor network is the basis to achieve certification.

2.4   Secure Routing

Common routing protocol is designed simply, mainly for efficiency and saving energy, not considering safety factors. So it is vulnerable to various attacks, such as forged routing information, selective forwarding, cesspools, etc. Secure router designs from two considerations: the first is using information encryption and authentication to ensure the integrity and authentication of information transmission, the second is using the redundant of sensor nodes to provide multiple paths.

2.5   Key Management

The key is used in all of above security technology, so key management is the base of the security of sensor networks. To implement the security of sensor networks, key management is the first problem to be solved. Currently, most of the key management are based on symmetric encryption systems. E-G basic random key pre-distribution protocol is the most classic key management protocol.

3   The Key Management of Monitoring System for the Availability of Devastated Road

In the design of monitoring system for the availability of devastated road based on wireless sensor networks, we have completed the design of deployment of nodes, routing protocol and the algorithm of the determination of combination events. To ensure the safety and availablity of the system, we give a new key management scheme for the monitoring system for the availability of devastated road.

3.1   Network Topology

After the earthquake, the roads and bridges are severely damaged, network, communications and other infrastructure are paralyzed. We can laid sensor nodes to temporarily set up heterogeneous wireless sensor networks in the affected area to achieve disaster information. The networks consists of station, cluster nodes and sense nodes. There are more sense nodes, they have less computing capacity, limited energy, limited storage space and communication range, they are responsible for collecting information within the monitoring area. There are less cluster nodes, they have strong computing capacity, enough energy, enough storage space and communication range, they are responsible for collecting information from sense nodes, and forward the information out to the station.

The sense nodes are deployed along the road on both sides, and seperated in cluster based on the communication range of cluster nodes. See Figure 1. Sense nodes in the same cluster can only communicate with its neighbor nodes and the cluster node. Cluster nodes communicate with station directly, and need not communicate with each others.
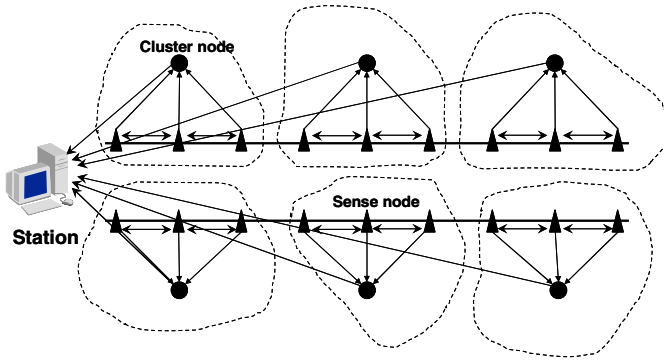
Fig. 1. Network topology

3.2   The Key Management Scheme

As the network is deployed in the affected area, the node can be physical damaged easily. The key management scheme is adopted to be able to better support dynamically adding and deleting nodes, to ensure that the replacement of cluster node does not affect network topology and key establishment. For the special nature of network application, we use the polynomial-based key predistribution protocol[4] to establish the shared key between cluster node and station. Each cluster node shares one key with the station seperately, so capturing one cluster node will not affect the safty of other cluster nodes. We use the key management scheme based on Chinese Remainder Theorem[6] to establish the shared key between cluster node and sense nodes, to reduce the number of keys computated and storaged in cluster nodes, to save energy and storage space for cluster nodes. In our new scheme, we combined the two schemes through intermediate variable. The station is responsible for large amount of computation to reduce energy consumption of cluster nodes and sense nodes.

3.2.1   System Initialization Phase

At the initialization phase, it is assumed that each node has a unique ID, for example, node u has ID_u. The key setup server randomly generates a bivariate t-degree polynomial $f(x,y)=a_{ij}x^iy^j$, it has the property of $f(x,y)=f(y,x)$. The polynomial $f(x,y)$ is pre-storaged in station and cluster nodes, $f(ID_i，y)$ is pre-storaged in cluster node i, and the master key K_{share} is pre-storaged in station, cluster nodes and sense nodes. Nodes are deployed according to network topology, and sense nodes chose nearly cluster node according to some rules. About how to chose cluster node , there are many effective solutions, and it will not be discussed here.

3.2.2   Key Establishment Phase

After the network is set up, the shared key should be consulted dynamicly between sense node and its cluster node, between sense node and its neighbor nodes, between cluster node and station to ensure the reliability and confidentiality of information.

Step 1: The cluster node i collects the ID of each sense node IDu (u=1,2,…, n, n is the number of sense nodes in the same cluster). And then sends the message M={EKshare(ID1), EKshare(ID2),…EKshare(IDn), EKshare(IDi)} to the station.

Step 2: The station decrypts M to achieve IDi of cluster node i and IDu (u=1,2,…,n) of sense nodes. Randomly choses a cluster key K, according to Chinese Remainder Theorem, we have:

$$X \equiv k1 \quad (\mathrm{mod}\ ID1)$$
$$X \equiv k2 \quad (\mathrm{mod}\ ID2)$$
…
$$X \equiv ku \quad (\mathrm{mod}\ IDu)$$
…
$$X \equiv kn \quad (\mathrm{mod}\ IDn)$$
$$X \equiv ki \quad (\mathrm{mod}\ IDi)$$

In which, ku=K⊕IDu, (u=1,2,…,n), ki=K⊕IDi. The station computes X and f(X, IDi), encrypts X by Kshare and sends it to cluster node i.

Step 3: Cluster node i gets X and computes f(IDi,X)=f(X, IDi) as the shared key between cluster node i and station. Then computes K=(X mod IDi)⊕IDi , and sends X to each sense node in the cluster.

Step 4: Sense node u(u=1,2,…,n) gets X and computes K=(X mod IDu)⊕IDu seperately as the shared key between cluster node and the sense node.

Then we established shared keys between station, cluster node and sense node seperately.

3.2.3   Adding and Deleting of Nodes

(1) Adding and Deleting of Sense Nodes

After key agreement is completed, if a new sense node joins the cluster, the cluster node collects IDnew of the new sense node, computes new value of M and forwards to the station. The station computes new encryption parameters through the Chinese Remainder Theorem:

$$Xnew \equiv k1 \quad (\mathrm{mod}\ ID1)$$
$$Xnew \equiv k2 \quad (\mathrm{mod}\ ID2)$$
…
$$Xnew \equiv ku \quad (\mathrm{mod}\ IDu)$$
…
$$Xnew \equiv kn \quad (\mathrm{mod}\ IDn)$$
$$Xnew \equiv knew\ (\mathrm{mod}\ IDnew)$$
$$Xnew \equiv ki \quad (\mathrm{mod}\ IDi)$$

The station sends Xnew to cluster node, cluster node sents Xnew to sense nodes, then cluster node and sense nodes computes shared key Knew=(Xnew mod IDx)⊕IDx seperately. So there is a new shared key in the cluster, and the shared key between cluster node and station is the same as before.

When the sense node exits the cluster because of energy depletion, physical damage, being captured et al, assume that the station can detect the occurrence of this event

through the information returned by cluster node, the station will delete the ID of this exiting node, recompute X, and send X to each node to renew the shared key in the cluster.

In the case that wireless sensor networks is used for collecting post-disaster information, the node exits mainly due to energy depletion or physical damage. When a certain number of nodes exit the network, we need to re-deploy nodes. The station will add the ID of new node, delete the ID of exiting node, compute the new value of X. Then all nodes in the cluster will compute new shared key.

(2) Replace of Cluster Node

In our application environment, the exiting of individual sense node does not cause much of the network function, but the damage to the cluster nodes influenced more. So once the cluster node exits, it must be updated in time. If the replace of cluster node occurs, then recompute the shared key between cluster node and station, between cluster node and sense nodes according to section 3.2.

3.3   Performance Analysis

(1) Performance Analysis of Security

The network deploys in the affected areas where roads and bridges are severely damaged. In this case, the probability of sensor node to be physical damaged is much more than to be captured. Another major security threat is information monitoring. The communication range between cluster node and sense nodes is too small to be monitored. If one node is captured, the station will delete its ID, and recompute the shared key in the cluster. The time of decrypting key is longer than the time of updating key. The communication range between cluster node and station is so long that it can be monitored easily, but the keys between each cluster node and station are different, so the failure of a cluster node will not affect other nodes.

(2) Storage Space

Common sense node only need store its own ID, shared master key Kshare and the shared key K. Cluster node need store its own ID, shared master key Kshare, polynomial value of $f(IDi, y)$, shared key $f(IDi, X)$ with the station, shared key K with the sense nodes in the cluster. Compared with most key management schemes, this scheme greatly saves the storage space of each node.

(3) Calculation of Consumption

Common sense node just do one encryption operation to send ID, do one decryption operation to achieve X, and do one modulo operation and one XOR operation to calculate a shared key K. The cluster node need do one encryption operation to send ID within cluster, do one decryption operation to achieve X, do one polynomial operation to calculate shared key $f(IDi, y)$ with station, and do one modulo operation and one XOR operation to calculate a shared key K. The X value and most of the polynomial operation are calculated by the station. So the energy consumption of nodes are saved significantly.

(4) Communication Cost

In wireless sensor networks, the energy consumption of once communication is much more than the energy consumption of once calculation. In this scenario, the communication is single-hop-based, and greatly reduces the communication energy.

4   Conclusion

In this paper, for the wireless sensor networks used in the situation of collecting post-disaster information, we proposed a new key management scheme combined with the polynomial-based key pre-distribution scheme and the Chinese Remainder Theorem based key distribution scheme. The program is divided into three stages: system initialization, key establishment, adding and deleting of nodes. In the system initialization phase, each node prestores relevant variables. In the key establishment phase, the station and nodes consult shared keys with stored variables, including the key between cluster node and sense node, the key between cluster node and station. In the last phase, we discuss the issues of key update in the case of adding and deleting nodes. The new scheme can better support dynamically adding and deleting of node to ensure the security of network communications, can better save the storage space, computing power and communication energy of nodes. The new scheme is suitable for monitoring system for the availability of devastated road.

References

1. Eschenauer, L., Gligor, V.D.: A key management scheme for distributed sensor networks. In: Proc 9th ACM Conf on Computer and Communication Security, Washington, DC, pp. 41–47 (2002)
2. Chan, H.W., Perrig, A., Song, D.: Random Key predistribution schemes for sensor networks. In: Proc 2003 IEEE Symp. on Security and Privacy, Berkeley, California, p. 197 (2003)
3. Du, W.-L., Deng J.: A pairwise key pre-distribution scheme for wireless sensor networks. In: Proc of the 10th ACM Conference on Computer and Communications Security (2003)
4. Liu, D.-G., Ning, P.: Establishing pairwise keys in distributed sensor networks. In: Proc of the 10th ACM Conference on Computer and Communication Security, pp. 52–61. ACM Press, New York (2003)
5. Zhu, S., Setia, S., Jajodia, S.: Leap: efficient security mechanisms for large-scale distributed sensor networks. In: Proc of the 10th ACM Conference on Computer and Communications Security(S.I.), pp. 62–72. ACM Press, New York (2003)
6. Zheng, X.-L., Huang, C.T., Matthews, M.: Chinese remainder theorem based group key management. In: Proc of ACMSE 2007, pp. 266–271 (2007)

Design and Implementation of Logistics Experiment Platform Based on OMT

Quan OuYang

School of Mathematics & Computer Science, Jianghan University,
WuHan 430056, China
Oyq8888@163.com

Abstract. The process of logistics experiment platform's design and implementation with OMT (Object Modeling Technology) techniques are presented in this thesis. We use OMT techniques to construct the object model, dynamic model and functional model in the logistics experiment platform, at the same time conduct an analytical research for the three models in design level, use multi-layer distributed architecture to achieve the logistics simulation system.

Keywords: OMT, object model, dynamic model, function model.

1   Introduction

The logistics enterprises mainly provide logistics services that include receiving, unloading, warehousing, warehouse management, shipping and distribution, return services, circulation-processing, transfer and other value-added logistics services to customers. In order to complete all the above services, the logistics enterprises must create a powerful, easy to use, stable, reliable and with good available growth logistics information system.

Logistics experiment platform based on "data accuracy"and "information security" provide the decision-makers with an advanced, reliable, and efficient management methods. Logistics experiment platform's design goal represents in the following areas: system reliability, system security; system advancement, extensibility; adaptability of system to the policy; achieving level management, helping leader to make decision; management standardization.

2   Main Design Idea of Experiment Platform

The organization structure of the logistics enterprises generally adopts a classification approach to design (as shown in Figure 1). The enterprise's headquarters coordinate and manage the cross-regional logistics activities. Regional logistics center is responsible for managing the region's orders, sales, warehousing, replenishment and other activities, at the same time submits the cross-regional goods information to enterprise's headquarters. The front-end logistics center's main duty is purchasing, shipping, warehousing and transportation. when the logistics enterprises receive the

cross-regional projects such organization structure allows each regional logistics center to exert full potential and work together to complete the logistics distribution tasks, while each regional logistics center can also carry out small-scale logistics distribution independently in own region .
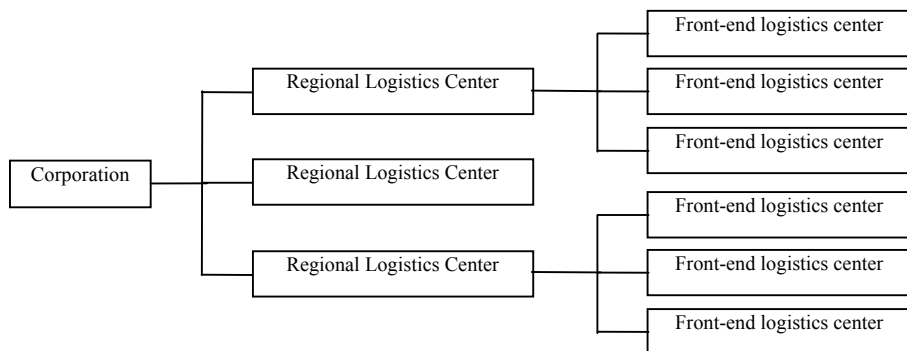
Fig. 1. Hierarchical management organization chart

The quality of services provided by logistics center directly affects the supply relationship between owners and customers. Logistics information system aims at monitor and industriously enhances the services quality of logistics center; make the logistics center become a reliable business partner of the goods owners. For this reason the entire logistics experiment platform can be divided into several interrelated modules are as follows (as shown in Figure 2): warehouse management module; procurement management module; sales management module; distribution management module; maintenance module; safety monitoring module.
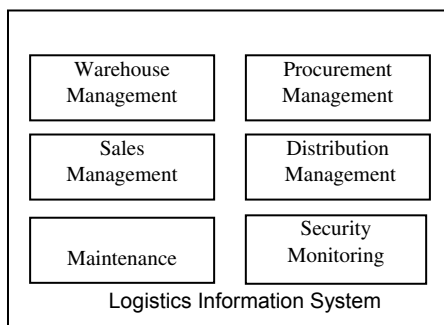
Fig. 2. Logistics Information System Modul

The work using OMT (Object Modeling Technology) [1],[2] to analyze and design was divided into four steps:

Analysis: it based on descriptions of the problems and the users' demands to build real-world models. The main product of this stage is description of problem, object model, dynamic model, and functional model.

Systems design: Combine the knowledge of problem domain and the architecture of target system and divide the target system into several subsystems. In this stage, the system design documents that describe the basic system architecture and high-level's decision will be formed.

Object design: combine the problem domain based on analysis model and add to implementation details to complete the system design. The main design content is to refine object model, dynamic model and functional model respectively and set the foundation of implement.

Implementation: it transforms the design to a particular programming language or hardware, while maintains traceability, flexibility and extensibility.

3   Establishment of Model

OMT is an object-oriented development method. The basis of development work is to model on the objects of real world, and then use the analysis model around these objects to carry on design independent of the language. Object-oriented modeling and design promote the understanding of demands, thus facilitate to develop clearer and easier to maintain software system. OMT describes the system from three aspects, correspondently provides three models, namely object model, dynamic model and function model [3],[4],[5].

Object model describes the static structure of objects and their relationships, which includes class, property, operation, inheritance, association, and aggregation and so on. Dynamic model describes the system's aspects changed with time, which includes state, sub-state, super-state, event, behavior, and activity and so on. Function model describes the conversion of data values within the system, which includes processing, data storage, data flow, control flow, and roles and so on.

3.1   Establishment of Object Model

OMT adopts the combination of bottom-up and top-down method to model. The first step starts from the problem statements, constructs the system model, which is a bottom-up inductive process. The work after system model building is decomposition, which is a service-based decomposition. This analysis and design processes from concrete to abstract and from abstract to concrete in turn follow the human's thinking pattern, make the requirement analysis more thorough and the system maintainability can be improved too. In accordance with the above analysis methods and steps, we construct the part object models of the logistics management information system (including object name, attribute, operation, and subclass as shown in Figure 3).

3.2   Establishment of Dynamic Model

Dynamic model describes the content related with time and sequence of operations of system, which mainly includes trigger events, event sequences, event status and the organization of event status. Dynamic model ffocus on the control that describes the sequence of operations occur in the system regardless of what to do, how to operate, and how to implement these operations. Creating a dynamic model must pass through

a complex gradual approximation process from writing the event script, outlining user's interface pattern diagram and event tracking diagram to describing the object state diagram.
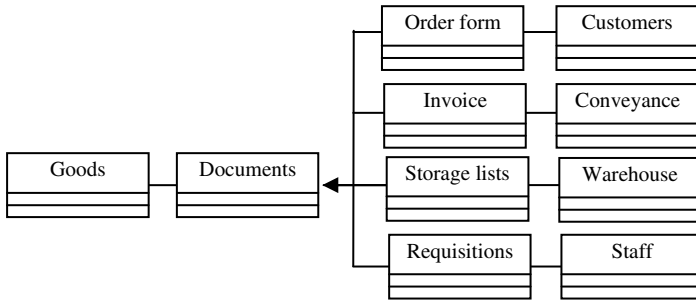
Fig. 3. Object Model

Step 1. Prepare the script of typical interactive behavior.
Script is a sequence of events, which is generated when the information exchanges occur between objects and customers of the system, the exchange information is the event's parameters. For each event, it should determine the action objects of triggered event, the external display format and the event parameters.

Step 2. Define the interface form.
Most interactions can be divided into two parts, namely application logic and application interface. Dynamic model represents the control logic of applications, so in analyzing the logistics management system, firstly the control flow should be concentrated on but not the display format. Format's description form is not important; the most important is the application logic can accept the command line, file, or mouse and so many different forms of input, enabling the exchange of information.

Step 3. Define events.
All the external events such as the signals coming form or sending to users and external device, input interrupt and conversion and so on must be ensured by checking all scripts. In the design process using scripts to find the normal events (such as passwords legitimacy), the error events (the value of illegal) and abnormal events (such as transmission errors) and assemble the events that control flow have same effect, and give them a unique name. Represent the script with an event trace diagram, which describes the series of events during the transmission. Multiple objects exist in the diagram; assign a separate column to each object, every event affects specific object directly can be found by observing the trace of each column of diagram. Figure 4 is the diagram of event tracking.

3.3   Function Model

Function model is used to describe all the derivation processes of the calculation or function in the system. It shows the operation meaning of object model, meaning of

constraints and action meaning of dynamic model, which uses data flow diagram (Data Flow Diagram, DFD) to express. The process of DFD corresponds to the activities or actions of class status diagram and the data flow of DFD corresponds to the object or attribute of the object diagram. The construction procedures of function model are as follows: determine the input/output, establish DFD, describe function and determine the constraints between objects. Logistics Information System DFD is as shown in Figure 5.
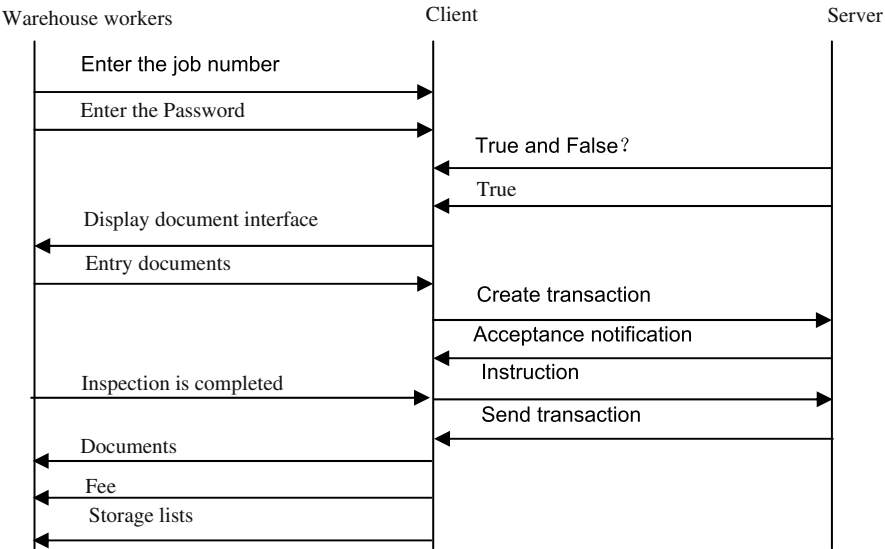
Fig. 4. Tracking diagram of goods warehousing events
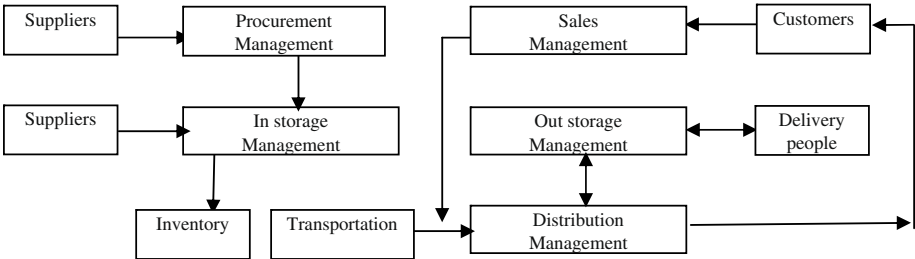
Fig. 5. Top-level DFD of logistics information system

4 Architecture Design of Logistics Experiment Platform

System design complete the advanced problem-solving strategies, which contains decomposing the system into subsystems, subsystem's hardware and software configuration, detail design, frame construction and other methods and strategies.

Architecture design's main task is to combine the three models mentioned above, add to some internal object classes implemented conveniently, and then implement the division for a system.

Logistics experiment platform is a distributed information management system, so use B/S structure to achieve is more reasonable, the application system under B/S environment usually composes browser, Web server, database server. Implementation of logistics information system adopts three architecture layers and consists of three relatively independent units as presentation layer, business logic layer and data source layer. The structure is as shown in Figure 6.

Browser	Application Server	Database Servers
	WEB Server	
Said layer	Functional layer	Database layer
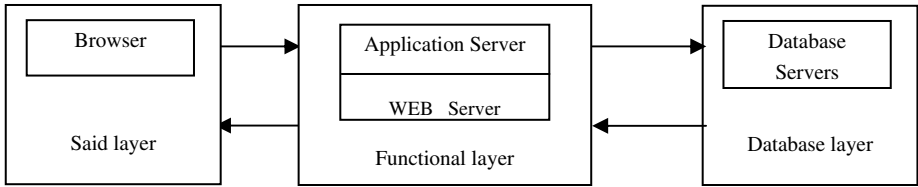
Fig. 6. Three-layer structure of the logistics information system

Presentation layer contains the system's display logic, is located in client and responsible for human-computer interaction, including the graphics and interface operations related to data and applications.

Business Logic contains the transaction processing logic of the system. WEB server is mainly responsible for responding to the client applications request. Firstly it needs to implement the relative extend applications and connect with the database connection, by means of SQL and other methods apply the processing applications to the database server. Back-end database server submits the data processing results to the Web server and Web server then returns the results to the client. Application server is responsible for centralized management of application logic namely the transaction processing. The application server is divided into several parts according to specific business processed by which.

Database server is mainly responsible for data storage and organization, distributed database management, database backup and synchronization.

5   Design of Object

Object design phase is to determine the whole definition of the classes used in implementation and all kinds of associations and the forms of interfaces, and to achieve the operation on objects. The object design of logistics information system is to design the objects in object model, function model and dynamic model described in front analysis phase and the relationship between the objects. In addition, to determine the classes and the inheritance of class used in implementation, and to construct the internal object needed in implementation phase, at the same time optimize the algorithms and data structures of the object.

Since the task of logistics information system is mainly to carry on decentralized acquisition, comprehensive utilization and centralized management. Therefore, to the

specific object design in the logistics information system, it mainly carries on the specific design of the tables in object model got from proceeding analysis and defines its attributes. In addition, decompose the operations of table object, select the appropriate algorithm, design the necessary internal object, analyze the relations with other objects, and determine the pattern of message transmission.

6   Conclusion

Logistics experiment platform uses OMT to modeling and uses the multi-layer distributed architecture to carry out it. It can simulate the management methods of logistics enterprise's network and informationization based on Internet. The design process of system covers the effective points of the logistics management, which consist of procurement management, warehousing management, inventory management, out of warehouse management, sales management, distribution management, customer management, staff management, system maintenance and other modules. These modules interconnect and form a tight, organic and complete system to achieve a centralized management of logistics information.

References

1. Meyers, S.: More effective C++ Photocopy. Publishing House of Electronics Industry, BeiJing (2006)
2. Martin, R.C.: Agile software development principles, patterns, and practices Photocopy. China Electric Power Press, BeiJing (2003)
3. Li, M., Xu, H.-Z., Chen, W.-P., Huang, T.O.: The application of object-oriented modeling technology. Journal of Northwest University (Natural Science Edition) 29(06), 507–509 (1999)
4. Booch, G.: Object Solutions Managing the Object-Oriented Project, pp. 95–103. China Machine Press, BeiJing (2003)
5. Bray, L.: An Introduction to Requirements Engineering, pp. 156–159. Posts & Telecom Press, BeiJing (2003)
6. Wu, J., Jin, M.-Z.: Object-Oriented Analysis Of UML, pp. 165–178. Publishing House of Electronics Industry, BeiJing (2002)
7. Zhou, Y., Zhao, Z.-W.: The design of university MIS based on B/S and component technology. Journal of Yanbian University(Natural Science) (2), 112–117 (2004)
8. Meilir, P.-J.: Foundation Of Object Oriented Design UML, pp. 24–30. Science Press, BeiJin (2001)
9. Brown, A.: Large-Scale Component—Based Development. Prentice Hall,Inc., New Jersey (2000)
10. Lippman, S.B.: Inside the C++ object model Photocopy. China Electric Power Press, BeiJing (2003)
11. Meyers, S.: Effective C++ Photocopy. Publishing House Of Electronics Industry, BeiJing (2006)

A Data Fusion Strategy of Wireless Sensor Network Based on Specific Application

Yajie Fei[*]

Shenyang Institute of Engineering, Shenyang, Liaoning, China 110136
`feiyajie@126.com`

Abstract. Because the energy consumption of wireless communication between nodes is greater than its data processing, Based on the data fusion strategy of sensor network, this paper proposes a method of setting the level of connectivity between nodes based on similarity of the nodes, so that it can greatly reduce data redundancy, and effectively reduce the amount of data transmission network, thereby reduce the consumption of communication, so it can achieve to save energy.

Keywords: rough set, data fusion, connectivity level, routing strategy.

1   Introduction

Since wireless sensor networks have some characteristics, for examples, no default network equipment, and network automatically and quickly, and easy to spread, so the wireless sensor network has broad application prospects in the military, environmental monitoring, industrial, medical health[1].

Wireless sensor network consists of a large number of sensor nodes, these nodes were scattered in the monitored scene by arranged randomly or point placed, For the individual sensor nodes, all the tasks can not be completed because its limited monitoring range and reliability[2][3]. Therefore, to ensure the accuracy of monitoring information and network communications connectivity, the distribution of sensor nodes required to reach a certain density[4]. At the same time, inevitably the monitoring scope of multiple nodes overlap with each other, especially when there are many homogeneous sensor nodes overlap with each other, these neighboring nodes collect the same information, so it brings data redundancy, as with the node density increases, this situation becomes worse[5].

The emergence of data fusion is conducted for the data processing within the network, that is, the data between the multi-source nodes fusion each other they are sent to next node, it can reduce redundancy, and reduce the net flow of data transmission and not lost the amount of information[6][7].

As the energy consumption of wireless communication between nodes is greater than tits data processing, so although the node energy consumption will increase by its computing and storage because the data fusion technology is lead into the sensor network, but also the communication consumption is reduced through the network, so

---

[*] Professor, the main research areas: data processing and communications direction.

it can achieve to save energy. In the ideal case, the input data of the middle M nodes which have the equal amount of data can be combined into an equivalent output data, and the energy consumption is I / M of the original data transfer; In the worst cases, fusion operation dose not reduce the amount of data by correlation effects, but by reducing the number of data groups the energy consumption of the channel negotiation or competitive can reduce.In recent years, with the rapid development of integrated circuit technology, micro-processor, the processing energy consumption continue to be reduced. In the near future, the data fusion within the network and reducing redundant data communication is become more important[8].

2   Sensor Data Fusion Strategy

The key of data fusion is the relevance of data, in a specific application there must be related between the data, and because the role of different attribute is different in describing node character, so the attribute weight is different. The relevance of sensor nodes is determined according to weights of attributes, and the connectivity level between nodes is determined according to relevant of sensor nodes, and the data fusion route is determined, so it effectively reduces the data redundancy, reduces the amount of data transmission, saves communication energy[9].

First of all sensor nodes is expressed as:

G (A, W, Gt, T)

G is the sensor node of network, A is the node attribute set, W is the attribute weight set, Gt is the node set which connected to G, T is connectivity level set which correspond to Gt, and T is calculated.

2.1   Attribute Weights

Many methods for calculating attribute weight have been described in many papers, can use neural network, genetic algorithm, but the rough set method is more objective reflection of the importance of the attribute itself, eliminating maximum the influence of human factors, so this paper uses the rough sets theory to determine the attribute weight.

There are more and less many uncertainty factors in many actual applications, the data sets collected from actual application are often contains noise, inaccurate or incomplete. Rough set theory is another mathematical tool for dealing with uncertainty problem after the probability theory, fuzzy sets, evidence theory. As a relatively new soft computing method, rough set theory obtains more and more attention in recent years, its effectiveness has been confirmed in many scientific and engineering fields, and becomes a research hot spot in the field of artificial intelligence theory and its application now.

Rough set theory is based on classification mechanism, and it will be understood as a particular the equivalence relations on classification space, and equivalence relations determine the division of the space. Knowledge is understood as the division of data in Rough set theory, each division is called a concept. The main idea of rough set theory is to approximately characterize the imprecise or uncertain knowledge based on the known knowledge. The most notable difference between rough set

theory and other theories dealing with the problem of uncertainty and imprecision is that it is not required to provide any prior information except the needed dataset, so the description or process of the uncertainty problem is more objective. Because this theory could not contain the methods of dealing with imprecise or uncertain raw dataset, so this theory is highly complementary with probability theory, fuzzy mathematics and evidence theory dealing with uncertain or imprecise problem.

Rough set theory abstracts the objective or object world into an information systems, the information systems is to study to describe the knowledge of object by specifying the basic characteristics and characteristic values of object, in order to discover useful Knowledge or decision rules from large amounts of dataset with using a certain method, so the information system is also called attribute - value system.

The concrete steps to determine attribute weights based on rough set theory will be introduced as follows [10].

(1) Construction of decision table

At first, in order to calculate attribute weigh, we should construct a decision table, the decision table is consist of condition attribute set and decision attribute set, each attribute has a value. A is the set of all attributes, U is the set of all attribute value.

For the same node, decision attributes is different form different applications, for example, for the same plant node, the decision attribute is the harmful attribute if the node is used to distinguish that the plants is harmful or not, the decision attribute is the traits attribute if the node is used to distinguish plant classification. In this way, decision attribute of different applications is different, and the construction of decision table is also different.

(2) Attribute discretization

The data processed by the rough set theory must be discrete, it is the preparation of calculating attribute weight. There are two methods, automatic and expert discrete.

(3) Calculating attribute SGF

C is the condition attribute set, D is the decision attribute set, C is the sub-set of node attribute set, and D also is, $ax_i \in C$, then the SGF of ax_i is expressed as：

$$SGF(ax_i, C, D) = \gamma(C,D) - \gamma(C - \{ax_i\}, D)$$

$\gamma(C,D)$ expresses the dependence degree of C and D, $\gamma(C - \{ax_i\}, D)$ expresses the dependence degree of C and D when C excludes ax_i.

$$\gamma(C,D) = |POS(C,D)| / |U|$$

$|POS(C,D)|$ is the attribute number of $POS(C,D)$, $POS(D,C)$ is the positive domain value, U is the attribute number of U.

For the same node, different training dataset of different application can obtain different attribute SGF, therefore, for the same node, you can provide different training dataset of different applications to obtain the attributes SGF of different applications, it can enhance the reusability degree of node[11].

(4) Calculating attribute weight

According to the above attribute SGF, we can obtain the attribute weight using the normalized method, the calculation formula is shown as follows:

$$W(ax_i) = SGF(ax_i) / \sum SGF(ax_j) (j = 1, 2, \ldots\ldots)$$

$W(ax_i)$ is the weight of attribute i, $SGF(ax_i)$ is the SGF of attribute i.

2.2   The Level of Connectivity between Nodes

According to the attribute weight of the sensor node, it can determine the similarity between different nodes, and determine the relationship between nodes.

First it gives the definition of the node similarity, it has two kinds of similarity: the same similarity and the different similarity.

The same similarity is defined as:

Sim (Gi, Gj) = ΣWaik-Wajk
Ak =AGi∩AGj, aik∈Ak∧aik∈Ai,ajk∈Ak∧ajk∈Aj

The different similarity is defined as:

Dif (Gi, Gj) = ΣWai'+ ΣWaj',
ai'∈ AGi ∧ ai'∉ AGj, aj'∈ AGj ∧ aj'∉ AGi

The similarity is defined as:

Sum (Gi, Gj) = Sim (Gi, Gj) + Dif (Gi, Gj)

Gi, Gj is two separate nodes, AGi is the attribute set of Gi, AGj is the attribute set of Gj, Ak is the intersection set of AGi and AGj, aik and ajk are the same attribute of Ak, aik is an attribute of Ak, Waik is the attribute weight of aik in Gi, ajk is an attribute of Ak, Wajk is the attribute weight of ajk in Gj.

Wai' is the attribute weight of ai', ai' is an attribute of Gi, but it is not an attribute of Gj, Waj' is the attribute weight of aj', aj' is an attribute of Gj, but it is not an attribute of Gi.

Nodes are organized according to the similarity between the different nodes.

(1) If the similarity Sum (Gi, Gj) between node Gi and Gj is less than the specified threshold, and then granularity Gi and Gj are identified as complete similar, Tij=0. If the similarity Sum (Gi, Gj) between node Gi and Gj is bigger than the specified threshold, and then granularity Gi and Gj are identified as different, Tij>0.

The different nodes can be further compared.

(2) If the same similarity Sim (Gi, Gj) between node Gi and Gj is less than the specified threshold, and then node Gi and Gj are identified as approximate similar, Tij=1.5.

(3) f not, the two different nodes can be further compared, the set of the same attributes can be shrunk. If the same similarity Sim (Gi, Gj) between node Gi and Gj based on the shrunk attribute set is less than the specified threshold, and then node Gi and Gj are identified as partial similar, Tij=2.0.

(4) If not, the two different nodes can be further compared, the set of the same attributes can be shrunk. If the shrunk attribute set is Φ, and then node Gi and Gj are identified as different, Tij=∞。

So by comparing the similarity between the nodes, we can determine the kind of similarity between two nodes, and form a set of node links between nodes according to different similarity.

2.3   Dynamic Routing Strategy

According to the connectivity level between nodes, We can dynamically organize route of data fusion.

The follows id the principles of dynamically routing.

(1) If Tij=0, Gi, Gj is identified as directly connectivity, and add Gj to Gti, add Gtj to Gti, delete all the nodes of Gtj except Gi, delete Gj from all nodes.

(2) If Tij=1.5, Gi, Gj is identified as basic connectivity.The same attribute set and its weight construct a new virtual node Gij, the node Gij is called as the parent node, each set of different attributes and their weights construct two nodes Gin, Gjn, the two nodes are called as the children node, add Gij to Gtin, Gtjn, Tijin=0,Tijjn=0,and delete all nodes of Gtij from Gi, Gj, and Gtin=Gti, Gtjn=Gtj.

(3) If Tij=2.0, Gi, Gj is identified as part connectivity. The shrinkable same attribute set and its weight construct a new virtual node Gij, the node Gij is called as the parent node, each set of different attributes and their weights construct two nodes Gin, Gjn, the two nodes are called as the children node, add Gij to Gtin, Gtjn, Tijin=0, Tijjn=0, and delete all nodes of Gtij from Gi, Gj, and Gtin=Gti, Gtjn=Gtj.

(4) If Gi, Gj is identified as different, Tij = ∞, and delete Gi from Gtj, delete Gj from Gti.

(5) The principle of selecting route is based on connectivity level, from small to big, first select the directly connectivity routes, then select the basic connectivity routes, finally select the part connectivity route.

(6) Tij = Tji.

When the dynamic self-organizing network connect nodes based on different levels, choose low-level connectivity route, disconnect the high side compared with other connectivity, so the network structure is transparent and avoid a lot of duplicate data transmission, saving energy.

2.4   Attribute Move Algorithm

In the construction course of dynamic route, the main problem is the attribute movement.

The follows introduces the algorithm of attribute movement[12].

(1) Attribute up

Step 1: searching the node which the attribute belongs to, searching its parent nodes, listing all the children node of the same parent, listing all the attribute weight of each child node, if one child node has not the attribute, its attribute weight is 0;

Step 2: calculating the attribute weight difference between all the children nodes, calculating the average of the attribute weight difference of all the children nodes;

Step 3: moving the attribute to its parent node from all the children nodes, the weight is the average of the attribute weight of all the children nodes, and delete the attribute from all the children nodes, but the attribute weight of each child node still stores in database, the algorithm is ended.

(2) Attribute down

Step 1: searching the node which the attribute belongs to, listing all the children nodes of it, listing all the attribute weight stored in database of all the children nodes, if a child node has not the attribute, its attribute weight is 0;

Step 2: calculating the attribute weight difference between all the children nodes;

Step 3: moving the attribute to all the children nodes of it, and delete the attribute from it, but the attribute weight of it still stores in database, the algorithm is ended.

If the thresholds are changed, the data fusion route must be reconstruction, the attribute may move up or down, this algorithm synthesizes algorithm 1 and algorithm 2, but it considers all attributes, it will be discussed in the other paper.

3   Conclusions

Sensor network is a new research field of the computer science and technology, has very broad application prospects, and has been pay close attention by academic and industry.

In this paper, the strategy of data fusion makes the structure more clarity, data redundancy is extremely reduced, effectively increase data transmission efficiency and saving energy.

References

1. Akyildiz, L.E., Su, W.L., Sankarasubramanizm, Y., Cayirci, E.: A survey on sensor networks. IEEE Communications Magazine 40(8), 102–114 (2002)
2. Pister, K., Hohlt, B., Jeong, J., Doherty, L., Vainio, J.P.: Ivy- A sensor network infrastructure (2003),
   `http://vvwwbsac.eecs.berkeley.edu/projects/ivy`
3. University of California at Los Angeles. WINS: Wireless integrated network sensors,
   `http://wwwjanet.ucla.edu/WINS/biblio.htm`
4. Tilak, S., Abu-Ghazaleh, N.B., Heinezlman, W.: A taxonomy of wireless micro-sensor network modest. Mobile Computing and Communications Review 1(2), 1–8 (2002)
5. Kahn, J.: Next Century Challenges:Mobile Networking for"Smart Dust". In: Conference on Mobile Computing and Networking, vol. 9 (1999)
6. IIyas, M., Mahgoub, L.: Handbook of Sensor Networks: Compact of wireless and wired sensing systems. CRC Press LLC (2005)
7. Hall, D.L., Linas, J.: Handbook of multi sensor data fusion. CRC Press, Boca Raton (2001)
8. Ren, F.Y., Huang, I.-I., Lin, C.: Wireless sensor networks. Journal of Software 14(2), 1148–1157 (2003)
9. Bin-Ru, Y., Ya-Dong, J., Jiang-Tao, S.: KDD based on double-base cooperating mechanism and its realization of software. Systems Engineering and Electronics 22(6), 69–72 (2000)
10. Yao, Y., Gerhke, J.: The cougar approach to in-network query processing in Sensor networks. ACM SIGMOD Record 31(3), 9–18 (2002)
11. Madden, S., Hellerstein, J., Hong, W.: TinyDB: In-network TinyOS. IRB-TR-02-014, IntelResearch, UC Berkeley, queryprocessing, 10 (2002)
12. Fei, Y.: Research on construction of the virtual dynamic knowledge discovery tree based on node reusebility. In: FSDK 2010, pp. 2886–2890 (2010)

Computational Technique of Learning Progress Motivation: Diagnosis of Learning and Innovation Status

Pi-Shan Hsu[1] and Te-Jeng Chang[2,*]

[1] Ching Kuo Institute of Management and Health, Human Resource Development,
203 Keelung, Taiwan
`ivymax950@yahoo.com.tw`
[2] National Taiwan Normal University, Industrial Education,
106 Taipei, Taiwan
`tjmax950@yahoo.com.tw`

Abstract. Learning Progress Motivation (LPM) was developed to intrinsically incent organizational members adapting both exploratory and exploitative learning in innovation processes. LPM was applied on 103 engineers in the experiments which simulated innovation contexts. The computational technique of LPM was developed to dynamically transform learning records to a Learning Progress Characteristic (LPC) curve at real-time base. Through analyzing LPC curve, LPM four-phase cycles and the steady-state condition of LPM innovation process were identified. Engineers are motivated intrinsically and continuously by LPM to pursue maximal learning progress. The learning progress, innovation performance, and steady-state condition can be diagnosed by interpreting LPC curve. Therefore, the visual aided LPC curve is a user-friendly tool for managerial leaders of organizations in diagnosing learning and innovation status in innovation processes.

Keywords: Diagnosis, innovation, intrinsic motivation, learning progress.

1   Introduction

Innovation is categorized as exploitative innovation and exploratory innovation [1]. Organizations are constantly required to monitor both their exploitative and exploratory innovation activities and strive to achieve a balance between exploratory and exploitative learning in increasingly uncertain and competitive environments. In order to be innovative, implementation is a key aspect of the innovation process [2]. A new suitable motivation is required in implementation to replace current practices in order to encourage people to achieve successful exploration of new possibilities and the exploitation of old certainties in innovation processes.

Through literature review the authors identified that Maximal Learning Progress (MLP) reward is suitable in motivating and balancing exploitative learning and exploratory learning in innovation processes. However, no studies have dynamically

---

explored the relative progress between exploitative learning and exploratory learning by a quantitative approach. Hence, the authors developed the computational technique of Learning Progress Motivation (LPM) according to the concept of MLP reward in an aim to quantitatively transform both exploitative learning and exploratory learning status at dynamic real-time base in innovation processes. The experiment was designed to lead subjects to experience different contexts during innovation processes. The comparative learning progress ratio is defined as the ratio of exploitative learning progress and exploratory learning progress and calculated according to the computational technique of LPM through the experiment process. After all the quantitative records of comparative learning progress ratio were converted into a Learning Progress Characteristic (LPC) curve, the authors were able to diagnose learning and innovation performance status by analyzing LPC curve.

2   Learning, Motivation, Innovation

People who engage in exploratory innovation pursue new knowledge and develop new products for emerging applications. People who pursue exploitative innovation, by contrast, build on existing knowledge resources and extend existing products for current applications [3], [4]. Sustained performance is rooted in simultaneously pursuing both exploitation and exploration innovations [2], [3] by exploiting existing competences and exploring new opportunities [5], [6], that is, to explore new capabilities while exploiting existing ones [7], [8]. Intrinsic motivation is a driver which pushes people to concentrate on situations that maximize learning progress [9]. People are motivated intrinsically to integrate exploration and exploitation learning by exploring new capabilities with exploratory learning while exploiting existing ones with exploitative learning [10].

3   Learning Progress Motivation

Kaplan and Oudeyer [11] presented Maximal Learning Progress (MLP) reward which is an intrinsic motivation and pushes an agent towards situations in which it maximizes its learning progress [12]. MLP reward has been successfully adopted by [13], [14], [15], [16].

In this study, Learning Progress Motivation (LPM) was developed according to the concept of MLP reward and adopted in experiments of anticipation games which simulated innovation processes without an explicit target to achieve. LPM evaluates both exploratory learning and exploitative learning instead of treating learning as a single factor by MLP reward.

3.1   The Computational Technique of LPM

The computational technique of LPM applied in this study is described as followings. The subject receives an input signal from previous situations and predicts an output signal $O(n)$ corresponding to his or her actions at any step n in the learning context. The reward received at step n is $R(n)$. The goal of the subject is to maximize the amount of rewards received in a given time frame.

The entire situation is summarized as *OR (n)*. The subject anticipates *O (n)* based on previous situations *OR (n-1), OR (n-2),….* Then the subject takes the current situation *OR (n)* as an input and tries to predict the future situation *OR (n+1)*. At specific step *n*, the value of error *e(n)*, which is the distance between the predicted *O (n)* and the target number T, is calculated as equation (1).

$$e(n) = \left| O (n) - T \right| \tag{1}$$

In the meantime, the authors define the "learning progress" *p(n)* as the decrease of error rate. In case of an increase in *e(n)*, learning progress is zero. Corresponding equations (2) and (3) are represented as follows:

$$p(n) = e(n\text{-}1) - e(n): \quad e(n) < e(n\text{-}1) \tag{2}$$

$$p(n) = 0: \qquad\qquad e(n) \geqq e(n\text{-}1) \tag{3}$$

Because "learning progress" is the only variable to maximum, the reward *R (n)* equals to *p(n)*. The equations (4) and (5) shown above are revised as follows:

$$R (n) = p(n) = e(n\text{-}1) - e(n): \; e(n) < e(n\text{-}1) \tag{4}$$

$$R (n) = p(n) = 0 \qquad : \quad e(n) \geqq e(n\text{-}1) \tag{5}$$

Because organizational members conduct both exploitative learning and exploratory learning in innovation processes; therefore, the exploitative learning progress $p_{exploitative}(n)$ is represented for a specific subject who applies exploitative learning and the exploratory learning progress $p_{exploratory}(n)$ is represented for a specific subject who applies exploratory learning.

In each step *n*, the cumulative learning progress *P (n)* is computed as the integration over time of previous learning progress *p(n)* or rewards *R (n)*. The cumulative learning progress *P (n)* is represented as equation (6):

$$P (n) = \Sigma^{n}_{j=1} \; p(n) = \Sigma^{n}_{j=1} \; R (n) \tag{6}$$

The cumulative exploitative learning progress $P_{exploitative} (n)$ generated by $p_{exploitative}(n)$ and the cumulative exploratory learning progress $P_{exploratory} (n)$ generated by $p_{exploratory}(n)$ is represented as equation (7) and (8).

$$P_{exploitative} (n) = \Sigma^{n}_{j=1} \; p_{exploitative}(n) \tag{7}$$

$$P_{exploratory} (n) = \Sigma^{n}_{j=1} \; p_{exploratory}(n) \tag{8}$$

In order to evaluate the comparative learning progress performance between exploitative learning and exploratory learning, the comparative learning progress ratio *RP (n)* is defined as equation (9):

$$RP (n) = P_{exploitative} (n) \div P_{exploratory} (n) \tag{9}$$

4   Method

Based on the concept of MLP reward, LPM is designed to motivate organizational members to adapt both exploratory and exploitative learning according to innovation contexts in order to lead people into effective exploratory and exploitative innovation.

In this study, LPM was applied in a situated experiment of anticipation games which simulated innovation processes. The process-phase learning records of subjects, which were generated in experiments, were dynamically converted into numerical data at real-time base by the computational technique of LPM. A graphic curve, named Learning Progress (LP) curve, was generated by the computational technique of LPM for each subject. LP curve is used for further analysis to explore subjects' learning progress and innovation performance.

4.1   Experiments

The authors designed an experiment of anticipation game to simulate innovation processes in order to explore the learning dynamics developed by LPM, The concept of the experiment applied in this study was similar to the one applied in Kaplan and Oudeyer's experiments [11]. Subjects anticipated target numbers by the strategy of maximizing their learning progress. The learning progress is converted into quantitative data by the computational technique of LPM.

Subjects of experiments. 103 engineers were selected as subjects of this experiment. Three to five engineers were selected randomly from each firm to form a cluster, and totally 25 clusters were grouped to simulate micro organizations.

Mechanisms of Anticipations. Subjects were requested to anticipate target numbers from number 1 to 200. The anticipation will be terminated when the subject conducts anticipation 100 times or all the target numbers are anticipated. The mechanism of anticipation is shown below:

Generation. Three target numbers are generated by the computer randomly. The first target number T is picked randomly by the computer and the other two target numbers T-1 and T+1 are generated accordingly.

Strategies. There are two strategies to approach anticipation which are "exploratory random generation" $M_{exploratory}$ and "exploitative approach" $M_{exploitative}$. $M_{exploratory}$ is defined as the subject picks numbers generated by the computer randomly, which simulates exploratory learning. $M_{exploitative}$ is defined as the subject induces numbers based on evaluating learning progress, which simulates exploitative learning.

Evaluation. Subjects evaluate $P_{exploitative}$ (n) generated by $p_{exploitative}(n)$ and the $P_{exploratory}$ (n) generated by $p_{exploratory}(n)$ to conduct anticipations.

Decision Making. If the subject can interpret the meaning from the evaluation of $p(n)$ and $P(n)$, then the subject adopts $M_{exploitative}$ to induce a number. If the subject cannot interpret the meaning from the evaluation of $p(n)$ and $P(n)$, then he or she adopts $M_{exploratory}$ to generate a number randomly by computer.

4.2   Analysis Tool of Experiments

The values of step *n* and *RP (n)* were generated from specific step *n* of anticipation. The two-dimensional point was defined on the X-Y axis which took step *n* as the horizontal

axis (X-axis) and *RP (n)* as the vertical axis (Y-axis). The curve, named "LP Curve", was constructed by connecting the points generated from all steps of anticipation. Every subject has his or her unique LP curve generated by 100 anticipations. A Total of 103 LP curves were generated by subjects. A single curve, called "Learning Progress Characteristic (LPC) Curve", was obtained by conducting multi-factor regression on those 103 LP curves. LPC curve is used for analysis of experiment.

5   Results

5.1   LPC Curve

LPC curve (refer to Figure 1) is obtained by conducting multi-factor regression on 103 LP curves. LPC curve was generated the computational technique of LPM in the innovation process. Therefore, this innovation process is named as LPM innovation process. LPC curve represents for the overall learning behavior and progress of LPM innovation process.
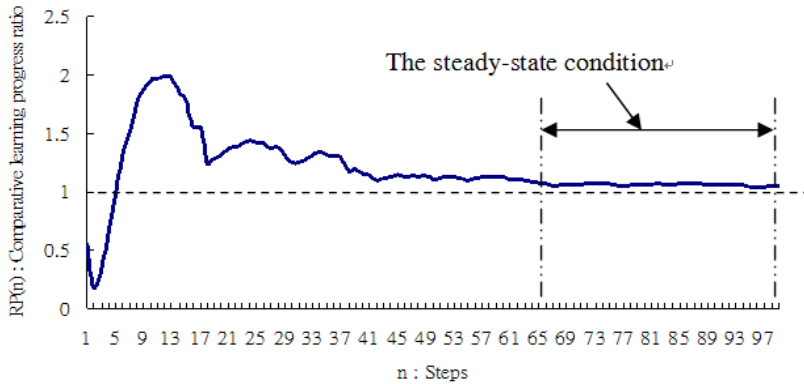
Fig. 1. Learning Progress Characteristic (LPC) curve

5.2   LPM Four-Phase Cycle

The learning behavior of subjects in the innovation process was evaluated by analyzing LPC curve. From the analysis results, LPC curve was formed by several cycles, named LPM four-phase cycle, with similar curve pattern. Each cycle was divided into four phases which were described as followings (refer to Figure 2).

Phase I – Exploration. In the uncertain and unknown context, subjects preferred to use the strategy of $M_{exploratory}$ in order to learn about unknown environments and discover contingencies efficiently. $M_{exploratory}$ outperformed $M_{exploitative}$ which drove subjects to use the exploratory learning more than exploitative learning. Therefore, *RP (n)* was less than 1 and $P_{exploratory}(n) > P_{exploitative}(n)$.

Phase II – Interpretation. On phase II, subjects using $M_{exploitative}$ anticipated the target number by chance at the specific step. From that moment, subjects started progressing rapidly and $M_{exploitative}$ outperformed $M_{exploratory}$. Therefore, *RP (n)* increased and approached 1 rapidly as long as subjects improved the proficient level of interpretation. *RP (n)* was still less than 1. Subjects interpreted how to adapt learning by evaluating the progress of *p(n)* and *P (n)* to achieve efficient anticipation.

Phase III – Proficient. The moment of *RP (n)* equaling to 1 was called "transition point" After passing the transition point, *RP (n)* tended to be larger than 1 as long as subjects kept improving their proficient level of interpretation. $M_{exploitative}$ outperformed $M_{exploratory}$, which drove subjects to use the exploitative learning more than exploratory learning. *RP (n)* was larger than 1. The condition of successfully anticipating target number increased dramatically after passing the transition point. This suggests that LPM inspired subjects to improve the efficiency of anticipation continuously and significantly by adapting exploitative learning and exploratory learning according to the progress of contexts.

Phase IV – Saturation. In Figure 2, the *RP (n)* kept increasing on phase III but the increasing rate reduced moderately and emerged in a saturation condition as long as *RP (n)* reached 2. At this stage, subjects' learning tended to saturate gradually and reached a kind of habituation phase. Subjects were no longer to intensively experience rapid learning progress. The chance to learn new knowledge reduced dramatically once it overtook *RP (n)=2*. Hence, *RP (n)* decreased rapidly and tended to approach 1 to reach a saturation condition.
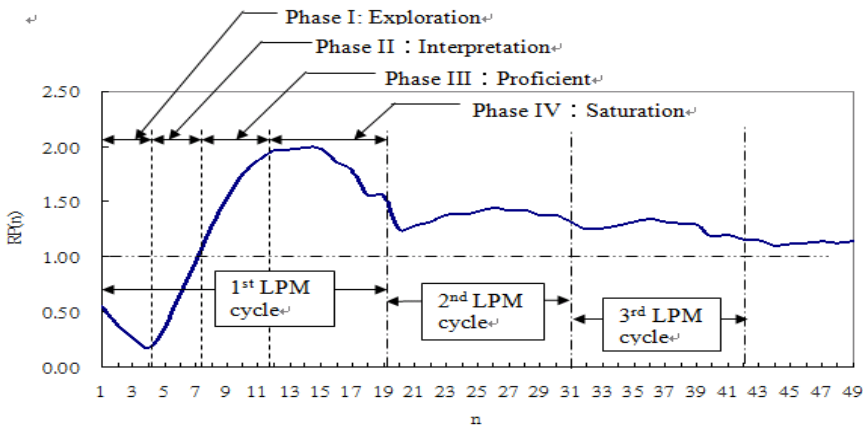
Fig. 2. LPM four-phase cycle vs. LPC curve

5.3   The Steady-State of LPM Innovation Process

In Figure 2, subjects conducted exploitative and exploratory learning by a specific four-phase pattern and repeated such a learning pattern in every evolution to construct LPM innovation process. Through several LPM four-phase cycles, *RP (n)* of LPC

curve approaches 1 gradually and forms a steady-state condition. In the steady-state condition (refer to Figure 1), the LPC curve nearly parallels the line of *RP (n)*=1 at a constant narrow gap after several LPM four-phase cycles. Subjects tended to adapt exploitative learning and exploratory learning according to the innovation contexts and approach a steady-state condition. In the steady-state condition, subjects' learning tends to saturate rapidly and reach a certain habituation phase. The steady-state condition takes place while subjects stay in the similar task content for a long while according to the findings of the experiment. In this study, the efficiency of anticipation represents the innovation performance and indicates continuous improvement but it reaches saturation in the steady-state condition.

6   Discussions and Conclusions

Through the analysis of the LPC curve generated by the computational technique of LPM, organizational members are motivated intrinsically by LPM to adapt exploratory learning and exploitative learning flexibly according to the innovation context of four phases in order to receive maximal learning progress, which results in continuous learning and innovation performance improvement. Progresses along with LPM innovation process, *RP (n)* of the LPC curve drops gradually to a constant and forms a steady-state condition. In the steady-state condition, organizational members loose the strong motivation to achieve maximal learning progress, which results in a decrease in learning progress and innovation performance. To avoid sticking to the steady-state condition, managerial leaders of organizations should seek to identify the steady-state condition and then take action to re-organize team members into a different set-up or assign the team members to other projects which have different task contents from the ones with which they used to work. In summary, the computational technique of LPM realizes the feasibility of dynamically diagnosing organizational members' learning and innovation performance status at real-time base. The LPC curve generated by the computational technique of LPM provides a user-friendly visual aided tool in diagnosis for managerial leaders in the innovation process.

References

1. March, J.G.: Exploration and exploitation in organizational learning. Organization Science 2(1), 71–87 (1991)
2. Oke, A., Munshi, N., Walumbwa, F.O.: The influence of leadership on innovation processes and activities. Organizational Dynamics 38(1), 64–72 (2009)
3. Benner, M., Tushman, M.L.: Exploitation, exploration, and process management: The productivity dilemma revisited. Academy of Management Review 28, 238–256 (2003)
4. Jansen, J.J.P., Vera, D., Crossan, M.: Strategic leadership for exploration and exploitation: The moderating role of environmental dynamism. The Leadership Quarterly 20, 5–18 (2009)

5. He, Z.L., Wong, P.K.: Exploration vs. exploitation: An empirical test of the ambidexterity hypothesis. Organization Science 15, 481–494 (2004)
6. Gibson, C.B., Birkinshaw, J.: The antecedents, consequences, and mediating role of organizational ambidexterity. Academy of Management Journal 47, 209–226 (2004)
7. O'Reilly, C.A., Tushman, M.L.: The ambidextrous organization. Harvard Business Review 82(4), 74–81 (2004)
8. Tushman, M.L., O'Reilly, C.A.: Ambidextrous organizations: Managing evolutionary and revolutionary change. California Management Review 38, 8–30 (1996)
9. Schmidhuber, J.: Curious model-building control system. In: IEEE International Joint Conference on Neural Networks, vol. 2, IEEE Press, Singapore (1991)
10. Crossan, M., Vera, D., Nanjad, L.: Transcendent leadership: Strategic leadership in dynamic environments. The Leadership Quarterly 19, 569–581 (2008)
11. Kaplan, F., Oudeyer, P.Y.: Maximizing learning progress: An internal reward system for development. Embodied Artificial Intelligence 3139, 259–270 (2004)
12. Oudeyer, P.Y., Kaplan, F., Hafner, V.V.: Intrinsic motivation systems for autonomous mental development. IEEE Transactions on Evolutionary Computation 11(2), 265–286 (2007)
13. Barto, A., Singh, S., Chentanez, N.: Intrinsically motivated learning of hierarchical collections of skills. In: 3rd International Conference on Development Learn, San Diego, CA, pp. 112–119 (2004)
14. Igari, I., Tani, J.: Incremental learning of sequence patterns with a modular network model. Neurocomputing 72(7–9), 1910–1919 (2009)
15. Oudeyer, P.Y., Kaplan, F.: Discovering communication. Connection Science 18(2), 189–206 (2006)
16. Takamukua, S., Arkinb, R.C.: Multi-method learning and assimilation. Robotics and Autonomous Systems 55(8), 618–627 (2007)

Study on the Processing Method of Cycle Slips under Kinematic Mode

Long Fan[1,2,*], Guojun Zhai[2,**], and Hongzhou Chai[1,***]

[1] Institute of Surveying and Mapping, Zhengzhou, China 450052
[2] Naval Institute of Hydrographic Surveying and Charting, Tianjin, China 300061
{fl19841108,zhaigj,chaihz1969}@gmail.com

Abstract. Through analyzing the DIA method, two step Kalman filter method and continuous cycle slips detecting method which is based on Kalman filter to deal with cycle slips, this paper proposes the improved method to deal with kinematic cycle slips which is also suitable to the high kinematic condition. By choosing "Current" statistic model to be the filter state model, this paper combines the carrier phase and Doppler observation to identify the cycle slip, meanwhile estimates and corrects the slip immediately. The result of calculating and analyzing the different simulated situation shows that the algorithm can better withstand the influence of maneuvering errors. As to the problem of multiple cycle slips and successive cycle slips, the algorithm can also deal with it fast and correctly.

Keywords: Kalman filter, Cycle slips, DIA method, "Current" statistics model.

1   Introduction

The kinematic measurement technique of GNSS has been widely used in the area ofairplane, auto-mobile, vessel navigating and positioning. The cycle slip is the main reason that affect the accuracy of carrier phase observation in kinematic measurement, and the appearance of cycle slips is complex in kinematic mode, the slips may occur only in one epoch and also may occur in some successive epochs; meanwhile in one epoch there may be only one satellite that occur slips, and also may be many satellites that occur slips. In this case, instantly correcting the influence of the cycle slips is important. At present, the cycle slips processing method which is based on Kalman filter to test and correct the cycle slips by using new information vector which is obtained through filter during the data processing course, such as DIA method[1][2], two step Kalman filter method[3] and successive cycle slips detection method[4]. The proposing of DIA method provides the theory base for the cycle slips processing method with Kalman filter; On the base of DIA method, the two step Kalman filter method pay more attention to the problem of multiple cycle slips, but the MDB[5][6] value are easily influenced by the error of observation, the Geometric Feature of

---

satellite and the error of carrier maneuvering in practical and will get wrong identification result; The proposing of successive cycle slips detection method is based on the two methods mentioned before, the method can solve the problem of successive cycle slips, however it dose not take the influence of kinematic model error into account, the result of this method will become bad when carrier is maneuvering.

In this research, the detection, identification and adaptation three steps of the cycle slips processing method based on Kalman filter are improved, simulating and analyzing the different situation of cycle slips in kinematic mode by data observed from the experiment of aviation flying, the result shows that the improved method can correctly solve the problems which include the single cycle slip, multiple cycle slips and successive cycle slips when carrier is maneuvering.

2   Kalman Filter Method of Kinematic Cycle Slips Processing

Under the condition of phase slipping in current epoch, the observation model that contains the influence of cycle slips is defined as[7]:

$$L_k = A_k X_k + C_k b_k + e_k \tag{1}$$

where X_k is state vector; L_k is the measurement of the receive; A_k is the design matrix, the e_k are measurement noise; C_k is the coefficient matrix of cycle slips bias, the $C_k^i = [0 \ \cdots \ \overset{i}{1} \ \cdots \ 0]^T$ under condition of none slip; b_k is the slips bias vector[1].The final filter result will contain the influence of cycle slips if the standard filter algorithm is being used, consequently the influence should not be neglected in high precision data processing of kinematic survey. The cycle slips processing procedure which bases on Kalman filter includes the bias detection, identification and adaptation[1][2][7].

2.1   Cycle Slips Detection

On the hypothesis that no cycle slips, the innovation vector abide by the zero mean normal distribution, suppose that the bias number is the same with the dimension of the innovation vector, the local forecast warning statistic can be construct as:

$$T_k = \bar{V}_k^T \Sigma_{V_k}^{-1} \bar{V}_k \tag{2}$$

where $\bar{V}_k = A_k \bar{X}_k - L_k$ is the innovation vector of the epoch k, Σ_{V_k} is covariance matrix of innovation[7], normally the statistic obeys the central $\chi^2(n_k, 0)$ distribution, the degree of freedom n_k is bias number[1][7], however it obeys $\chi^2(n_k, \lambda)$ distribution the $\lambda = b_k^T (S_k^T Q_{V_k}^{-1} S_k) b_k$ is the non-centrality parameter of alternative hypothesis, $S_k = C_k + A_k \Phi_{k,k-1} U_k$ and $U_k = \Phi_{k,k-1} U_{k-1} - K_k S_{k-1}$.Through the calculating the local forecast warning statistic of each epoch, under the significance level α, judge the relationship between the forecast warning statistic and the quantile value χ_α^2, if T_k is

greater than the it, the current epoch exists cycle slip and should make a further identification to make sure the cycle slips exist on which observation.

2.2 Cycle Slips Identification

After making sure that the cycle slips exist in current epoch, the observation of each observed satellite should be checked to find out the slips existed in the which observations. Constructing the one dimension bias identification statistic

$$T_k^1 = \frac{(C_k^{iT} \Sigma_{\bar{V}_k}^{-1} \bar{V}_k)^2}{C_k^{iT} \Sigma_{\bar{V}_k}^{-1} C_k^i} \tag{3}$$

where C_k^i is the coefficient vector of bias in case that the observation of the i satellite exists slips, which is mentioned above, $i = 1 \ldots n$, n is the number of observations in current epoch. The statistic T_k^1 is agreeing with the $\chi^2(1,0)$ distribution[7]. The coefficient matrix C_k can be constructed when all observations of the current epoch have been checked. However T_k^1 is sensitive to the bias in practical using, it is easily influenced to get the wrong identification result. In order to solve the problem, using the MDB to supplement the χ^2 testing[5][6]. First of all, identifying cycle slips initially, then estimating the identified slips bias, determining whether the estimation is grater than the MDB, if greater, the identification result is right, else it is wrong[5].

2.3 Cycle Slips Adaptation

In order to correct the cycle slips，the bias $\hat{b}_k$ should be estimated, the common method is recursively estimating it by using the sequential adjustment. For the linear relationship between the bias $\hat{b}_k$ and the innovation vector, the corrected innovation vector is given as:

$$\bar{V}_k^a = \bar{V}_k + S_k b_k \tag{4}$$

Using the innovation vector which contains slip errors as the observation, $\hat{b}_{k-1}$ as the prediction of state vector, the estimation of $\hat{b}_k$ is[4]

$$\hat{b}_k = \hat{b}_{k-1} + K_{b_k} (\bar{V}_k - S_k \hat{b}_{k-1}) \tag{5}$$

where $K_{b_k} = (S_k^T \Sigma_{\bar{V}_k}^{-1} S_k + \Sigma_{\hat{b}_{k-1}}^{-1})^{-1} S_k^T \Sigma_{\bar{V}_k}^{-1}$, S_k is mentioned before, and $S_k = C_k$ in case that the preceding epochs did not exist slips, the variance matrix of epoch k can be deduced according to the law of propagation of errors, the variance matrix of epoch k can be deduced according to the law of propagation of errors

$$\Sigma_{\hat{b}_k} = (I - K_{b_k} S_k) \Sigma_{\hat{b}_{k-1}} (I - K_{b_k} S_k)^T + K_{b_k} \Sigma_{\bar{V}_k} K_{b_k}^T \tag{6}$$

supposing that $M = (S_k^T \Sigma_{\bar{V}_k}^{-1} S_k + \Sigma_{\hat{b}_{k-1}}^{-1})^{-1}$, the variance matrix of $\hat{b}_k$ can be written as:

$$\Sigma_{\hat{b}_k} = M = (\Sigma_{\hat{b}_{k-1}}^{-1} + S_k^T \Sigma_{\bar{V}_k}^{-1} S_k)^{-1} \tag{7}$$

3   The Improved Kinematic Cycle Slips Processing Method

The method mentioned above is based on the CV or CA model, under the circumstance that the maneuvering of carrier is intensive, as a result even the cycle slips can be detected, the bias estimation will be influenced by the state model error. Therefore, the model which can more truly describe the movement of carrier should be used as the filter state model, the "Current" statistic model is chosen in this paper. The "current" statistic model indicate the statistic character of accelerate by using the corrected rayleigh distribution, it can truly describe the movement of carrier in local scope, the model thinks of that the accelerate of next epoch is limited, and will just change in the area with related to the current accelerate, when the carrier is moving[8].

According to the model definition, the filter state model can be written as follow

$$X_k = \Phi_{k,k-1}X_{k-1} + \bar{u}_k + w_k \tag{8}$$

where $\Phi_{k,k-1} = diag[\Phi_{x(k,k-1)}, \Phi_{y(k,k-1)}, \Phi_{z(k,k-1)}], \bar{u}_k = \begin{bmatrix} \bar{u}_{xk} & \bar{u}_{yk} & \bar{u}_{zk} \end{bmatrix}^T$

$$\Phi_{x(k,k-1)} = \begin{bmatrix} 1 & T & \dfrac{(\alpha T -1+e^{-\alpha T})}{\alpha^2} \\ 0 & 1 & \dfrac{(1-e^{-\alpha T})}{\alpha} \\ 0 & 0 & e^{-\alpha T} \end{bmatrix} \tag{9}$$

$$\bar{u}_{xk} = \begin{bmatrix} (-T+0.5\alpha T^2 + \alpha(1-e^{-\alpha T}))\big/\alpha \\ T - (1-e^{-\alpha T})\big/\alpha \\ (1-e^{-\alpha T}) \end{bmatrix} \bar{a}_x(t) \tag{10}$$

$\Phi_{y(k,k-1)}, \Phi_{z(k,k-1)}, \bar{u}_{yk}, \bar{u}_{zk}$ have the same form with Eq.(9)and(10), The system error vector is the zero-mean Gaussian white noise vector, the Variance matrix of w_k is $\Sigma_{w_k} = diag[\Sigma_{w_{xk}}, \Sigma_{w_{yk}}, \Sigma_{w_{zk}}]$, the expression of $\Sigma_{w_{xk}}$ is

$$\Sigma_{w_{xk}} = 2\alpha\sigma_{ax}^2 \begin{bmatrix} \dfrac{T^5}{20} & \dfrac{T^4}{8} & \dfrac{T^3}{6} \\ \dfrac{T^4}{8} & \dfrac{T^3}{3} & \dfrac{T^2}{2} \\ \dfrac{T^3}{6} & \dfrac{T^2}{2} & T \end{bmatrix} \tag{11}$$

σ_{ax}^2 is the acceleration variance on x axis, the form of $\Sigma_{w_{yk}}$ and $\Sigma_{w_{zk}}$ is the same as the Eq.(11).

The innovation vector can be calculated by using the constructed state model, according to the statistic mentioned in section 2.1, the existence testing step of cycle slips can be finished.

After testing the existence of cycle slips, the identification can be implement to find out the slips exist on which observations. However under the condition that the accuracy of observations is poor or carrier maneuvering strongly, even using the MDB to associate the identification, the MDB value will be affected and lead to the false identifying results[4]. Taking the relationship between phase and Doppler into account, this paper uses the Doppler observation to associate the cycle slips identification[9]. The statistic can be constructed as:

$$\Delta\boldsymbol{\varphi d}_\mathrm{t} = (\boldsymbol{\Phi}_{t-1} - \boldsymbol{\Phi}_t)/\Delta T - \frac{1}{2}(\boldsymbol{D}_{t-1} + \boldsymbol{D}_t) \tag{12}$$

where $\boldsymbol{\Phi}_t$ and $\boldsymbol{D}_t$ are the phase and Doppler observation in epoch t, ΔT is the sampling interval. Theoretically, the accuracy of carrier phase and Doppler observation can respectively reach 1mm and 2mm/s[10]. According to the law of propagation of errors, the statistic mean square error of data with 1Hz sample rate in L1 channel is $\sigma_{\Delta\varphi d} = 0.08\mathrm{cycle}\,/\,\mathrm{s}$.

The testing principle is

$$\begin{cases} |\Delta\boldsymbol{\varphi d}| < 3\sigma_{\Delta\varphi d} & \text{none slip} \\ |\Delta\boldsymbol{\varphi d}| > 3\sigma_{\Delta\varphi d} & \text{exist slip} \end{cases} \tag{13}$$

according to the principle, all observation in current epoch can be tested to find the slips exist in the phase observations of which satellites.

The bias should be estimated after checking out the observation that exist cycle slips. The estimation of the cycle slips starting from current epoch will become inaccurate in follow epoch, because of the influence of errors accumulating. In this paper, the slips bias is just estimated in the epoch where they start, in order to keep the observation of the follow epochs cleaning, correct the observation of the follow epochs after estimating the slips bias.

The proposed method thinks that the cycle slips started from preceding epoch, having no influence to the estimating procedure of current epoch, therefore the corrected innovation vector can be written as:

$$\bar{V}_k^a = \bar{V}_k + C_k b_k \tag{14}$$

according to LS method the bias can be estimated

$$\hat{b}_k = (C_k^T \Sigma_{\bar{V}_k}^{-1} C_k)^{-1} C_k^T \Sigma_{\bar{V}_k}^{-1} \bar{V}_k \tag{15}$$

$$\Sigma_{\hat{b}_k} = (C_k^T \Sigma_{\bar{V}_k}^{-1} C_k)^{-1} \tag{16}$$

Meanwhile, the filter result will be influenced by the cycle slips in current epoch, if pass the result directly to the processing procedure of next epoch, the statistic which constructed in next epoch will also be influenced not to agree with the $\chi^2(\boldsymbol{n}_k, 0)$

distribution even if the next epoch do not exist cycle slip. In order to keep the next epoch immune from the cycle slips of current epoch, the filter result and its variance matrix should be corrected.

For the reason that the prediction of state vector in epoch k only has the relationship between the state vector of epoch k-1, consequently it would not be influenced by cycle slips. The corrected filter result is estimated by using the corrected innovation vector in Eq.(14)

$$\hat{X}_k^a = \bar{X}_k - K_k \bar{V}_k^a = \hat{X}_k - K_k C_k \hat{b}_k \tag{17}$$

where $K_k = \Sigma_{\bar{X}_k} A_k^T [A_k \Sigma_{\bar{X}_k} A_k^T + \Sigma_k]^{-1}$. The covariance matrix between prediction vector of state and observation is given as:

$$\Sigma_{\bar{X}_k L_k} = \begin{pmatrix} \Sigma_{\bar{X}_k} & 0 \\ 0 & \Sigma_k \end{pmatrix} \tag{18}$$

the uncorrected state vector $\hat{X}_k$ and innovation $\bar{V}_k$ can be written as:

$$\hat{X}_k = \begin{pmatrix} I - K_k A_k & K_k \end{pmatrix} \begin{pmatrix} \bar{X}_k \\ L_k \end{pmatrix} \quad \bar{V}_k = \begin{pmatrix} -A_k & I \end{pmatrix} \begin{pmatrix} \bar{X}_k \\ L_k \end{pmatrix} \tag{19}$$

the covariance matrix between two vectors is deduced as:

$$\begin{aligned} \Sigma_{\hat{X}_k \bar{V}_k} &= \begin{pmatrix} I - K_k A_k & K_k \end{pmatrix} \begin{pmatrix} \Sigma_{\bar{X}_k} & 0 \\ 0 & \Sigma_k \end{pmatrix} \begin{pmatrix} -A_k^T \\ I \end{pmatrix} \\ &= K_k \Sigma_k - \Sigma_{\bar{X}_k} A_k^T + K_k A_k \Sigma_{\bar{X}_k} A_k^T \end{aligned} \tag{20}$$

$\hat{X}_k$ and $\hat{b}_k$ also can also be rewritten into the form as:

$$\hat{X}_k = \begin{pmatrix} I & 0 \end{pmatrix} \begin{pmatrix} \hat{X}_k \\ \bar{V}_k \end{pmatrix}, \hat{b}_k = \begin{pmatrix} 0 & K_b \end{pmatrix} \begin{pmatrix} \hat{X}_k \\ \bar{V}_k \end{pmatrix} \tag{21}$$

$$\begin{aligned} \Sigma_{\hat{X}_k \hat{b}_k} &= \begin{pmatrix} I & 0 \end{pmatrix} \begin{pmatrix} \Sigma_{\hat{X}_k} & \Sigma_{\hat{X}_k \bar{V}_k} \\ \Sigma_{\bar{V}\hat{X}_k} & \Sigma_{\bar{V}_k} \end{pmatrix} \begin{pmatrix} 0 \\ K_b^T \end{pmatrix} \\ &= \Sigma_{\bar{X}_k} (A_k^T \Sigma_{\bar{V}_k}^{-1} \Sigma_{\bar{V}_k} - A_k^T) K_b^T = 0 \end{aligned} \tag{22}$$

the deducing procedure proves that the $\hat{X}_k$ and $\hat{b}_k$ are uncorrelated, meanwhile the variance matrix of corrected filter result is given as:

$$\Sigma_{\hat{X}_k^a} = \Sigma_{\hat{X}_k} + K_k C_k \Sigma_{\hat{b}_k} C_k^T K_k^T \tag{23}$$

transmitting the corrected state vector and its variance matrix to the next epoch, the form of innovation vector of epoch k+1 $\bar{V}_{k+1}$ can be written as:

$$\bar{V}_{k+1} = A_{k+1} \Phi_{k+1,k} \hat{X}_k - L_{k+1} - A_{k+1} \Phi_{k+1,k} K_k C_k \hat{b}_k \tag{24}$$

The three elements of the right part of Eq.(24) are irrelative with each other, therefore the innovation of epoch k+1 is also agree with the zeros mean normal distribution, the cycle slips starting from last epoch have no influence to the successive processing procedure.

4   Testing Computation and Analysis

The data are collected from the experiment of aviation fly, the sampling rate is 1HZ. Through choosing the data observed from the course that flight taking off, the signal of SVN3, SVN8, SVN11, SVN19, SVN27 and SVN28 can be received during the chosen period, the ambiguity of those satellites are prefixed on at the static mode. The figure 1 shows the acceleration of flight during the chosen period.
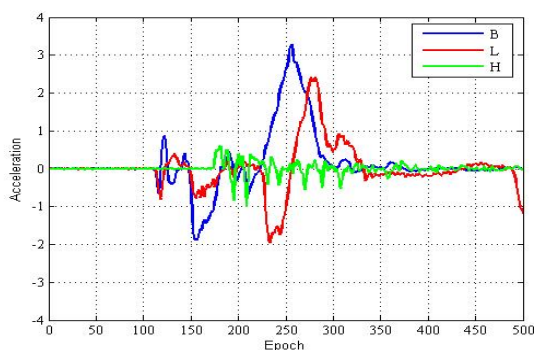
Fig. 1. The acceleration of BLH directions

As shown in figure, during the chosen period, the flight is static in the period, and then it starts accelerating, the acceleration that close to the epoch 150 and 253 has fiercely changed. The observations used in this paper are none cycle slips existing, in order to test the validity and the effectiveness, simulating the different situation manually. In the static mode, the movement of plane is steady, the all the method that based on Kalman filter can correctly process the cycle slips.

In the kinematic mode, in order to test the validity and effectiveness of the proposed method under the condition that flight maneuvering, simulating the situation of single cycle slip, multiple cycle slips and successive cycle slips to analyze. With the single cycle slip situation, adding the slip to different satellite in the epoch 253 that acceleration changes the most fiercely, the results are showed in table 1.

As is shown in table 1, in case of carrier maneuvering, only one satellite exist the cycle slip, whatever the it exist in which satellite, the algorithm can correctly detects, identifies and calculates the cycle slip bias.

Table 1. The result of single cycle-slip identification and bias estimation

epoch	prn	true value (cycle)	identification	Estimation (cycle)
253	28	1	28	1.114
253	11	3	11	3.037
253	8	5	8	5.146
253	19	6	19	5.701
253	3	8	3	8.244

Table 2. The result of multiple cycle-slip identification and bias estimation

epoch	prn	true value (cycle)	identification	Estimation (cycle)
253	3	6	3	6.150
	11	20	11	20.197
	19	15	19	14.720
253	3	1	3	1.150
	8	10	8	10.013
	11	20	11	20.187
	19	15	29	14.731

Table 3. The result of successive cycle-slip identification and bias estimation

epoch	prn	true value (cycle)	identification	Estimation (cycle)
253	11	3	11	3.231
254	11	13	11	12.880
255	11	12	11	11.643
253	3	6	3	6.163
254	19	4	19	3.889
255	28	8	28	8.393
	8	7	8	7.074
253	3	6	3	6.163
	28	4	28	4.353
254	11	11	11	10.719
	19	3	19	3.143
255	3	8	3	8.086

With the situation of multiple cycle slips, analyzing by dividing the situation into the three kinds which are the cycle slips exist in the observation of three satellites and four satellites. The results are shown in table 2.

In the epoch 253, whether three or four satellites, the statistics constructed by the proposed algorithm can correctly detect the slips errors, position the errors, and estimate the size of bias values.

With the situation of successive cycle slips, choosing the epoch 253, 254 and 255, respectively simulating the situation that successive slips exist in the same satellite, exist in different satellites and combine the multiple slips.

As is shown in table 3, the result shows that whether the same satellite or different satellite exist slips in three successive epochs, the procedure of subsequent processing is not affected by cycle slips in current epoch, because of the filter result and variance matrix are directly corrected after estimating the bias value.

5   Conclusions

The paper proposed the method that based on "current" statistic model and use the Doppler observation to assist the carrier phase to identify the cycle slips, at last independently estimate and repair the slips bias at current epoch. Through calculating and analyzing the observation which simulating the different cycle slips condition, making the following conclusions:

(1) To some extent, the impact of carrier maneuver can be resisted by using the "current" statistical model, as the state model of filter, therefore the existence of cycle slips can be correctly detected through using the constructed inovation vector.

(2) The bias estimation of successive epochs will be affected by the observation errors to become inaccurate, when estimating the cycle slips bias through sequential adjustment. The proposed method which estimates the cycle slips in each epoch, meanwhile repair the successive observations to avoid the bias repeated estimating, and not to affect processing the cycle slips of subsequent epochs, eventually the method can correctly process the successive cycle slips.

References

1. Teunissen, P.: Quality Control in Integrated Navigation Systems. J. IEEE AES Magazine 5(7), 35–41 (1990)
2. Teunissen, P., Salzmann, M.: A Recursive Slip-page Test for Use in State-space Filtering. J. Manuscript Geodaetica 14, 182–190 (1989)
3. Lu, G.: Statistical Quality Control for Kinematic GPS Positioning. J. Manuscript Geodaetica 17, 270–281 (1992)
4. He, H., Yang, Y.: Detection of Successive Cycle Slips for GPS Kinematic Positioning. J. Acta Geodaetica et Cartographica Sinca 28(3), 199–203 (1999)
5. Salzman, M.: MDB: A Design Tool for Integrated Navigation System. J. Bulletin geodesique 65 (1991)
6. Teunissen, P.: Minimal detectable biases of GPS data. J. J Geod 72 (1998)
7. Yuan-xi, Y.: Adaptive Navigation and Kinematic Positioning. Publishing house of Surveying and Mapping, Beijing (2006)
8. Wen, Z., Sun, J., Sun, K., Xu, D.: Study of Model of Airborne GPS Kinematic. J. Surveying Target Tracking. Applied Science and Technology 29(3), 12–15 (2002)
9. Xu, G.: GPS-Theory-Algorithms and Applications. Springer, Heidelberg (2007)
10. Xiao, Y., Xia, Z.: Comparison Between Phase-Rate and Doppler to Determine Velocity. J. Geomatics and Information Science of Wuhan University 28(5), 581–582 (2003)

The Research of Building VPN Based on IPsec and MPLS Technology

Hong-Yun Xu

School of Mathematics & Computer Science, Jianghan University,
WuHan 430056, China
`xhy1978@163.com`

Abstract. IPSec uses encrypting and encapsulating technology in client device and establishes a secure tunnel connection. The private network built by MPLS technology can ensure good transmission performance and service quality. This study concludes several methods of building VPN in existing network facilities through the analysis and research of IPsec and MPLS technology. In addition, it compares these programs and researches and proposes some practical problems need to consider in VPN establishment.

Keywords: IPSec, MPLS, VPN, PPTP.

1   Introduction

VPN evolves from the private network access provided by the PSTN (public switched telephone network). VPN developed by now contains a variety of technologies and solutions and to different people the word has different meanings. VPN can be understood as a method, which by means of tunneling, encryption, authorization, access control, and many other technologies and services through the Internet / Intranet / Extranet to transfer data. Technologies are used in VPN: IPSec (IP security protocol), PPTP (Point-to-Point Tunneling Protocol), Layer Two Tunneling Protocol, MPLS (Multi Protocol Label Switching) technology using DES (Data Encryption Standard), and other security management technology[1],[2],[3].The high-speed access services based on cable modem and digital line technology grow rapidly, but from the view of commerce, these services have some insufficiencies that they only provide a high-speed Internet access but do not provide the method to build enterprise networks, just this makes VPN has a role to play. VPN technology can build a secure, private and can be fully controlled enterprise network in high-speed, low-cost and unsecured Internet [4] (as shown in Figure 1).

2   Function Properties of VPN

Virtuality: Different from traditional private network, VPN does not establish a permanent connection, when the end-to-end connection disconnects the physical resources released can be used for other things [5].

Security: VPN enhances the security of network in many ways and ensure safety and reliability by providing identity authentication, access control and data encryption [5]. Low cost: Users do not lease special line to construct private network and do not need large numbers of network maintenance personnel and device investment [5].

Easy to implement and extend: Network route device's configuration is simple, without adding too much device, saving human and material resources[5].

Since VPN based a series of open protocols, the implementation means of VPN can be quite flexible. Users can select the appropriate solutions according to cost, implementation complexity, performance, management features and the company's system requirements .
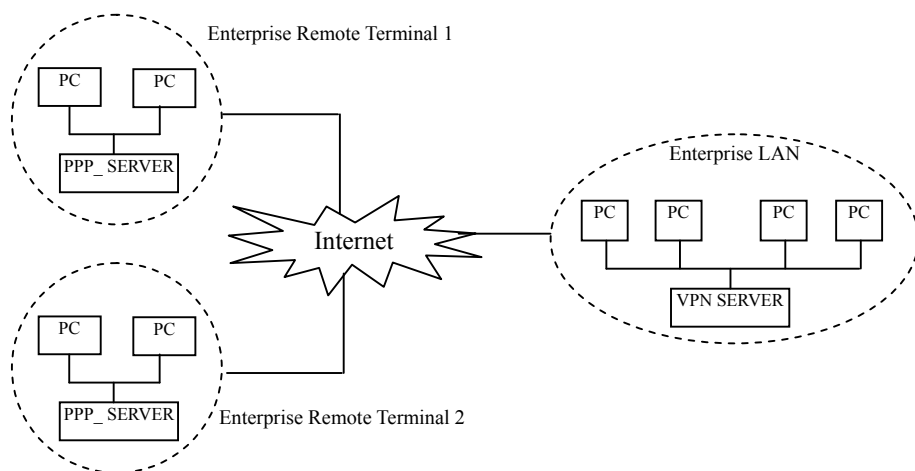
Fig. 1. Enterprise VPN Structural

3   Implement VPN by Installing the Software on Existing Device

For the existing network of company, building VPN by installing software is easier and faster than by purchasing new device. There are approximately three methods to build VPN by installing software as follows: router-based VPN, server software-based VPN, firewall-based VPN. Although the three devices are very different, but in the course of implementation there are many similarities (as shown in Figure 2).

The companies select which program to implement the VPN according to its network policies. Some of the companies' network is router-focus, may decide to add VPN services to router. Some of the companies' network is LAN-focus, and the server will become the main considerations of plan. In addition, some companies look the firewall as the nucleus of security Internet communication, which leads to the selection of the VPN-based firewall plan.

In these plans, there is not a plan better than another one. When building whole company VPN plan, each method has its advantages and corresponding disadvantages.
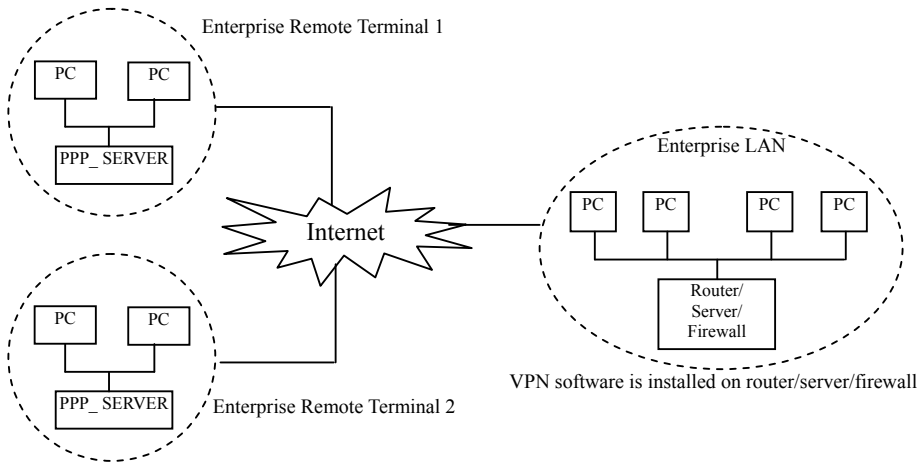
Fig. 2. Software –based VPN

3.1   Router-Based VPN

Installing VPN software on the existing router means no additional internal network devices in network. At present, most manufacturers of router have added VPN services to their products. By means of routers that have VPN functions, network managers are able to communicate with branches through Internet or other network provided by certain service providers. The dial-up users are able to build the tunnel on the service provider network to access the company's network.

To the managers of network, the most attractive point of the router-based method is that the addition of VPN service to router is usually just a software upgrade, in most cases, simply from the manufacturer's website to download some software or from the manufacturer to get some disks. Installing them on the existing router, it can achieve the VPN extension to the existing network functions.

New router usually has the software packages of VPN service module or includes the VPN function within the router's operating system. Typically, the additional VPN software packages of router contain the encryption and tunneling capabilities, some manufacturers connect the user authentication to the existing authentication services server.

Additional software on the router-based approach means that the existing management system can still be used in VPN, thus there is no need to train IT staff for new device or management systems. This also has other advantages such as simple configuration, multi-level Qos achievement, system stability, affordable and so on. Another advantage of router-based approach is not necessary to change the existing network, thus can save operating costs and reduce the total cost of using VPN.

3.2   Server Software-Based VPN

Another way to build VPN is to install a direct software-based VPN. Operating system providers and some third-party software companies provide VPN applications of encryption and tunnel authentication services to connect users to a VPN. This

method is similar with the router-based VPN method, which allows the use of existing device. Software is installed on an existing server, which means you can keep the same network configuration and management skills and tools to manage VPN. Therefore, we do not need additional training or management software to maintain the VPN connection and running.

Another advantage of Software-based VPN lies in that the program regularly is related to the authentication services of the existing network operating systems, thus it can connect VPN access right to the defined user rights, so can greatly simplify VPN management.

Before adopting software-based VPN, an important factor must be considered is efficiency. In the case of router-based VPN, the performance is a matter, executing the encryption and tunneling task of VPN need to consume processor power.

Assessing such a VPN method there is a problem that there is not a standard to determine the processor loading on a server accurately. The factors of determining load contain the number of concurrent VPN sessions must support, each session encryption level, the tunnel type and the data transmission rate.

Obviously, comparing with the remote dial-up provided by the service providers only supporting some analog telephone line, connecting hundreds of branches to a central site need a more powerful processor. The consequences of high load may not be the same, have to limit the numbers of concurrent sessions supported and lead to some users cannot connect.

3.3   Firewall-Based VPN

Many companies put their focus on the firewall to preclude hackers. For these network managers, it is meaningful to add the VPN security services to their firewall. Currently, many manufacturers provide services supporting VPN in their firewall, the more support VPN services by means of software, it provides a simple way for network managers to start using VPN. Network managers can install some new extra software packages simply on certain firewall. In some cases, only pay an additional fee to get the technical support of VPN services.

In such VPN, encryption, tunneling and other technologies are implemented by software; performance will be a problem too, just same as the methods of routers-based VPN and servers-based VPN. Essentially, these tasks may consume more processing power than that provided by the firewall. If performance becomes an issue, you may need more high-performance firewall.

Under what circumstances is it best to select the firewall-based VPN? When the remote users in the network may be unfriendly, it is best to use this product. Network managers create a DMZ (Demilitarized Zone) segment; generally, firewall uses a third-party interface, coupled with access control rules. Hackers may enter the DMZ, but they cannot destruct the internal network segment.

For pure internal network, using the firewall-based VPN is economical and easy to strengthening and management. For the external network, the firewall must use one rule that allows the encryption traffic to be sent from Internet to the DMZ (Demilitarized Zone) and the other rule that allows the application traffic to be sent from the DMZ to internal network. If the authentication server on the internal network, it is in need of configuring the firewall in order to transfer the authentication requests between the DMZ and private network.

The firewall-based VPN takes advantage of security mechanisms of firewall, including access restrictions for the internal network. It also performs address translation, consistent with strong authentication requirements, to issue real-time alerts, and provides extensive logging capabilities. Most firewall in commerce cut off the risk service and extra service of the host operating system, thus strengthen the operating system kernel. Operating system protection is a major additional feature.

4   Buy the Dedicated (VPN) Device

Special device is designed to fundamentally implement the task of connecting users and sites through VPN. In particular, the dedicated VPN device handles the encryption and tunnel services for the multiple concurrent VPN sessions. They usually use the specially designed hardware for these tasks. Like any network operated by the hardware, these devices have their advantages and relevant considerations. The major advantage of using the dedicated VPN device lies in its performance. These products have different specifications, but its high-end models can support more concurrent VPN sessions than the software VPN running on the server, router or firewall. In addition, dedicated VPN device also typically supports more sessions under circumstance of a high-strength encryption and data traffic load. Using the dedicated VPN device to implement VPN services means that other devices on the network, such as router, server or firewall do not experience performance problems.

Despite the high performance and the ability of maintain the performance of existing network is the benefit of using dedicated VPN device, but still exist shortness. One of the most serious points is the network configuration must be changed as the consequence of adding device to the network.

There are the dedicated VPN products in present market. Technically, the encryption tunnel can certificate and connect the different platforms and termination, including firewalls, routers, PC (using software) and the dedicated VPN device. Each device of these platforms relates to benefits and costs. However, no matter what platform or device is used, the encryption methods of protecting the safety of the VPN tunnel are same. Hardware-based solutions typically require large-scale hardware configuration, the dedicated and based the existing device of client VPN is suitable for large-scale remote access applications. Using VPN concentrator, its routing greatly improves the flexibility of remote Internet device; there are obvious advantages in security, manageability (especially implementation of the strategic management), scalability, maintainability, cost effectiveness, transmission qualities and other aspects, it is a VPN application innovation.

VPN concentrator is an ideal solution for remote access VPN. It includes easy to use standards-based VPN client, scalable VPN tunnel termination devices and gateways, as well as enables customers to easily install, configure and manage their remote access VPN client management system. By combining high-availability features with the unique dedicated remote access architecture, VPN concentrator enables customers to build high-performance, scalable and solid VPN infrastructures to support remote access applications of their critical business. VPN concentrator is an extendible platform that supports to provide the components of field replacement and customers upgrading.

VPN concentrators' advantages are: (1) easy to deploy, by integrating a routing engine, the packet filtering firewall and the abundant support to certification database, concentrator can be installed in the network infrastructure and the existing architecture has no obvious changes. (2) High performance and scalability, high modularization level, all of the options can be field installed, fully configured platform can support up to 100Mbps of 3DES encryption throughput. (3) The powerful management, VPN concentrators have intuitive and easy to use management interface, although very powerful, but complex underlying technology organized in a very simple way, so that the new users can easily configure the device and management.

5 Conclusion

From the above analysis, we can educe that the approaches of establishment and implementation of VPN generally are only two ways: using software technology to build a VPN and using hardware method to build VPN[7].

Pure software VPN products can protect the original investment without any additional hardware. Do not change existing applications and network architecture, and ensure the normal operation of businesses avoid effect. Support a variety of accesses to network, no lines, supports dynamic IP Addressing. for saving enterprises' costs, the network platform has strong adaptability, good scalability, and supports any C/S, B/S structure software. Economic efficiency, easy to use and do not need professionals to maintain. Using advanced encryption algorithms to prevent data from eavesdropping and distorting.

Using hardware to implement VPN refers the encryption and decryption to a special high-speed hardware to process, provides better performance and provides a strong physical and logical security to prevent illegal invasion better. Its configurations and operations are simple. In general, the hardware program's cost performance is higher.

References

1. Liu, H.-j., Yang, Z.-q.: Research on VPN based on MPLS. The Computer Security 20(8), 38–40 (2007)
2. Liu, H., Yang, S., He, D., Xia, W.: Design And Implementation Of An Ipsec Vpn Education Experiment System. Computer Applications and Software 23(7), 3–4 (2006)
3. Zhao, X.: Research and Simulation on Network based on MPLS. ChongQing Engineering College Journal 21(4), 36–38 (2007)
4. Dennis, F.: Netnews: VPNS become a virtual reality. NetWorker 2(2), 5–8 (1998)
5. RFC 2764, A framework for IP based Virtual Private Networks
6. RFC 3031, Multi-protocol Label Switching Architectures
7. Jiang, D.-y., Lv, S.-w., Luo, X.-g.: Analysis on the Key Techniques in VPN. Computer Engineering and Applications 39(15), 173–177 (2003)
8. Li, M., Xu, H.-z., Chen, W.-p., Huang, T.: OMT: The application of object-oriented modeling technology. Journal of Northwest University (Natural Science Edition) 29(6), 507–509 (1999)

Embedded Smart Tracker Based on Multi-object Tracking

Xu Yan, Wang Lei, Liang Jianpeng, Li Tao, and Cao Zuoliang

Tianjin University of Technology, Xiqing District, Tianjin, China
{xuyan200612,yangawang,litao.tut}@163.com,
{jianpeng_liang,zlcao}@126.com

Abstract. This paper presents a high integrated and efficient embedded smart tracker with an Omni-vision tracking method to realize a real-time multi-object tracking. To achieve stable tracking, we improve a tracking method based on Mean Shift Embedded Particle Filter. An approach for image format conversion is used to provide front-end pretreatment. The tracker is composed of a Digital Signal Processor (DSP), a Field-Programmable Gate Array (FPGA), a CMOS image sensor and a Fisheye lens which can capture 180° view of the environment. Due to its small-size, the tracker could be flexibly applied to vehicle navigation, mobile monitoring and other related areas. We demonstrate the performance of the tracker and the method on several factors. Experimental results have been presented to show the accuracy and the robustness of the proposed system.

Keywords: omni-vision, multi-object tracking, embedded, smart tracker.

1 Introduction

Available digital trackers based on the single Complementary Metal Oxide Semiconductor (CMOS) have been a central concern commercially and sample the color spectrum using a monolithic array of color filters overlaid on the CMOS such that each sample point captures only one color band. The Bayer Array [1], as shown in Fig.1, is one of the common realizations of color filter array (CFA) [2] possible. Since each pixel contains only one spectral color, the other colors must be estimated using information from the neighboring area. In order to obtain a high definition color image, interpolation must be performed on the Bayer array image data. A preferable method performs this interpolation in this paper and attempts to limit hue transition.

Real-time object recognition and tracking is a challenging task in video sequence and has induced enormous interests. Particle filter [3] has been proven to solve the problems of non-linear and non-Gaussian successfully, which has been widely used in visual tracking. Nevertheless, the traditional particle filter [4] has limited identification power, particularly when the illumination is extremely volatile. Mean shift is a typical and popular method, which is a non-parametric method for climbing density gradients to find the peak of probability distributions [5]. However, if the background is complex or the object is moving with haste, the tracking normally makes for failure. Combining

the strengths of the two methods has been in application to hand tracking [7][8]. In this paper, we develop an algorithm based on Mean Shift Embedded Particle Filter, which embeds a region of interest (ROI) filter in it.

2   Interpolation Method

Since the characteristics of the Bayer pattern, as Figure.1 is shown, we must estimate the other colors via interpolation. There are a variety of methods available, the simplest being linear interpolation, which has a weakness in maintaining edge information. Taking account of the fisheye lens imaging features and the tracking algorithm required, we propose an interpolation based on bilinear which is a two part process, the first being a bilinear interpolation, and the second part being a color correction.
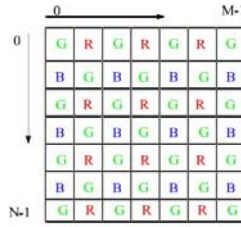
Fig. 1. Bayer pattern

Considering the array of pixels as shown in Fig.1, the green color is sampled at a higher rate than the red and the blue. In order to obtain an expected estimate for the missing sample value, we choice an interpolation filter kernel space of $3*3$ in the first part. At a blue centre B(x, y) (where blue color was measured), as shown in Fig. 2(a), we need to estimate the other two components. Consider (x, y) the pixel location and the red color is R(x, y); G(x, y) refers to the green color. Then, the estimates for R(x, y) and G(x, y) are as follows:

$$R(x,y) = \frac{f(x-1,y-1)+f(x+1,y-1)+f(x-1,y+1)+f(x+1,y+1)}{4}. \tag{1}$$

$$G(x,y) = \frac{f(x,y-1)+f(x,y+1)+f(x-1,y)+f(x+1,y)}{4}. \tag{2}$$

At the red centre R(x, y), we could computer the blue and the green accordingly. If G(x, y) represents the given pixel location, the value of the luminance (G) is measured. Referring to Fig. 2 (b), we can get:

$$R(x, y) = \frac{f(x, y-1) + f(x, y+1)}{2} \tag{3}$$

$$B(x, y) = \frac{f(x-1, y) + f(x+1, y)}{2} \tag{4}$$

B/R	G	B/R
G	R/B	G
B/R	G	B/R

G	R/B	G
B/R	G	B/R
G	R/B	G

(a)   (b)
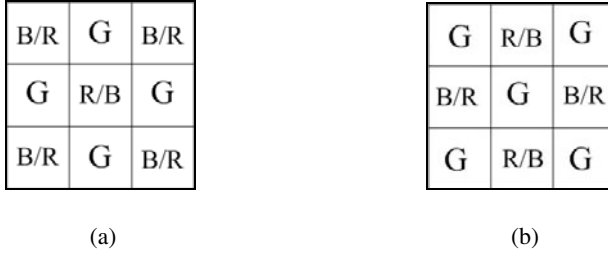
Fig. 2. The kernel of Bayer Array

In the second part, the color correction method is used to balance color consistency. Referring to (5)

$$
\begin{cases}
R(x,y) = R(x,y) \dfrac{\sum\limits_{I} R(x,y)}{\sum\limits_{I} f(x,y)} \\[3ex]
G(x,y) = G(x,y) \dfrac{\sum\limits_{I} G(x,y)}{\sum\limits_{I} f(x,y)} \\[3ex]
B(x,y) = B(x,y) \dfrac{\sum\limits_{I} B(x,y)}{\sum\limits_{I} f(x,y)}
\end{cases}
\tag{5}
$$

The f(x, y) is related as the current color value of the original Bayer array samples and 'I' represents the whole image.

3 Combination Algorithm Based On EMSPF

3.1 Particle Filter

Roughly speaking, visual tracking can be divided into two groups: deterministic tracking and stochastic tracking [6]. The approach we proposed combines the merits of both stochastic and deterministic tracking approached in a unified framework using particle filter and mean shift principle.

Particle filter is a sequential Monte Carlo approach based on point mass, which is an inference technique for estimating the unknown motion state X_k from a noisy collection of observations $Z_K = \{Z_1,...,Z_K\}$. The particle filter is a means to approximate the posterior distribution $p(x_k, z_k)$ by a set of weighted particles $\{x_k^i, w_k^i\}_{i=1}^{N}$ with $\sum_{i=1}^{N} w_k^{(i)} = 1$ and then the work is reduced to computing and updating the posterior probability over the current motion state X_k iteratively. Assuming that the probability density function $p(x_{k-1}|z_{1:k-1})$ is given at the time k-1, and then the prior probability $p(x_k|z_{1:k-1})$ at time k could be estimated as follows:

$$p(x_k|z_{1:k-1}) = \int p(x_k|x_{k-1})p(x_{k-1}|z_{1:k-1})dx_{k-1} \tag{6}$$

According to the Bayesian formula, the new prior probability is updated as:

$$p(x_k|z_{1:k}) = \frac{p(z_k|x_k)p(x_k|z_{1:k-1})}{p(z_k|z_{1:k-1})}. \tag{7}$$

Where $p(z_k|x_k)$ represents the likelihood function that an object being in a specific state. Based on the Monte Carlo approximation of the integral, the posterior probability is estimated as follows:

$$p(x_k|z_k) \approx kp(z_k|x_k)\sum_{i=1}^{N} w_{k-1}^{(i)}p(x_k|x_{k-1}^{(i)}) \tag{8}$$

3.2   Combination Algorithm Based on Mean Shift Embedded Particle Filter

Considering the general particle filter algorithm, when the targets begin to be tracked, the particles are generated around the targets randomly. If the targets move with haste, the tracking will be failure and the particle filter tracking window might drift. To obtain stable and accurate tracking, a large number of particles are required which would cost massive operation time. It is impractical for real-time system. Reference [6] introduces a method combining mean shift algorithm and particle filter for tracking hand. In our embedded navigation system, we improve the MSEPF method. Our method is described as the following: the first sample particles are generated by the particle filter, which is called Particle Sets Initialization. Next, particles move along the gradient direction estimated by Mean Shift to find the maximum location where the particles would be re-assigned closer to the real target area. After Mean Shift, each particle has a larger weight. Then filter the particles with low weight in a region of interest (ROI). If the weight is still below a threshold, then resample a new set of particles.

The principal steps in the MSEPF algorithm are:

STEP 1. Initialization

Generate a new set of particles $\{x_o^i, w_o^i\}_{i=1}^{N}$ and estimate the state according to the initial distribution $p(X_0)$.

STEP 2. Propagation

Draw samples $Z_k^{(i)}$ according to

$$p(Z_k^{(i)}|X_{0:k-1}^{(i)}) \qquad i = 1, 2, \ldots, N \tag{9}$$

STEP 3. Weighting Calculate the weight using

$$\widetilde{w}_k^{(i)} = w_{k-1}^{(i)}p(Z_k|X_{k-1}^{(i)}) \qquad i = 1, 2, \ldots, N \tag{10}$$

Normalize the weight using

$$w_k^{(i)} = \frac{\widetilde{w}_k^{(i)}}{\sum\limits_{i=1}^{N} \widetilde{w}_k^{(i)}} \qquad i = 1, 2, \ldots, N \tag{11}$$

Then predict the posterior distribution using

$$p(\widetilde{Z}_K | Z_K) = \sum_{i=1} w_k^{(i)} \delta(X_k - X_k^{(i)}) \tag{12}$$

Where $\delta(x)$ is the Dirac delta function.

STEP 4. Shifting

Shift the particles around their centre until they reach their maximum weight. The principle is described as:

$$y_1 \frac{\sum_{i=0}^{N} x_i w_j g\left(\left\|\frac{y - x_i}{h}\right\|^2\right)}{\sum_{i=1}^{N} w_i g\left(\left\|\frac{y - x_i}{h}\right\|^2\right)} \qquad i = 1, \ldots, N \tag{13}$$

STEP 5. ROI Filtering

According to $\left\{X_k^{(i)}, w_{k-1}^{(i)}\right\}_{i=1}^{N}$, adopt preferable ROI window to degrade low weight particles.

STEP 6. Resample

If the weight is also below a threshold, resample new particles $X_k^{(i)}$ to obtain N independent and identically distributed random particles $X_k^{(j)}$ approximately distributed according to $p(Z_k | X_k)$.

STEP 7. Return to step2 and set $k = k + 1$.

4   Smart Tracker

The programmable smart tracker is designed to merge the image acquisition, image processing and data output into a unified framework. The central components the smart tracker equipped with are: a CMOS digital image sensor, a FPGA, a high-performance DSP and an extremely wide angle lens.

4.1   The Image Acquisition Module

It contains two parts: fisheye lens and CMOS image sensor. The COMS digital image sensor we choose in this module is Micron's MT9V022 [9], for its rugged specs and high quality for scene-understanding and smart imaging applications. The COMS is

connected to the fisheye lens and adapted to output digital image data of a view field. The MT9V022 pixel array is configured of 782 columns by 492 rows and the active imaging pixel array is 752H×480V. In default mode, the MT9V022 could output a wide-VGA-sized image at 60 frames per second (fps).

4.2   The Image Processing Module

This module is equipped with a Field-Programmable Gate Array (FPGA) [10], a Flash memory, and a Digital Signal Processor (DSP). The FPGA we employ Altera's EP2C20, which is connected to the CMOS, and could be used to command capturing time sequence of the CMOS image sensor and then store the image data into the Synchronous Dynamic Random Access Memory (SDRAM). The DSP we select TI's TMS320DM642 processor [11], which is a high-performance fixed-point DSP and is good at digital media applications.

4.3   Data Communication Module

This module contains necessary communication interfaces, e.g. Ethernet, as well as JTAG for connected to the PC with emulator. The user could input data, such as aim points and feature through the Ethernet interface. It could also receive image data processed by DSP and transmit beacons tracking information to PC or other external devices.

(a)

(b)

(c)

(d)
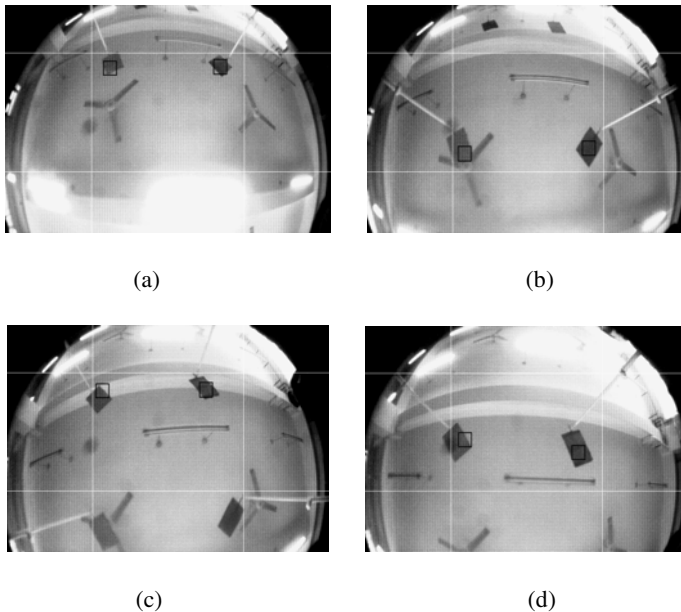
Fig. 3. Experimental results of the smart tracker based on combinational algorithm

5   Experimental Result

In our implementation, we use the following choice to demonstrate our algorithm and the smart tracker. We fix our smart tracker vertically on the top of an autonomous guiding vehicle (AGV), to track the double-color beacons.

When the vehicle is moving at a variable speed, the results of tracking multi-object are shown in Fig. 2. The beacons move throughout the entire view field and the tracking method successfully tracks these beacons.

Comparing our method to traditional particle filter, though two of them use the same color histogram, the traditional particle filter is easily disturbed and our method is more effectual correspondingly. In the same tracking conditions, the number of particles of the algorithm embedded on Mean Shift is 40, which is only a quarter of the number of traditional particle filter. The rate of available particles is actually increasing from 25% to 35%, as Fig. 3(a) is shown.

| (a) | (b) | (c) |
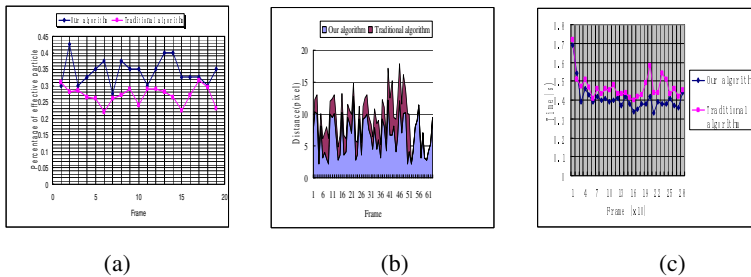
Fig. 4. Comparison of the two methods: (a) Percentage of the available particles (b) Astringency (c) Operation time

To further illustrate the importance of this built-up algorithm, we computed the distance between the particles to object, i.e. astringency. The result is presented in Fig.3(b). Finally, we illustrate the effectiveness of our method by comparing its operation time with the traditional particle filter as Fig.3(c) shown.

6   Conclusion

The experimental results strongly demonstrate that our smart tracker and the proposed algorithm are feasible to track a multiple objects with an indoor environment. While we have achieved a realistic tracker and a successful multi-object tracking, some limitations of our task remain to be addressed. If the background is complex or the object is moving with haste, the tracking normally makes for failure.

References

1. Ramanath, R., Snyder, W.E., Bilbro, G.L.: Demosaicking method for Bayer color arrays. J. Journal of Electronic Imaging 11(3), 306–315 (2002)
2. Doucet, A., Freitas, N.D., Gordon, N.: Sequential Monte Carlo Methods in Particle. Springer, New York (2001)
3. Cao, Z., Liu, S., Roing, J.: Omni-directional Vision Localization Based on Particle Filter. In: Fourth International Conference on Image and Graphics, Chengdu China, pp. 478–483 (2007)
4. Comaniciu, D., Ramesh, V., Meer, P.: Real-time Tracking of Non-rigid Objects using Mean Shift. CVPR, South Carolina 99, 142–149 (2000)
5. Zhou, S.K.: Visual Tracking and Recognition Using Appearance-Adaptive Models in Particle Filters. IEEE Transactions on Image Processing 13(11) (November)
6. Shan, C., Wei, Y., Tan, T., Ojardias, F.: Real Time Hand Tracking by Combining Particle Filter and Mean Shift. In: Proceedings of the Sixth IEEE International Conference on Automatic Face and Gesture Recognition, pp. 669–674 (2004)
7. Zhang, B., Tian, W., Jin, Z.: Joint tracking Algorithm Using Particle Filter and Mean Shift with Target Model Updating. J. Chinese Optics Letter 4(10), 569–572 (2006)
8. Micron, MT9V022 Producti Brief –rew.A 1/06 EN, Mircon Technology (2006)
9. Pellerin, D., Thibault, S.: Practical FPGA Programming in C. Prentice Hall PTR, Englewood Cliffs (2005)
10. Texas Instruments, TMS320DM642 Digital Media Processor. Texas Instruments (2008)

A Survey on Indoor Positioning Technologies

Zhenlong Song[1], Gangyi Jiang[1], and Chao Huang[2]

[1] Faculty of Information Science and Engineering, Ningbo University,
315211 Ningbo, China
[2] Institute of Computing Technology Chinese Academy of Science,
100080 Beijing, China
`szlzhenlong@163.com`

Abstract. Location-aware service is one of the most important parts of the internet of things. And how to obtain the location information is the key point of location-aware service. This paper investigates some key technologies and algorithms of indoor positioning and analyzes their advantages and disadvantages in the terms of the positioning range, accuracy and cost. Finally some issues need to be resolved in future are discussed.

Keywords: Location-aware service, positioning technology, Infrared, WLAN, Ultrasonic, RFID.

1   Introduction

Location-aware services have become more and more popular with the development of modern communication and internet of things. Indoor positioning applications show huge prospect in areas such as location-based network management and security, medicine and health care, personalized information delivery, and context awareness [1].

Well-known example of the earliest modern positioning system is Global Positioning System (GPS) [2], [3]. GPS receiver measures satellite signals from 5-24 satellites and utilizes the time difference of arrival (TDOA) to estimate the position. The highest positioning accuracy of GPS in outdoor environments can reach 5m [4]. In reality environments, however, the coverage of GPS is limited. Because of GPS satellites radio signals can not penetrate most of the buildings or dense vegetation, GPS can not react in high-rise urban areas or building where people often work and locate. In recent years, the cellular network-based location technology [5] also made rapid development as the promulgation of E-911 which had generally positioning accuracy of 50 meters for outdoor applications [6], [7], [8]. The 50-meter positioning accuracy, however, is not satisfied for indoor application [9]. The users desire to control the indoor positioning within several meters.

The location estimation accuracy of GPS or the cellular network-based location technology is often inadequate for indoor environment. In order to improve the accuracy of indoor positioning application, the research on indoor positioning technologies has attracted more and more scholars and research institutes.

2   Paper Preparation

At present, many technologies can be used for indoor positioning, such as infrared, ultrasonic, computer vision and radio frequency (RF). And the RF could be divided into four technologies by different specifications: ZigBee, Radio Frequency Identification (RFID), Ultra Wideband (UWB), and Wireless Local Area Networks (WLAN).

2.1   Infrared Positioning Technology

Infrared positioning technology firstly need to yield a certain time interval transmitting infrared signals by a emitter, then measure the position of the object according to the receiving time of infrared signals. The representative of infrared indoor positioning systems is the Active Badge location system which developed by W. Roy and others [10]. To use Active Badge, each user needs to carry small infrared marking equipment. The marking equipment sends a globally unique identification number every 15 seconds. The infrared sensors fixed in the building collect the data then transmit to a central server which accomplishes the positioning process. Active Badge is low cost and easy to use, but it is vulnerable to the impact of fluorescent and sunlight. In addition, the effective transmission range of this positioning technology is only a few meters since the poor penetration of infrared.

2.2   Ultrasonic Positioning Technology

Ultrasonic positioning technology used mainly reflective distance method to determine the location of the object. Active Bat system [11] is an ultrasonic indoor positioning system researched by AT&T Labs. When positioning, the central controller sends a request packet by radio, Active Bat shows a response by sending ultrasonic pulses to the signal receiver distributed in the ceiling upon receipt of request packets. The receiver on the ceiling is able to measure the time interval and calculate the distance between the receiver and Active Bat tag. Local controller transmits the measured distance information to the central controller which calculates the user's location technology using geometry. The system can control the positioning error within the 9cm. Ultrasonic positioning system requires large-scale layout with many of receiver hardware, and the positioning result is very sensitive with the environment.

2.3   Computer Vision Positioning Technology

Computer vision positioning technology estimates the location of objects by using image processing. Easy Living system is developed by Microsoft Research using computer vision technology [12]. Easy Living uses two real-time three-dimensional color camera Digiclops to locate, which can identify the status of multiple users by processing images. The accuracy of Easy Living is high. Positioning technology of computer vision can only locate in the line of sight (LOS), which is difficult to overcome the occlusion problem by the walls, obstacles. So the coverage of such systems is limited. The cost computer vision positioning technology is high because of needing the three-dimensional camera.

2.4   ZigBee Positioning Technology

ZigBee is a short distance, low-rate wireless network technology. This technology achieves positioning with the coordination of communications by thousands of tiny sensors. These sensors require very little energy to relay the data passing between the sensors adopted by radio waves, so the communication is very efficiently. Wireless Dragon positioning system is a representative ZigBee positioning system developed by Chengdu Wireless Dragon Communication Technology Co., Ltd. Wireless Dragon can be used for large areas by using CC2431 and CC2430. Because of the positioning accuracy of ZigBee positioning system is limited, C.Hyunggi proposed a maximum likelihood estimation method [13].

2.5   RFID Positioning Technology

Radio Frequency Identification (RFID) is a non-contact automatic identification technology, which automatic target recognition and access to relevant data radio through frequency signal. LANDMARCE positioning system is a RFID-based indoor positioning system developed by Michigan State University and the Hong Kong University of Science and Technology [14]. The system introduces the concept of reference tags. Reference tag placed in a fixed position, RFID readers compare the signal strength from the target and reference tags to determine the nearest reference tag from the target tag. Then the nearest reference tag gets a higher weight. The Location can be determined by the higher weight and the reference tag. G.Y. Jin, et al has been improved LANDMARC from the perspective of system energy consumption and system costs [15]. The disadvantage of such positioning systems is the RF signal influenced by the antenna, the role of proximity does not have the communications capabilities, positioning coverage is small, and not easily integrated into other systems.

2.6   UWB Positioning Technology

UWB location technology mainly utilizes the time of arrival (TOA) or the time difference of arrival (TDOA) of the RF signals to get the distance between the target and the reference point. Ubisense positioning system [16] is a UWB real-time positioning system developed by Cambridge University. Ubisense overcomes the constraints of line of sight (LOS) because of the UWB signal has a strong penetration. Ubisense can achieve real-time location positioning system utilizing the millisecond response time [17]. However, there are many issues of technical theory to be researched. UWB technology is not widely used on account of the high cost of UWB equipment. The research of the UWB location technology presently focuses on reducing the error of NLOS [18], [19] and improving the positioning accuracy [20].

2.7   WLAN Positioning Technology

WLAN positioning technology exploits received signal strength (RSS) or signal to noise ratio (SNR) for positioning. This positioning technology uses the WLAN client (laptop, PDA or smart phone) to get the RSS or SNR from wireless network interface card [21]. As wireless LAN is widely used in business districts, universities, airports

and other public areas, WLAN positioning technology is becoming to the hottest indoor localization application for which can take full advantage of these existing resources [22], [23], [24]. Horus positioning system is a representative WLAN-based indoor positioning system which designed by the University of Maryland [25]. Horus is a probability distribution based positioning system for wireless local area network, which in the offline stage stores the probability distribution histogram of RSS for each AP at the reference point in the database, and in the online positioning stage some certain matching algorithms are used to get the optimal estimating position. Horus proposed a method of clustering the location sets in the radio map to improve the searching speed and reduce the computation. Horus requires collecting large amounts of RSS at the reference locations in offline phase though the system is accurate.

3 Indoor Positioning Algorithm

Indoor positioning algorithm can be divided into four types according to the signal measurements: Time of Arrival (TOA), Time Difference of Arrival (TDOA), Arrival of Angle (AOA) and Received Signal Strength (RSS).

3.1 TOA Algorithm

TOA algorithm needs firstly to measure the signal transmission time between the receiver and the transmitter. The distance of the receiver and the transmitter can be got from the speed and the measured time of the signal. Then the location of target estimates by using triangulation [26]. If he distance of the target to the base station (BS) i is R_i, ($i = 1, 2, 3$), as shown in Fig. 1(a), the target must be in a circle. The center of the circle is the ith BS and the radius of the circle is R_i . Then the intersection of the circles is the position of the target. Suppose (x_0, y_0) and (x_i, y_i) represent the locations of the target and the ith BS respectively. They must meet the formula (1).

$$(x_i - x_0)^2 + (y_i - y_0)^2 = R_i^2 , i = 1, 2, 3 \tag{1}$$

Where i means the number of base stations involved. This method requires precise synchronized clock between the transmitter and receiver, which is high cost.

3.2 TDOA Algorithm

TDOA algorithm measures the propagation time difference among the target and the multiple base stations, and gets the distance difference from the time difference by multiplying the speed of the signal [27]. Let $R_{21} = R_2 - R_1$ is the distance difference between the target to BS1 and BS2, as shown in Fig. 1(b), the target must be located in the hyperbola which focuses on these two base stations. The target also locates in the hyperbolas which focus on BS1 and BS3 in a similar way. Then the intersections of two hyperbolas are likely to be the location of the target. That is, the locations of the target and base stations must meet the formula (2).
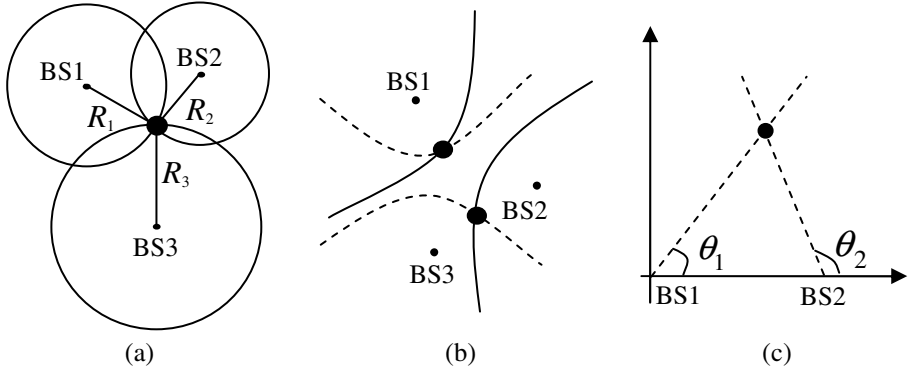
Fig. 1. Indoor positioning algorithms. (a) TOA algorithm. (b) TDOA algorithm. (c) AOA algorithm.

$$R_{i1}{}^2 = \left(\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2} \right), i = 2,3 \qquad (2)$$

This algorithm only needs synchronize the base stations participated in the positioning, without the precise synchronization between the target and the base station described in TOA. There are two solutions obtaining from formula (2), which corresponding to the two intersections of two hyperbolas. However, only one intersection is representative of the real location of the target, it needs some prior knowledge to distinguish true solution to eliminate the position ambiguity.

3.3   AOA Algorithm

AOA algorithm needs to detect the arrival of angle of incidence launched by the target wave through the base station antenna array. A radial attachment forms from the base station to the target, which is namely the azimuth line [28]. Using the angles offered by two or more than two base stations determines the azimuth lines. The intersection is the estimated position for target. The AOA algorithm is shown in Fig. 1(c). Assuming θ_1 and θ_2 represents the arrival of angles detected by the antenna of BS1 and BS2, respectively, then obtaining formula (3):

$$\tan \theta_i = (y_i - y_0) / (x_i - x_0) , i = 1, 2 \qquad (3)$$

By solving the above nonlinear equations can get estimated position of the target. AOA positioning technology needs to use the directional antennas, such as intelligent antenna array, which realizes complexly and costs greatly.

3.4   RSS Algorithm

RSS Algorithm estimates the position according to the Received Signal Strength (generally refers to radio frequency signal). RSS localization method can divide into two tepes: propagation model method algorithm and fingerprinting algorithm.
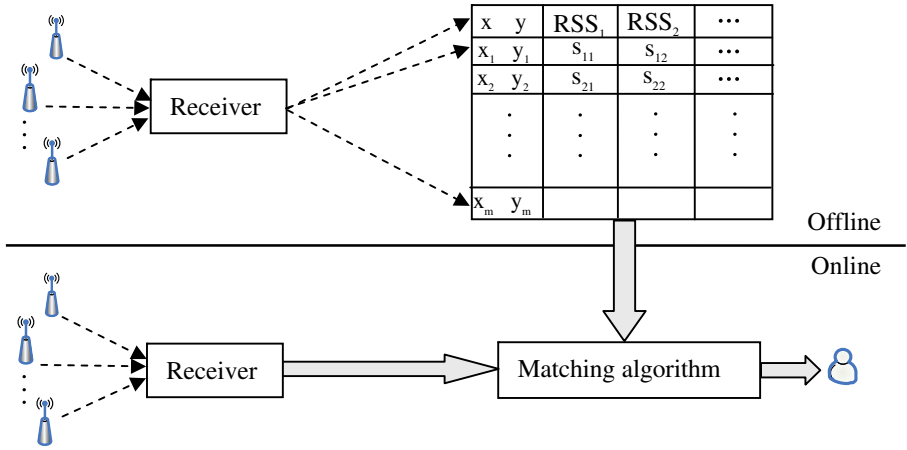
Fig. 2. Fingerprinting positioning method

Propagation model algorithm (PMA) needs to establish the model between RSS and the distance [29], [30]. Generally, the lager of the RSS values the closer from the access point (AP). In the open free space, attenuation of signal strength is inversely proportional to the distance from AP. But the indoor environment is very complex, the furniture, equipment windows and doors may cause multiparty propagation, such as reflection, refraction diffraction. And different structure of the obstacles may cause the different attenuation coefficient for RF signals. So the establishment of accurate indoor propagation model is very difficult.

Fingerprinting algorithm has two stages: offline phase for training and online phase for positioning [31]. Offline phase determines some reference locations, and stores the pre-recorded RSS and position coordinates in a database called Radio Map. Online phase estimates the location of the user by comparing the obtained RSS values to the radio map. The fingerprinting positioning algorithm is shown in Fig. 2. Fingerprinting algorithm needs not to establish the complex propagation model, but the workload is huge [32] and RSS values change susceptibly by multipath in the indoor environment [33]. Shihhau F. has proposed a dynamic system approach into the fingerprinting module to exploit the characteristic of the multipath effect [34], where the location is estimated from the state instead from RSS directly. The state is reconstructed from the temporal sequence of RSS samples by incorporating a proper memory structure. Because of the impact of the temporal variation due to multipath is considered a more accurate state location correlation is estimated.

4   Comparison of Indoor Positioning Technologies

The indoor locating technologies above have the advantages and disadvantages in coverage, location accuracy and system cost. All sorts of positioning technologies coexistence are possible in the future. The user may choose suitable positioning system according to his/her own needs. The comparison of indoor positioning technology is shown in Table 1.

Table 1. Comparison of indoor positioning technologies

Technology		System	Range	Accuracy	Algorithm	Cost
Infrared		Active Badge	5m	7cm	TOA/TDOA	Low
Ultrasonic		Active Bat	30m	9cm	TOA/TDOA	Moderate
Computer Vision		Easy Living	Rome Scale	10cm	Image Process	High
RF	ZigBee	Wireless Dragon	40m	3~5m	RSS- PMA	Moderate
	RFID	LANDMARCE	35m	2~5m	RSS-Fingerprinting / PMA	Moderate
	UWB	Ubisense	20m	10cm	TOA/TDOA	High
	WLAN	Horus	50m	2~3m	RSS-Fingerprinting / PMA	Low

5   Summary and Outlook

Location-based service is a very important basic link for Internet of Things and Smart City. Well-known positioning systems such as GPS and cellular network based systems can not be used effectively in indoor environments, motivating the research of other positioning technologies such as infrared, ultrasonic, computer vision and radio technologies. This paper analyzes the key technologies and algorithms of indoor positioning. The analysis shows that the different positioning technologies have their own advantages and disadvantages. On the whole, a breakthrough improvement of positioning accuracy is difficult to obtain from any of the single positioning technology. To achieve higher positioning accuracy, there must be appearing some systems fuse different positioning technologies considering the cost in future. In addition, the security of the positioning systems have little regarded currently. Although security is not the unique requirements of indoor positioning systems, security is a factor that must be considered, which makes sure the systems beyond attack. Thus the security issues of positioning systems will also be an important direction of indoor positioning research.

References

1. Hightower, J., Borriello, G.: Location Systems for Ubiquitous Computing. IEEE Computer Mag. 34(8), 57–66 (2001)
2. Mingfeng, L., Baohong, F., Sanzhi, L.: GPS positioning technology and application. National Defence Industry Press, Beijing (2006)
3. Enge, P., Misra, P.: Special issue on GPS: The Global Positioning System. Proceedings of the IEEE 87(1), 3–15 (1999)
4. Kaplan, E., Hegarty, C.: Understanding GPS: Principles and Applications. Artech House, Boston (2005)
5. Pingzhi, F., Ping, D., Lin, L.: Cellular wireless location. Electronic Industry Press, Beijing (2002)

6. FCC Docket No. 94-102: Revision of the Commission Rules to Insure Compatibility with Enhanced 911 Emergency Calling Systems. Federal Communications Commission Tech. Rep. RM–8143 (1996)
7. Zagami, J.M., Parl, S.A., Bussgang, J.J.: Providing Universal Location Services Using a Wireless E911 Location Network. IEEE Communications Magazine 36(4), 66–71 (1998)
8. FCC, Wireless 911 Services,
    `http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html`
9. The Definitive Wireless E-911 Reference Guide 2005. Mind Commerce (2005)
10. Want, R., Hopper, A., Falcao, V.: The Active Badge Location System. ACM Transactions on Office Information Systems (TOIS) 10(1), 91–102 (2003)
11. Ward, A., Jones, A., Hopper, A.: New Location Technique for the Active Office. IEEE Personal Communications 4(5), 42–47 (2004)
12. Microsoft Research. Easy living,
    `http://www.research.microsoft.com/easyliving`
13. Hyunggi, C., Myungseok, K., Jonghyuk, P., Byungsung, P., Hagbae, K.: Performance Analysis of Location estimation algorithm in ZigBee networks using received signal strength. In: 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINAW 2007, Niagara Falls, pp. 302–306 (2007)
14. Ni, L.M., Liu, Y.H., Lau, Y.C.: LANDMARC: Indoor Location Sensing Using Active RFID. Wireless Networks 10(6), 701–710 (2004)
15. Jin, G.Y., Lu, Y., Park, M.: An Indoor Localization Mechanism Using Active RFID Tag. In: Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitousand Trustworthy Computing, Taichung, pp. 4–8 (2006)
16. Steggles, P., Cadman, J.: A Comparison of RF Tag Location Products for Real World Applications. Technical report, Ubisense Limited (2004)
17. Gezici, S., Tian, Z., Giannakis, G.B.: Localization Via Ultra Wideband Radios: A look at positioning aspects of future sensor networks. IEEE Signal Processing Magazine 22(4), 70–84 (2005)
18. Angela, H., Ruben, B., Juan, C., Ignacio, A., Antonio, V.: Accurate Indoor Wireless Location With IR UWB Systems: A Performance Evaluation of Joint Receiver Structures and TOA Based Mechanism. IEEE Transactions on Consumer Electronics 54(2), 381–389 (2008)
19. Chinder, W., Chihsheng, H.: NLOS Mitigation With Biased Kalman Filters for Range Estimation in UWB Systems. TENCON 2007 IEEE Region 10 Conference, October 30-November 2, pp. 1–4, Taipei (2007)
20. Shaohua, W., Qinyu, Z., Naitong, Z.: NLOS error reduction methods in UWB dense multipath environment. Chinese of Journal Electronics 36(1), 39–45 (2008)
21. Azadeh, K., Konstantinos, N., Anastasios, N.: Venetsanopoulos. Intelligent Dynamic Radio Tracking in Indoor Wireless Local Area Networks. IEEE Transaction On Mobile Computing 9(3), 405–419 (2010)
22. Hamid, M., Nitin, K.T., Taravudh, T.: Indoor Positioning System Using Artificial Neural Network. Journal of Computer Science 6(10), 1219–1225 (2010)
23. Yinsen, F., Taichi, W., Shihyu, C., Hsipin, M.: Location Estimation in Indoor Wireless Networks by Hierarchical Support Vector Machines with Fast Learning Algorithm. In: International Conference on System Science and Engineering, Taipei, pp. 321–326 (2010)
24. Jaegeol, Y., Seunghwan, J., Kiyoung, G., Jaehun, J.: Improvement of Kalman filters for WLAN Based Indoor Tracking. Expert Systems with Applications 37, 426–433 (2010)
25. Youssef, M., Agrawala, A.: Handling Samples Correlation in The Hours System. IEEE Infocom (2004)

26. Zhao, F., Yao, W., Logothetis, C.C.: Comparison of Super-resolution Algorithms for TOA Estimation in Indoor IEEE 802.11 Wireless LANs. In: Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, Wuhan, pp. 1–5 (2008)
27. Tao, H., Xiaochun, L., Qi, L.: Pattern Recognition Based Kalman Filter for Indoor Localization Using TDOA Algorithm. Applied Mathematical Modelling 34, 2893–2900 (2010)
28. Roshanei, M., Maleki, M.: Dynamic-KNN: A Novel Locating Method in WLAN Based on Angle of Arrival. In: IEEE Symposium on Industrial Electronics and Applications (ISIEA), Kuala Lumpur, Malaysia (2009)
29. Fengyan, X., Liangbin, L., Zongxin, W.: A new regional division based on the distance of a loss model indoor WLAN positioning system. Journal of Electronics & Information Technology, 1405–1408 (2008)
30. Anvar, N., Yongwan, P., Kookyeol, Y., Jaehwang, Y.: A Fast and Accurate Calibration Algorithm For Real-Time Locating Systems Based on the Received Signal Strength Indication. International Journal of Electronics and Communications 64(11), 999–1104 (2010)
31. Honkavirta, V., Perala, T., Ali-Loytty, S., Piche, R.: A Comparative Survey of WLAN Location Fingerprinting Methods. In: Proceeding of The 6th Workshop On Positioning, Navigation and Communication, Hannover, pp. 243–251 (2009)
32. Kuofong, K., IEn, L., Jiasiang, L.: An Indoor Location-Based Service Using Access Points as Signal Strength Data Collectors. In: International Conference on Indoor Positioning and Indoor Navigation (IPIN), Zurich, pp. 1–6 (2010)
33. Chan, E.C., Baciu, G., Mak, S.C.: Effect of Channel Interference on Indoor Wireless Local Area Network Positioning. In: Wireless and Mobile Computing, Networking and Communications (WiMob), Niagara, pp. 239–245 (2010)
34. Shihhau, F., Tsungnan, L.: A Dynamic System Approach for Radio Location Fingerprinting in Wireless Local Area Networks. IEEE Transaction on Communications 58(4), 1020–1026 (2010)

A New Channel Calibration Method
of Eddy Current Array Technology

Bo Liu, Fei-Lu Luo, Meng-Chun Pan, and Liang-Jie Hou

National University of Defence Technology, Changsha 410073,
Hunan Province, China

Abstract. One of the preconditions of accurate defect feature extraction is the consistent channels of eddy current array testing equipment. This paper changes the problems of channel calibration into the regression analysis problems, and presents a new channel calibration method of eddy current array technology based on the crack features. Making use of the partial least-squares regression algorithm on the spline transform and the partial least-squares regression algorithm on the kernel function transform, the functions between the crack feature difference and amplitude of excitation, frequency of excitation, scan direction and detecting time, are set up. The experimental results show that the calibrated resolution of the partial least-squares regression algorithm on the spline transform is superior to the latter algorithm.

Keywords: Eddy Current Array, Channel Calibration, Partial Least-Squares Regressions, Crack, Feature Extraction.

1 Introduction

Eddy Current Array (ECA) technology is a new branch of nondestructive testing technologies. According to designing the coil units' placement specially and making full use of digital signal process technology, ECA can achieve the effective and rapid inspection of key components[1]. Needless of mechanical scanning equipment, eddy current array sensors need fewer time to detect large areas work-piece whose surfaces to check up are unfolded or closed, and can achieve the equal sensitivity compared to single coil inspection[2]. Therefore, in-service inspection (ISI) may be possible. ECA probe is one of the biggest evolutions in eddy current probe technology[3].

One of the most important advantages of ECA is that the coverage area of the ECA sensor is rather large and might be irregular shape adapted for many of components. However, the cost for the advantage is more and more coil units of ECA sensor and complex placement. More and more channels of ECA instrument bring on more advanced channel calibration method.

In recent years, almost all of the calibration methods are aimed at dealing with the raw detecting data. Because of the large mount of data and the complex of electromagnetic systems, the calibrated results are unsatisfied but the consumed time is quite long. This paper presents the calibration method based on crack feature. The method is not only short time consuming for the calibrated object is the crack feature, for example, length, depth, direction and etc, but also has higher calibration accuracy.

2   ECA Instrument, Sensor and Detecting Mode

2.1   ECA Instrument

As Fig.1 is shown, ECA instrument commonly consists of ECA probe, circuit of DDS(Direct Data Synthesize) signal generate, circuits of operational amplifier and power amplifier, analog switches array, orthogonal lock-in amplifier circuit(orthogonal LIA), signal acquisition, signal processing and ECA imaging. DDS generates single-frequency signals, dual-frequency signals or pulse signals. After filtering and amplification, signals drive ECA probe coil elements selected by analog switches array. Detecting coil elements can sense variation of the work-piece properties, and bring in harmonic signals, whose amplitude and phase's minute changes commonly measure by means of orthogonal LIA circuit. PCI card acquires detecting signals. Finally, ECA software complete signal processing and C scan image.
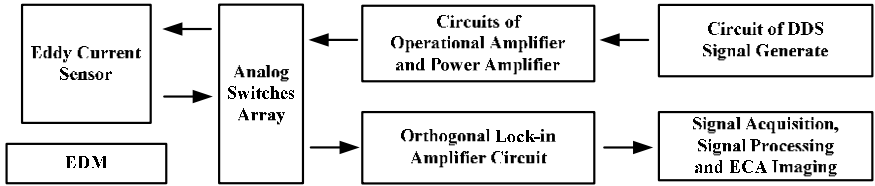
Fig. 1. This shows the whole principle block of ECA instrument
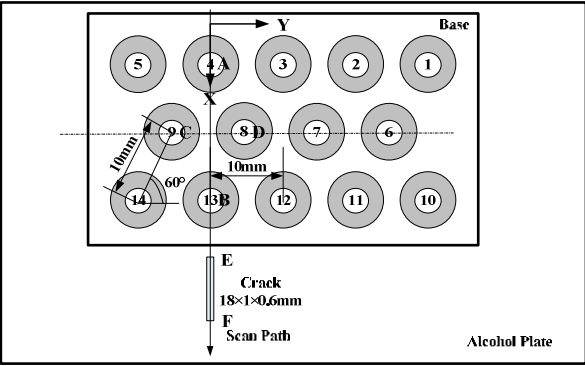
Fig. 2. This shows the ECA sensor. All coil units of the sensor has the same size. The outer radius of every coil unit is approximately 3.5mm, the inner radius is 1.0mm, the height is 3.0mm, the distance between two adjacent coil units is 10.0mm.

2.2   Sensor and Detecting Mode

Fig.2 is ECA sensor that this paper uses. According to the crack feature extraction methods, the detection mode of ECA instrument may be divided into inclined line mode, line mode and row mode. The amplititue curves of LIA output in each detecting mode has similar troughs and crests, but these feature points stand for different meanings.

3   Channel Calibration Method Based on Crack Features

In the online detecting process, the raw data are continuously acquired because of continuity testing. The task of signal processing and ECA imaging is difficult to complete. Therefore, the signal processing algorithms are almost simple and short time consuming. However, the ECA testing results are influenced by many of factors, such as the size of coil unit of ECA sensor, the placement of ECA, hardware of ECA excitation and conditioning, work mode, conductivity and permeability of components, defect feature, scan path, lift-off, environment noise and etc. The calibration methods directly dealing with the raw data can hardly trade-off in the time-consuming and resolution.

Another idea to consider this problem, reducing the amount of the data is key point. Acquired defect features are the main goal of ECA, therefore, firstly we can use the median filtering algorithm and the feature extraction method to the raw data, and then the crack features come into the dealing data of the channel calibration method. For the amount of data decreases remarkably, the time consuming of the channel calibration algorithm decreases, even we can develop more advanced channel calibration methods to acquire higher resolution. This method is adapted for the need for the defect feature extraction, but not suitable for C scan imaging data calibration.

Supposed amplititude of excited signal is x_1, frequency is x_2, scanning direction is x_3, detecting time point is x_4, defect feature is y, $G_{i,j} (i = 1, 2, 3, 4, j = 1, 2, \cdots, 32)$ is respectively channel calibration of x_1, x_2, x_3, x_4, $\varepsilon_k' (k = 1, 2, \cdots, 32)$ is random error of each channel after calibration, and then the mathematic model of channel calibration method based on crack features is that

$$\begin{cases} y + G_{1,1}(x_1) + G_{2,1}(x_2) + G_{3,1}(x_3) + G_{4,1}(x_4) + \varepsilon_1' = L \\ y + G_{1,2}(x_1) + G_{2,2}(x_2) + G_{3,2}(x_3) + G_{4,2}(x_4) + \varepsilon_2' = L \\ \qquad \cdots\cdots \\ y + G_{1,32}(x_1) + G_{2,32}(x_2) + G_{3,32}(x_3) + G_{4,32}(x_4) + \varepsilon_{32}' = L \end{cases} \tag{1}$$

Change eq.1 into eq.2, y is changed into the difference between actual defect feature and the calculated result of the feature extraction method.

$$\begin{cases} y = g_{1,1}(x_1) + g_{2,1}(x_2) + g_{3,1}(x_3) + g_{4,1}(x_4) + \varepsilon_1 \\ y = g_{1,2}(x_1) + g_{2,2}(x_2) + g_{3,2}(x_3) + g_{4,2}(x_4) + \varepsilon_2 \\ \qquad \cdots\cdots \\ y = g_{1,32}(x_1) + g_{2,32}(x_2) + g_{3,32}(x_3) + g_{4,32}(x_4) + \varepsilon_{32} \end{cases} \tag{2}$$

From eq.2 it is known that the channel calibration function can be evaluated by regression methods. Partial least-squares(PLS) regression, combining the advantages of linear regression, principal component analysis and canonical correlation analysis, is used to estimate eq.2[4].

(1) PLS Regression Based on the Spline Transform

To be convenient to describe the algorithm, the calibration methods of channel 1 are shown. Supposed $\hat{g}_{j,1}(x_j)(j = 1, 2, 3, 4)$ is the spline fitting function of $g_{j,1}(x_j)$ [5]

$$y = \beta_0 + \hat{g}_{1,1}(x_1) + \hat{g}_{2,1}(x_2) + \hat{g}_{3,1}(x_3) + \hat{g}_{4,1}(x_4) + \varepsilon_1 \tag{3}$$

If $\hat{g}_{j,1}(x_j)(j = 1,2,3,4)$ is cubic B-spline fitting function of x_j, and then

$$\hat{g}_{j,1}(x_j) = \beta_0 + \sum_{l=0}^{M_j+2} \beta_{j,l} \Omega_3 (\frac{x_j - \zeta_{j,l-1}}{h_j}) \tag{4}$$

In eq.4, $\beta_0, \beta_{j,l}$ are model parameters to be determined, and Ω_3 is cubic B-spline fitting basis function, it is shown as

$$\Omega_3 (\frac{x_j - \zeta_{j,l-1}}{h_j}) = \frac{1}{3!h_j^3} \sum_{p=0}^{4} (-1)^p \begin{pmatrix} 4 \\ p \end{pmatrix} (x_j - \zeta_{j,l-3+p})_+^3 \tag{5}$$

Combine eq.3 with eq.4, the nonlinear relationship of the difference of feature y and x_1, x_2, x_3, x_4 can be described as

$$y = \beta_0 + \sum_{j=1}^{4} \sum_{l=0}^{M_j+2} \beta_{j,l} \Omega_3 (\frac{x_j - \zeta_{j,l-1}}{h_j}) + \varepsilon_1 \tag{6}$$

It is seen that the relation of y and $z_{j,l} = \Omega_3[(x_j - \zeta_{j,l-1})/h_j]$ in eq.6 is linear, and can be transformed into a linear regression model. To avoid multicollinearity in the process of calculating the linear regression model, use partial least squares method to solve the model.

(2) PLS Regression Based on the Kernel Function

The solving problem process of PLS regression based on the Kernel function is similar to the process of PLS regression based on the Spline transform. The difference of these two algorithms is that each dimension nonlinear function of the former is decomposed by the kernel function transform, while each dimension nonlinear function of the latter is decomposed by the cubic B-spline fitting basis function transform.

The Gaussian kernel function is shown as the below eq.7:

$$\left\{ K(\frac{x - \zeta_{l-1}}{h})(a \leq x \leq b; l = 0,1,\cdots,M_j + 2) \right\} \tag{7}$$

Specific calculation process can be referred in reference [6]. The nonlinear relationship of the difference of feature y and x_1, x_2, x_3, x_4 can be described as eq.8.

$$y = \beta_0 + \sum_{j=1}^{4} \sum_{l=0}^{M_j+2} \beta_{j,l} K(\frac{x_j - \zeta_{j,l-1}}{h_j}) + \varepsilon_1 \tag{8}$$

4   Experiment and Results Analysis

To ensure accuracy of the calibrated results, the process of requiring the raw data consists of four steps. Step 1, set the amplitude of excited signals from 6.0V to 10.0V, and then test the work-piece with crack 18×1×0.9mm; Step 2, set the frequency of excited signals from 4.0kHz to 40.0V, and detect the crack; Step 3,

change the scan direction from 0^0 to 180^0, and detect the crack; finally, when the detection time is every two minutes point, such as 2, 4, 6,…, etc, after setting up the ECA instrument, and detect the crack. The raw data gained as the above are denoised by the median filter and the crack feature data is calculated by the crack feature extraction method.
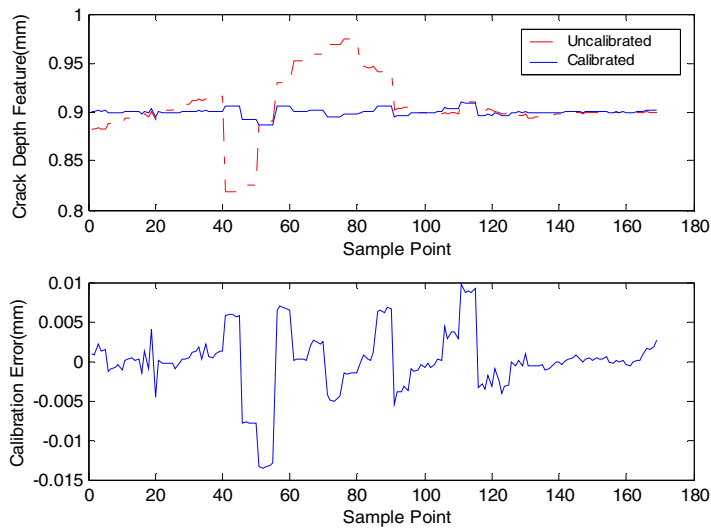
Fig. 3. This shows the calibrated results of the crack depth in PLS regression based on the Spline transform
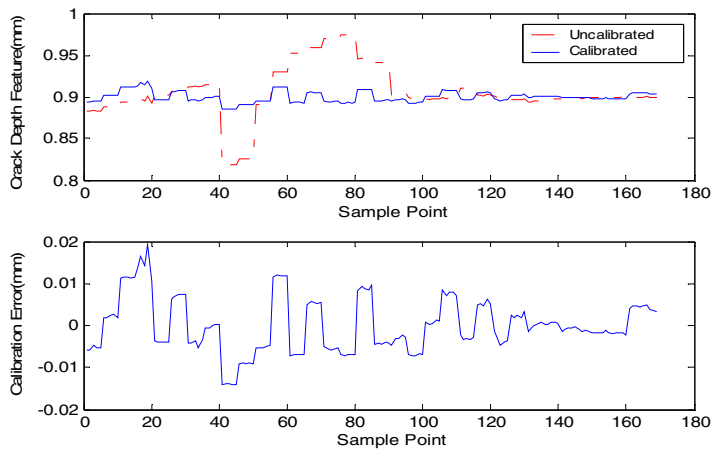
Fig. 4. This shows the calibrated results of the crack depth in PLS regression based on the Kernel function

PLS regression based on the Spline transform and PLS regression based on the Kernel function is respectively used to dealing with the crack feature data. The segment numbers of 4 independent variables of the two algorithms are 4, and the principal components of the former PLS algorithm is 6, while the principal components of the latter is 7. Percentage of the maximum absolute error of the former PLS algorithm is 1.09%, and that of the latter is 2.14%. The variance of the former PLS algorithm is 0.0040, and that of the latter is 0.0064. It is seen from the above analysis, the calibration method fulfilled by PLS regression based on the Spline transform is superior to the calibration method fulfilled by PLS regression based on the Kernel function in the crack quantitative detection of ECA.

5   Conclusion

This paper presents a new channel calibration method of ECA testing, and transforms the channel calibration of ECA testing into the difference between actual defect feature and the calculated result of the feature extraction method regression analysis. The experimental results verify the algorithm is short time consuming, and have a higher resolution in the crack quantitative detection of ECA.

References

1. Plotnikov, Y., Wang, C., McKnight, W., Suh, U.: Eddy Current Inspection of Components With Complex Geometries. Review of Quantitative Nondestructive Evaluation 27, 376–383 (2008)
2. Chen, X., Ding, T.: Flexible eddy current sensor array for proximity sensing. Sensors and Actuators A 135, 126–130 (2007)
3. Bureau, J.-F., Ward, R.C., Jenstead, W.: Advances in Eddy Current Array Sensor Technology. In: 17th World Conference on Nondestructive Testing, Shanghai, China (2008)
4. Li, Y., Ren, F., Li, X., et al.: Soft sensoring of applied aviation kerosene dry point based on partial least-squares regression of spline transformation. Computers and Applied Chemistry 26, 300–304 (2009)
5. Wang, H., Wu, Z., Meng, J.: Patial least-squares regression linear and nonlinear methods. National Defense Industry Press, Beijing (2006)
6. Meng, J., Wang, H., Huang, H., et al.: Nonlinear Structure Analysis with Partial Least-squares Regression Based on Kernel Function Transformation. Systems Engineering 22, 93–97 (2004)

Fault Diagnosis of Automotive Engines Using Fuzzy Relevance Vector Machine

Pak-Kin Wong[1], Chi-Man Vong[2], Zaiyong Zhang[1], and Qingsong Xu[1]

[1] Department of Electromechanical Engineering, University of Macau,
Taipa, Macau
[2] Department of Computer and Information Science, University of Macau,
Taipa, Macau
{fstpkw,cmvong,ma96593,qsxu}@umac.mo

Abstract. For any faults of automotive engines, the diagnosis can be performed based on variety of symptoms. Traditionally, the description of the faulty symptom is just existence or not. However, this description cannot lead to a high accuracy because the symptom sometimes appears in different degrees. Therefore, a knowledge representation method which could precisely reflect the degree of the symptom is necessary. In this paper, the fuzzy logic is firstly applied to quantify the degrees of symptoms. A probabilistic classification system is then constructed by using the fuzzified symptoms and a new technique namely Fuzzy Relevance Vector Machine (FRVM). Moreover, both Fuzzy Probabilistic Neural Network (FPNN) and Fuzzy Probabilistic Support Vector Machine (FPSVM) are used to respectively construct similar classification systems for comparison with FRVM. Experimental results show that FRVM produces higher diagnosis performance than FPNN and FPSVM.

Keywords: Fuzzy Probabilistic Neural Network, Fuzzy Probabilistic Support Vector Machine, Fuzzy Relevance Vector Machine, Engine fault diagnosis.

1 Introduction

The engine fault rate always ranks first among the vehicle components because of its complex structure and the running conditions. Accordingly, how to detect engine problems is of importance for vehicle inspection and maintenance. So the development of an expert system for engine diagnosis is currently an active research topic. Traditionally, the description of the engine faulty symptom is just existence or not. However, this description cannot lead to a high diagnosis performance because the symptom always appears in different degrees instead of existence or not. Moreover, the engine fault is sometimes a simultaneous fault problem, so the occurrence of the engine fault should also be represented as probability instead of binary or fuzzy values. In addition, the relationship between faults and symptoms is a complex nonlinearity. In view of the natures of the above problems, an advanced expert system for engine diagnosis should consider fuzzy logic and probabilistic fault classifier to quantify the degrees of symptoms and determine the possibilities of simultaneous faults respectively. By fuzzy logic technique, the symptoms are

fuzzified into fuzzy value and then based on the values, diagnosis is carried out. By going through multi-fault classification or identification, the output of the diagnostic system is then defuzzified into fault labels.

Recently, many modeling/classification methods combined with fuzzy logic have been developed to model the nonlinear relationship between symptoms and engine faults. In 2003, Fuzzy Neural Network (FNN) was proposed to detect diesel engine faults [1]. Vong et. al, [2, 3] applied multi-class support vector machine (SVM) and probabilistic SVM for engine ignition system diagnosis based on signal patterns. Both FNN and FSVM have their own limitations. For FNN, firstly, the construction of FNN is so complex (involving number of hidden neurons and layers, and trigger functions, etc) that the choice of them is difficult. Improper selection will result in a poor performance. Secondly, the network model depends on the training data, thus, if the data is not large enough, the model will be inaccurate, but if it is excessive, which causes overfitting problem, then the FNN model will be inaccurate either. As for FSVM, it suffers from solving the hyperparameters. There are two hyperparameters (σ, c) for user adjustment. These parameters constitute a very large combination of values and the user has to spend a lot of effort for value selection.

Relevance Vector Machine (RVM) is an emerging machine learning technique motivated by the statistical learning theory, and it gains popularity because of its theoretically attractive features and its performance is generally superior to the neural network and support vector machine [4, 5]. Besides, RVM can also be used a probabilistic classifier. In 2008, a kind of Fuzzy Relevance Vector Machine (FRVM) was proposed for learning unbalanced data and noise in patterns [6]. In 2010, RVM and fuzzy system were combined for multi-objective dynamic design optimization [7]. Nevertheless, there is no research applying fuzzy RVM to any diagnosis problems yet. So a promising avenue of research is to apply FRVM to automotive engine simultaneous fault diagnosis.

In this paper, a new framework of FRVM is presented for fault diagnosis of automotive engines. Firstly, fuzzy logic gives the memberships of the symptoms depending on their degrees. Then, RVM is employed to construct some probabilistic diagnostic models or classifiers based on the memberships. Finally, a decision threshold is employed to defuzzify the output probabilities of the diagnostic models to be decision values.

2   System Design

Depending on domain analysis, the typical symptoms and engine faults are listed in Tables 1 and 2, respectively. Table 3 shows the relationship between the symptoms and the engine faults. If one engine is diagnosed with the ith fault, then y_i is set as 1, otherwise it will be set as 0. Hereby, the symptoms of one engine could be expressed as a vector $\mathbf{x}=[x_1, x_2,..., x_{11}]$. Similarly, the faults of an engine are also expressed as a binary vector $\mathbf{y}= [y_1, y_2,..., y_{11}]$.

Table 1. Typical engine symptoms

Case no.	Symptoms
x_1	Difficult-to-start
x_2	Stall on occasion
x_3	Backfire during acceleration
x_4	Unstable idle speed or misfire
x_5	Sluggish acceleration
x_6	Knocking
x_7	Backfire in exhaust pipe
x_8	Abnormal inlet pressure
x_9	Abnormal throttle sensor signal
x_{10}	Abnormal coolant temperature
x_{11}	Abnormal lambda signal

Table 2. Typical engine faults

Label	Engine faults
y_1	Idle-air valve malfunction
y_2	Defective ignition coil
y_3	Incorrect ignition timing
y_4	Defective spark plug
y_5	Defective throttle valve
y_6	Leakage in intake manifold
y_7	Defective air cleaner
y_8	Defective injector
y_9	Defective fuel pump system
y_{10}	Defective cooling system
y_{11}	Defective lubrication system

Table 3. Relationship of symptoms and possible engine faults

	y1	y2	y3	y4	y5	y6	y7	y8	y9	y10	y11
x1	√	√	√	√		√		√	√		
x2		√	√	√							
x3	√		√		√	√		√	√		
x4	√	√	√	√	√	√	√	√	√		
x5		√	√	√	√	√	√	√	√		
x6			√	√							
x7	√		√	√	√			√	√		
x8					√	√	√				
x9					√						
x10										√	√
x11		√		√		√		√			

2.1   Fuzzification of Input Symptoms

The engine symptoms have some degrees of uncertainties. So fuzzy logic is applied to represent these uncertainties and treated as system inputs. According to the domain knowledge, various membership functions for the inputs are defined below:

$$x_1 : \text{'Difficult-to-start'} = \frac{1}{\text{unable to start}} + \frac{0.7}{\text{able to crank but cannot start}}$$
$$+ \frac{0.3}{\text{immediately stall after starting}} + \frac{0}{\text{normal start}} \qquad (1)$$

$$x_2 : \text{'Stall on occasion'} = \frac{1}{\text{stall}} + \frac{0.7}{\text{severely unstable engine speed}}$$
$$+ \frac{0.3}{\text{unstable engine speed}} + \frac{0}{\text{stable engine speed}} \qquad (2)$$

$$x_3 : \text{'Backfire in acceleration'} = \frac{1}{\text{always}} + \frac{0.5}{\text{sometimes}} + \frac{0}{\text{normal}} \qquad (3)$$

$$x_4 : \text{'Unstable idle speed or misfire'} = \frac{1}{\text{misfire frequently}} + \frac{0.7}{\text{engine jerk}}$$
$$+ \frac{0.3}{\text{unstable engine speed}} + \frac{0}{\text{stable engine speed}} \qquad (4)$$

$$x_5 : \text{'Sluggish acceleration'} = \frac{1}{\text{misfiring during acceleration}}$$
$$+ \frac{0.7}{\text{unable to accelerate}} + \frac{0.3}{\text{accelerate very slow}} + \frac{0}{\text{normal acceleration}} \qquad (5)$$

$$x_6 : \text{'Knocking'} = \frac{1}{\text{serious}} + \frac{0.5}{\text{slight}} + \frac{0}{\text{no}} . \qquad (6)$$

$$x_7 : \text{'Backfire in exhaust pipe'} = \frac{1}{\text{always}} + \frac{0.5}{\text{sometimes}} + \frac{0}{\text{no}} . \qquad (7)$$

$$x_8 : \text{'Abnormal inlet pressure'} = \frac{1}{\text{below 0.1bar}} + \frac{0.5}{\text{0.1~0.3bar}} + \frac{0}{\text{0.3~1bar}} + \frac{0.5}{\text{above 1bar}} . \qquad (8)$$

$$x_9 : \text{'Abnormal throttle sensor signal'} = \frac{1}{1\% > \text{normal}} + \frac{0.5}{0~1\% > \text{normal}} + \frac{0}{\text{normal}} . \qquad (9)$$

$$x_{10} : \text{'Abnormal cooltant temperature'} = \frac{1}{>100°C \, or < 70°C} + \frac{0.5}{100-90°C} + \frac{0}{90~80°C} + \frac{0.5}{80~70°C} . \qquad (10)$$

$$x_{11} : \text{'Abnormal lambda signal'} = \frac{1}{1 \, or \, 0V} + \frac{0.5}{0.9~0.7V} + \frac{0}{0.7~0.3V} + \frac{0.5}{0.3~0.1V} . \qquad (11)$$

3   Fuzzy Relevance Vector Machine

Relevance vector machine (RVM) is a statistical learning method utilizing Bayesian learning framework and popular kernel methods. This approach is able to utilize more flexible candidate models, which are typically much sparser, offering probabilistic prediction and avoid the need to adjust additional hyperparameters. In fault diagnosis, RVM is desired to predict the posterior probability of each fault t_n for unseen symptoms $\mathbf{x}$, given a set of training data $(\mathbf{X}, \mathbf{t}) = \{\mathbf{x}_n, t_n\}$, $n = 1$ to N, $t_n \in \{0, 1\}$, N is the number of training data. It follows the statistical convention and generalizes the linear model by applying the logistic sigmoid function $\sigma(y) = 1/(1+e^{-l})$ to the predicted decision $y(\mathbf{x})$ and adopting the Bernoulli distribution for $P(\mathbf{t} |\mathbf{X})$, the likelihood of the data is written as [4]:

$$P(\mathbf{t}|\mathbf{X}, \mathbf{w}) = \prod_{n=1}^{N}\sigma\{y(\mathbf{x}_n;\mathbf{w})^{t_n}\}[1-\sigma\{y(\mathbf{x}_n;\mathbf{w})\}]^{1-t_n}$$

$$\text{where } y(\mathbf{x};\mathbf{w}) = \sum_{i=1}^{N}w_i K(\mathbf{x},\mathbf{x}_i) + w_0 \tag{12}$$

and $\mathbf{w} = (w_0, w_2, \ldots, w_N)^{\mathrm{T}}$ are the adjustable parameters, K is a radial basis function (RBF) since RBF kernel is usually adopted for classification problems. When introducing the fuzzy membership vector $\mathbf{s}=[s_1,s_2,\ldots,s_{11}]$ of the corresponding symptom vector $\mathbf{x}=[x_1 x_2,\ldots,x_{11}]$, the $\mathbf{X}$ in (12) can be transferred into $\mathbf{S}$ as below.

$$P(\mathbf{t}|\mathbf{S}, \mathbf{w}) = \prod_{n=1}^{N}\sigma\{y(\mathbf{s}_n;\mathbf{w})^{t_n}\}[1-\sigma\{y(\mathbf{s}_n;\mathbf{w})\}]^{1-t_n}$$

$$\text{where } y(\mathbf{s};\mathbf{w}) = \sum_{i=1}^{N}w_i K(\mathbf{s},\mathbf{s}_i) + w_0 \tag{13}$$

Now we want to find out the optimal weight vector $\mathbf{w}$ for the given dataset. It is equivalent to find $\mathbf{w}$ so as to maximize the probability $P(\mathbf{w}|\mathbf{t}, \mathbf{S}, \boldsymbol{\alpha}) \propto P(\mathbf{t}|\mathbf{S}, \mathbf{w}) P(\mathbf{w}|\boldsymbol{\alpha})$, with $\boldsymbol{\alpha} = [\alpha_0, \alpha_1, \ldots, \alpha_N]$ a vector of $N+1$ hyperparameters. However, we cannot determine the weights analytically, and so are denied closed-form expressions for either the marginal likelihood $P(\mathbf{w}|\boldsymbol{\alpha})$, or equivalently the weight posterior $P(\mathbf{w}|\mathbf{t}, \mathbf{S}, \boldsymbol{\alpha})$. We thus choose to utilize the following approximation procedure as used by MacKay [8], which is based on Laplace's method:

a)   For the current fixed values of $\boldsymbol{\alpha}$, the most probable weights $\mathbf{w}_{\mathrm{MP}}$ are found, which is the location of the posterior mode. Since $P(\mathbf{w}|\mathbf{t}, \mathbf{S}, \boldsymbol{\alpha}) \propto P(\mathbf{t}|\mathbf{S}, \mathbf{w}) P(\mathbf{w}|\boldsymbol{\alpha})$, this step is equivalent to the following maximization:

$$\mathbf{w}_{MP} = \arg\max_{\mathbf{w}} \log P(\mathbf{w}|\mathbf{t}\, \mathbf{S}, \boldsymbol{\alpha})$$

$$= \arg\max_{\mathbf{w}} \log\{P(\mathbf{t}|\mathbf{S}, \mathbf{w})\, P(\mathbf{w}|\boldsymbol{\alpha})\}$$

$$= \arg\max_{\mathbf{w}} \left\{\sum_{n=1}^{N}[t_n \log d_n + (1-t_n)(1-\log d_n)] - \frac{1}{2}\mathbf{w}^T \mathbf{A}\mathbf{w}\right\} \tag{14}$$

with $d_n = \sigma\{y(\mathbf{s}_n;\mathbf{w})\}$, $\mathbf{A} = diag(\alpha_0, \alpha_1, \ldots, \alpha_N)$

b)   Laplace's method is simply a Gaussian approximation to the log-posterior around the mode of the weights $\mathbf{w}_{\mathrm{MP}}$. (14) is differentiated twice to give:

$$\nabla_{\mathbf{w}}\nabla_{\mathbf{w}} \log P(\mathbf{w}\,|\,\mathbf{t},\mathbf{S},\boldsymbol{\alpha})|_{\mathbf{w}_{MP}} = -(\mathbf{\Phi}^T \mathbf{B}\mathbf{\Phi} + \mathbf{A}) \quad . \tag{15}$$

where $\mathbf{B}$ = diag $(\beta_1,..., \beta_N)$ is a diagonal matrix with $\beta_n = \sigma\{y(\mathbf{s}_n;\mathbf{w})\}[1 - \sigma\{y(\mathbf{s}_n;\mathbf{w})\}]$, and $\mathbf{\Phi}$ is a $N \times (N + 1)$ design matrix with $\mathbf{\Phi}_{nm} = K(\mathbf{s}_n, \mathbf{s}_{m-1})$ and $\mathbf{\Phi}_{n0} = 1$, $n = 1$ to N, and $m = 1$ to $N + 1$. By negating and inverting (15), the covariance matrix $\mathbf{\Sigma} = (\mathbf{\Phi}^T\mathbf{B}\mathbf{\Phi} + \mathbf{A})^{-1}$ can be obtained.

c)   The hyperparameters $\boldsymbol{\alpha}$ is updated using an iterative re-estimation equation. Firstly, randomly guess α_i and calculate $\gamma_i = 1 - \alpha_i\Sigma_{ii}$, where Σ_{ii} is the ith diagonal element of the covariance matrix $\mathbf{\Sigma}$. Then re-estimate α_i as follows:

$$\alpha_i^{new} = \frac{\gamma_i}{u_i^2} \ . \tag{16}$$

where $\boldsymbol{u} = \mathbf{w}_{MP} = \mathbf{\Sigma}\mathbf{\Phi}^T\mathbf{B}\mathbf{t}$. Set $\alpha_i \leftarrow \alpha_i^{new}$ and re-estimate γ_i and α_i^{new} again until convergence.

4   Experiments

4.1   Design of Experiments

The FRVM was implemented by MatLab. As the output of each FRVM classifier is a probability vector. Some well-known probabilistic diagnostic methods, such as fuzzy probabilistic neural network (FPNN) [9] and fuzzy probabilistic support vector machine (FPSVM) were also implemented with MatLab in order to compare their performances with FRVM fairly. For the structure of the FPSVM, the kernel was RBF. In terms of the hyperparameters in FPSVM, C and σ were all set to be 1 according to usual practice. Regarding the network architecture of the FPNN, there are 11 input neurons, 15 neurons with Gaussian basis function in the hidden layer and 11 output neurons with sigmoid activation function in the output layer.

In total, 308 symptom vectors were prepared by collecting the knowledge from ten experienced mechanics. The whole data was then divided into 2 groups: 77 as test dataset and 231 as training dataset. All engine symptoms were fuzzified using the fuzzy memberships of (1) to (11) and produced the fuzzified training dataset *TRAIN* and the fuzzified test dataset *TEST*. For training FRVM and FPSVM, each algorithm constructed 11 fuzzy classifiers f_i, $i \in \{1,2,..,11\}$, based on *TRAIN*. The training procedures of FRVM and FPSVM are shown in Fig. 1, whereas the procedure for FPNN is not presented in Fig. 1, because it is a network structure instead of individual classifier.
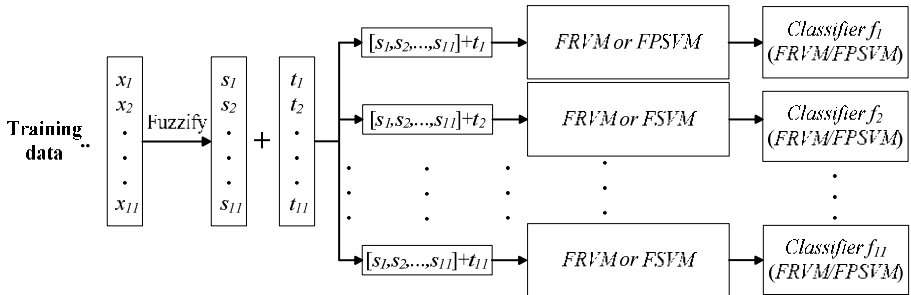

Fig. 1. Workflow of training of FRVM and FPSVM

4.2   Simultaneous Fault Identification

The outputs of FPNN, FPSVM and FRVM are probabilities, so a simple threshold probability can be adopted to distinguish the existence of simultaneously faults. According to reference [9], the threshold probability was set to be 0.8. The whole fault identification procedure is shown below.

1)   Input $\mathbf{x}= [x_1, x_2,..., x_{11}]$ into every classifier f_i and FPNN, and each f_i and the output neurons of FPNN could return a probability vector $\boldsymbol{\rho} = [\rho_1, \rho_2, ..., \rho_{11}]$. ρ_i is the probability of the ith fault label.   Where $\mathbf{x}$ is a test instance and $\boldsymbol{\rho}$ is the predicted vector of engine faults.

2)   The final classification vector $\mathbf{y} = [y_1, y_2,..., y_{11}]$ is obtained based on (17).

$$y_i = \begin{cases} 1 \text{ if } \rho_i \geq 0.8 \\ 0 \text{ otherwise} \end{cases}, \text{ for } i = 1 \text{ to } 11. \quad . \tag{17}$$

The entire fault diagnostic procedures of FRVM and FPSVM are depicted in Fig. 2 whereas the procedure of FPNN is not shown in Fig. 2, because it uses an entire network to predict the outputs, but the fault identification is the same.
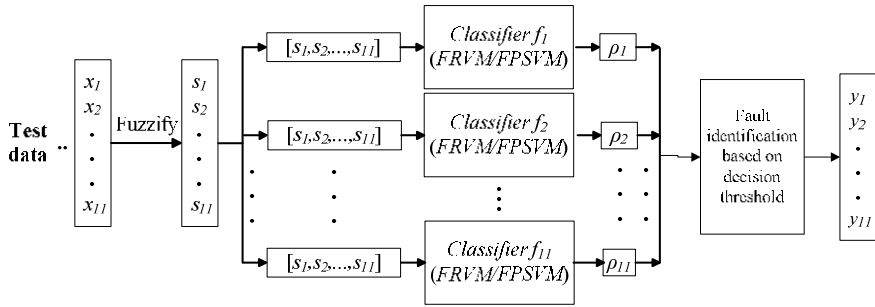
Fig. 2. Workflow of fault diagnosis based on FRVM and FPSVM

4.3   Evaluation

F-measure is mostly used as performance evaluation for simultaneous faults as it considers partial match. In this experiment, totally 77 instances were tested and each instance included 11 fault labels, so the F-measure equation is given in (18). The larger the F-measure value, the higher the diagnosis accuracy.

$$F = \frac{\sum_{j=1}^{11} \sum_{i=1}^{77} y_i^j t_i^j}{\sum_{j=1}^{11} \sum_{i=1}^{77} y_i^j + \sum_{j=1}^{11} \sum_{i=1}^{77} t_i^j} \in [0, 1] \quad . \tag{18}$$

The average F-measure of predicted faults over *TEST* is shown in Table 4, in which the average accuracy of FRVM is higher than that of FPNN and FPSVM. The reason of why FPNN gives poor accuracy is that the training data in this research is not large enough (231 only). The relatively low F-measure of FPSVM is due to the necessity to estimate its parameters (σ, c) manually while FRVM does not need.

Although Table 4 shows that FPSVM runs much faster than FPNN and FRVM under the same *TRAIN* and *TEST,* the diagnostic accuracy is always more important than the running time in terms of fault diagnosis problems. So FRVM is still a very good approach for this application.

Table 4. Overall F-measure and computational time comparison for the three classifiers

	FPNN	FPSVM	FRVM
Training time (over TRAIN)	271.4 ms	61.6 ms	381.6 ms
Diagnostic time (over TEST)	298.5 ms	57.1 ms	298.1 ms
Average F-measure of 11 faults	0.7691	0.8728	0.9495

5   Conclusions

In this paper, FRVM has been successfully applied to automotive engine simultaneous fault diagnosis. Moreover, FPNN, FPSVM and FRVM have been compared based on various combinations and degrees of symptoms. This research is the first attempt at applying FRVM for engine simultaneous fault diagnosis and comparing the diagnosis performance of several fuzzy classifiers. Experimental results show that FRVM outperforms FPSVM and FPNN in terms of accuracy even though its running time is not the best. However, it can still be concluded that FRVM is a very good approach for engine simultaneous fault diagnosis.

References

1. Li, H.K., Ma, X.J., He, Y.: Diesel Fault Diagnosis Technology based on the Theory of Fuzzy Neural Network Information Fusion. In: Proceedings of the Sixth International Conference of Information Fusion, pp. 1394–1410 (2003)
2. Vong, C.M., Wong, P.K., Ip, W.F.: Support Vector Classification using Domain Knowledge and Extracted Pattern Features for Diagnosis of Engine Ignition Systems. Journal of the Chinese Society of Mechanical Engineers 31, 363–373 (2010)
3. Vong, C.M., Wong, P.K.: Engine Ignition Signal Diagnosis with Wavelet Packet Transform and Multi-class Least Squares Support Vector Machines. Expert Systems with Applications (2011), doi:10.1016/j.eswa.2011.01.058
4. Tipping, M.E.: Sparse Bayesian Learning and the Relevance Vector Machine. Journal of Machine Learning Research 1, 211–244 (2001)
5. Majumder, S.K., Ghosh, N., Gupta, P.K.: Relevance Vector Machine for Optical Diagnosis of Cancer. Lasers in Surgery and Medicine 36, 323–333 (2005)
6. Li, D.F., Hu, W.C., Xiong, W., Yang, J.B.: Fuzzy Relevance Vector Machine for Learning from Unbalanced Data and Noise. Pattern Recognition Letters 29, 117–118 (2008)
7. Liu, X.M., Zhang, X.H., Yuan, J.: Relevance Vector Machine and Fuzzy System based Multi-objective Dynamic Design Optimization: A Case Study. Expert Systems with Applications 37, 3598–3604 (2010)
8. MacKay, D.J.C.: The Evidence Framework Applied to Classification Networks. Neural Computation 4, 720–736 (1992)
9. Li, G.Y.: Applications of Intelligence Control in Electronic Control Engine. Publishing House of Electronics Industry, Peking (2007) (in Chinese)

Stability and Oscillation Analysis in a System of Three Coupled Oscillators with Delays

Yuanhua Lin[1] and Chunhua Feng[2]

[1] Department of Mathematics, Hechi College, Yizhou, Guangxi, China 546300
[2] College of Mathematical Science, Guangxi Normal University,
Guilin, Guangxi, China 541004
lyh4773@163.com

Abstract. In this paper, a system of three coupled oscillators with delays is investigated. Some sufficient conditions to guarantee the existence of stability and oscillations for the model are obtained. Simulations are provided to demonstrate the proposed results.

Keywords: three coupled oscillators, delay, stability, oscillation.

1 Introduction

Recently, the two coupled van der Pol oscillators with time delay have been studied as a model of self-excited systems by many researchers [1-4]. For two dimensions of time delay age-structured model of a single species living in two identical patches, Yu et al. [5] have considered the stability of the equilibrium and Hopf bifurcation of the model by analyzing the distribution of the roots of associated characteristic equation. For two-dimensional SIS model with vaccination, Li et al. [6] have studied the stability and bifurcation of an SIVS epidemic model with treatment and age of vaccination. Based on the presence of circadian rhythms in the chemistry of the eyes, Rompala et al. [7] have studied the following no delay three coupled van der Pol oscillators model:

$$
\begin{aligned}
&x''(t)-\varepsilon\,(1-x^2(t))x'(t)+x(t)= \varepsilon\mu\,[w(t)-x(t)],\\
&y''(t)-\varepsilon\,(1-y^2(t))y'(t)+y(t)= \varepsilon\mu\,[w(t)-y(t)],\\
&w''(t)-\varepsilon(1-w^2(t))w'(t)+p^2w(t)=\varepsilon\mu\,[x(t)-w(t)]+ \varepsilon\mu\,[y(t)-w(t)].
\end{aligned}
\tag{1}
$$

Since the x and y oscillators are identical, and are not directly coupled to each other, only are coupled via the w oscillator, then in-phase the authors mode $x = y$ and dealt with the two coupled van der Pol oscillators. By means of computational tools, the authors successfully computed numerically and analytically the bifurcation curves. The qualitative behavior was determined for each distinct region in the parameter plane. For no delay three-variable circadian rhythm model, Nagy [8] investigated the possible phase portraits and local bifurcations in detail. The saddle-node and Hopf-bifurcation curves are determined in the plane of two parameters by using the parametric representation method. In this paper, we discuss a general model more

---

than (1) which is in one delay and each oscillator are directly coupled to each other, namely, the following model:

$$x''(t)-\varepsilon \ (1-x^2(t))x'(t)+ax(t)= \varepsilon\mu \ [y(t-\tau)-x(t)],$$
$$y''(t)-\varepsilon \ (1-y^2(t))y'(t)+by(t)= \varepsilon\mu \ [w(t-\tau)-y(t)], \tag{2}$$
$$w''(t)-\varepsilon(1-w^2(t))w'(t)+p^2w(t)=\varepsilon\mu \ [x(t-\tau)-w(t)]+ \varepsilon\mu \ [y(t-\tau)-w(t)].$$

where $p, \varepsilon, \mu, a, b$ are nonzero constants and $\tau >0$ is a time delay constant. Under very simple assumptions, we discuss the stability and oscillatory behavior of the trivial solution for system (2) by the approach of simplified analysis.

It is worth emphasizing that by using computational tools to determine the bifurcation curves of system (2) including time delay is difficult. Because the approach of bifurcation involves to deal with a high order algebraic equation.

2   Preliminaries

It is convenient to write (2) as an equivalent six dimensional first-order system

$$u'_1(t)=u_2(t),$$
$$u'_2(t)=-(a+\varepsilon\mu)u_1(t) + \varepsilon \ u_2(t)- \varepsilon\mu \ u_3(t-\tau)-\varepsilon \ u_1^{\ 2}(t)u_2(t),$$
$$u'_3(t)=u_4(t),$$
$$u'_4(t)=-(b+\varepsilon\mu)u_3(t) + \varepsilon \ u_4(t) - \varepsilon\mu \ u_5(t-\tau)-\varepsilon \ u_3^{\ 2}(t)u_4(t), \tag{3}$$
$$u'_5(t)=u_6(t),$$
$$u'_6(t)=-(p^2+2\varepsilon\mu)u_5(t))+ \varepsilon \ u_6(t)-\varepsilon\mu \ u_1(t-\tau)- \varepsilon\mu \ u_3(t-\tau)-\varepsilon \ u_5^{\ 2}(t)u_6(t).$$

System (3) can be expressed in the following matrix form:

$$U'(t)=AU(t)+BU(t-\tau)+P(U(t)). \tag{4}$$

where $U(t)=[u_1(t), u_2(t), u_3(t), u_4(t), u_5(t), u_6(t)]^T$, $U(t-\tau)=[u_1(t-\tau), u_2(t-\tau), u_3(t-\tau), u_4(t-\tau), u_5(t-\tau), u_6(t-\tau)]^T$, both A and B are six by six matrices, and vector $P(U(t))=[0 \ -\varepsilon \ u_1^{\ 2}(t)u_2(t) \ 0 \ -\varepsilon \ u_3^{\ 2}(t)u_4(t) \ 0 \ -\varepsilon \ u_5^{\ 2}(t)u_6(t)]^T$. The linearization of system (3) at origin is the following:

$$u'_1(t)=u_2(t),$$
$$u'_2(t)=-(a+\varepsilon\mu)u_1(t) + \varepsilon \ u_2(t)- \varepsilon\mu \ u_3(t-\tau),$$
$$u'_3(t)=u_4(t),$$
$$u'_4(t)=-(b+\varepsilon\mu)u_3(t) + \varepsilon \ u_4(t) - \varepsilon\mu \ u_5(t-\tau), \tag{5}$$
$$u'_5(t)=u_6(t),$$
$$u'_6(t)=-(p^2+2\varepsilon\mu)u_5(t) + \varepsilon \ u_6(t)-\varepsilon\mu \ u_1(t-\tau)- \varepsilon\mu \ u_3(t-\tau).$$

The matrix form of system (5) is the follows:

$$U'(t)=AU(t)+BU(t-\tau). \tag{6}$$

Definition 1. A solution of system (3) is called oscillatory if the solution is neither eventually positive nor eventually negative.

Lemma 1. If $p\neq0$, $\varepsilon\mu\neq0$, $a\neq0$, $b\neq0$ and $-(p^2+2\varepsilon\mu)(a+\varepsilon\mu)(\ b+\varepsilon\mu)+\varepsilon^2\mu^2(a+b+2\varepsilon\mu)\neq0$, then system (3) (or (4)) has a unique equilibrium point.

Proof. An equilibrium point $u^*=(u_1^*, u_2^*, u_3^*, u_4^*, u_5^*, u_6^*)^T$ is a constant solution of the following algebraic equation

$$u_2^*=0,$$
$$-(a+\varepsilon\mu)\, u_1^*+ \varepsilon\, u_2^* -\varepsilon\mu\, u_3^* -\varepsilon\, (u_1^*)^2 u_2^* =0,$$
$$u_4^*=0,$$
$$-(b+\varepsilon\mu)\, u_3^*+\varepsilon\, u_4^* - \varepsilon\mu\, u_5^* -\varepsilon(\, u_3^*)^2 u_4^* =0, \qquad (7)$$
$$u_6^*=0,$$
$$-(p^2+2\varepsilon\mu)u_5^* +\varepsilon\, u_6^*-\varepsilon\mu\, u_1^*- \varepsilon\mu\, u_3^*-\varepsilon\, (u_5^*)^2 u_6^* =0.$$

Since $u_2^*=0$, $u_4^*=0$, $u_6^*=0$, from (7) we have

$$-(a+\varepsilon\mu)\, u_1 ^* -\varepsilon\mu\, u_3^* =0,$$
$$-(b+\varepsilon\mu)\, u_3^*- \varepsilon\mu\, u_5^* =0, \qquad (8)$$
$$-(p^2+2\varepsilon\mu)u_5^* -\varepsilon\mu\, u_1^*- \varepsilon\mu\, u_3^* =0.$$

From the assumptions, the determinant of the coefficient matrix of system (8) does not equal to zero, implying that $u_1^*=0$, $u_3^*=0$, $u_5^*=0$. Therefore, system (3) has a unique equilibrium point $(0,0,0,0,0,0)^T$.

3   Main Results

Theorem 1. If $p\neq0$, $\varepsilon\mu\neq0$, $a\neq0$, $b\neq0$ and $-(p^2+2\varepsilon\mu)(a+\varepsilon\mu)(b+\varepsilon\mu)+\varepsilon^2\mu^2(a+b+2\varepsilon\mu)\neq0$, let $\|B\| =2|\varepsilon\mu|$, and $\theta=\max\{1, |a+\varepsilon\mu|+|\varepsilon|, |b+ \varepsilon\mu|+|\varepsilon|, | p^2+2\varepsilon\mu |\}$. Suppose that

$$(\|B\|\tau\, e)\mathrm{e}^{-\tau\theta} >1. \qquad (9)$$

then the unique equilibrium point $(0,0,0,0,0,0)^T$ is unstable. In other words, the trivial solution of system (3) is oscillatory.

Proof. Under the assumptions, system (3) has a unique equilibrium point $(0,0,0,0,0,0)^T$. Obviously, linearized system (5) with system (3) have the same equilibrium point $(0,0,0,0,0,0)^T$. If the equilibrium point $(0,0,0,0,0,0)^T$ in system (5) is unstable, implying that this equilibrium point in system (3) is still unstable. Therefore, we only need to prove that the equilibrium point $(0,0,0,0,0,0)^T$ is unstable in linearized system (5), thus   system (5) does not have eventually positive solution or eventually negative solution. In other words, the trivial solution of system (5) is oscillatory. Namely, system (3) generates an oscillatory solution. Suppose that the trivial solution of system (5) is stable, then there exists a $t^*>0$ such that the trivial solution is convergent for $t>t^*+\tau$ and as a consequence we will have for $t>t^*+ \tau$:

$$z'(t)\leq\theta\, z(t) +\|B\|\, z(t-\tau). \qquad (10)$$

where $z(t)=\sum_{i=1}^{6} |u_i(t)|$. Consider the scalar delay differential equation:

$$v'(t)=\theta\, v(t) +\|B\|\, v(t-\tau). \qquad (11)$$

with $v(s)=z(s)$, $s\in[t^*, t^*+\tau]$. From the comparison theorem of differential equation, we have $z(t)\leq v(t)$ for $t>t^*+2\tau$. We claim that the trivial solution of (11) is unstable. Suppose that this is not the case, then the characteristic equation associated with (11) given by

$$\lambda=\theta +\|B\|\, \mathrm{e}^{-\lambda\tau} \qquad (12)$$

will have a real non-positive root, say $\lambda^* <0$, and $|\lambda^*| \geq \|B\|\, e^{|\lambda^*|\tau}-\theta$. Noting that $e^{|\lambda^*|\tau} \geq e|\lambda^*|\tau$.   From (12) we get

$$1 \geq \|B\|\, e^{|\lambda^*|\tau}/(|\lambda^*|+\theta)= \|B\|\tau\, e^{-\theta\tau} \cdot e^{(|\lambda^*|+\theta)\tau}/(|\lambda^*|+\theta)\tau$$
$$\geq \|B\|\,\tau\, e\cdot(|\lambda^*|+\theta)\tau\cdot e^{-\theta\tau}/(\,|\lambda^*|+\theta)\tau=(\|B\|\tau\, e)e^{-\theta\tau} \qquad (13)$$

The last inequality contradicts (9). Hence, our claim regarding the instability of the trivial solution of (11) is valid. It follows that the trivial solution of (10) is also unstable, which means that the equilibrium point $(0,0,0,0,0,0)^{\mathrm{T}}$ of (5) is unstable, implying that system (3) generates an oscillation.

Noting that in Theorem 1, $e^{-\tau\theta}$ will tend to zero as τ tend to infinity. This means that Theorem 1 holds only for some $\tau^*>0$, $\tau \in [0,\ \tau^*]$. In the following we propose a criterion to guarantee the oscillation of the equilibrium point for any $\tau>0$.

Theorem 2. If system (3) has a unique equilibrium point. Let $\alpha_1,\ \alpha_2,\cdots,\ \alpha_6$ denote the characteristic values of matrix A. Suppose that there is at least one characteristic value of A has positive real part for given values of $p,\ a,\ b,\ \varepsilon$ and $\mu,$ then the unique equilibrium point $(0,0,0,0,0,0)^{\mathrm{T}}$ is unstable, and system (3) generates an oscillation.

Proof. Since system (3) has a unique equilibrium point $(0,0,0,0,0,0)^{\mathrm{T}}$. Similar to Theorem 1, we only need to prove that the equilibrium point $(0,0,0,0,0,0)^{\mathrm{T}}$ of linearized system (5) is unstable, implying that the equilibrium point in system (3) is still unstable. Considering the matrix form (6) of system (5), the characteristic equation of (6) is

$$\det(\lambda \mathrm{I}_6 - A + Be^{-\lambda\tau})=0. \qquad (14)$$

Noting that the characteristic equation (14) is a transcendental equation which may have complex characteristic values. However, we show that the equation (14) will have a positive real part under our assumptions. Indeed, from (14) we have immediately that

$$\prod\nolimits^6_{j=1} (\lambda-\alpha_j - \beta_j\, e^{-\lambda})=0. \qquad (15)$$

where β_j (j=1,2, $\cdots$,6) are characteristic values of B. Noting that each β_j is zero, then equation (15) reduced to

$$\prod\nolimits^6_{j=1}(\lambda-\alpha_j)=0. \qquad (16)$$

Under our assumptions, there is at least one characteristic value α_j, j∈{1,2,$\cdots$,6} has positive real part, this means that characteristic value λ_j of (15) has positive real part, implying that the unique equilibrium point $(0,0,0,0,0,0)^{\mathrm{T}}$ is unstable, and system (3) generates an oscillation.

Noting that $P(0)=0$ and $u_1^2,\ u_3^2,\ u_5^2$ are higher infinitesimal quantity as $u_1,\ u_3,\ u_5$ tend to zeros respectively. So we have immediately that

Theorem 3. If system (3) has a unique equilibrium point. Let $\alpha_1,\ \alpha_2,\cdots,\ \alpha_6$ denote the characteristic values of matrix A. Suppose that each characteristic value of A has negative real part for given values of $p,\ a,\ b,\ \varepsilon$ and $\mu,$ then the unique equilibrium point $(0,0,0,0,0,0)^{\mathrm{T}}$ is stable.

4   Simulation Result

In Fig. 1A we select the values: $\varepsilon=1.5$, $\mu=0.5$, $p^2=0.49$, $a=1$, $b=1.5$, time delay is 0.8. The characteristic values of the matrix A are 0.7500+1.0897i, 0.7500-1.0897i,

0.7500+1.1779i, 0.7500-1.1779i, 0.7500+1.7110i, 0.7500-1.7110i. In Fig. 1B, we select the values: ε=0.5, μ= -0.5, p^2=0.49, a=1, b=1.5, time delay is 1.2. The characteristic values of the matrix A are 0.2500+0.8292i, 0.2500-0.8292i, -0.8956, 1.3956, -0.0193 and 0.5193. It is easy to see that the conditions of Theorem 2 are satisfied. Permanent oscillations are appeared. In Fig. 2A and Fig. 2B, we select the same values: ε= - 0.15, μ=- 0.4, p^2=0.49, a=b=1, but the time delays are 1 and 20 respectively. For given parameter values, the characteristic values of the matrix A are -0.0750+1.0268i, -0.0750+1.0268i, -0.0750+1.0268i, -0.0750-1.0268i, -0.0750 +0.7774i, -0.0750-0.7774i. Thus the conditions of Theorem 3 are satisfied. The unique equilibrium point of system (3) is stable.

Fig.1A Oscillation of the equilibrium point, dotted line: x(t), solid line: y(t), dashed line:w(t), delay=0.8(0.8*10=10ms)

Fig.1B Oscillation of the equilibrium point, dotted line:x(t), solid line: y(t), dashed line: w(t), delay=1.2(1.2*10=12ms)
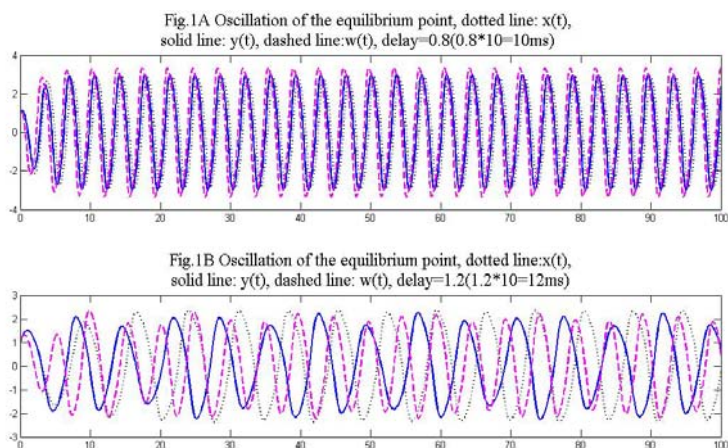
Fig. 1. In Fig.1A, ε=1.5, μ=0.5, p^2=0.49, a=1, b=1.5, τ =0.8, and in Fig.1B, ε=0.5, μ=-0.4, p^2=0.49, a=1, b=1.5, τ =1.2. Oscillations appear both in the two cases of parameter values.

Fig.2A Stability of the equilibrium point, dotted line: x(t), solid line: y(t), dashed line: w(t), delay = 1.2(1.2*10=12 ms)

Fig.2B Stability of the equilibrium point, dotted line: x(t), solid line: y(t), dashed line: w(t), delay = 12(12*10=120 ms)

Fig. 2. Both in Fig.2A and Fig.2B, the parameter values are ε=-0.15, μ=-0.4, p^2=0.49, a=1, b=1.5, time delay τ =1.2 and 12 respectively. The equilibrium point is stable.

5   Conclusion

In this paper, we have discussed the effect of time delays in a mathematical model of three coupled oscillators. Some sufficient conditions to guarantee the existence of permanent oscillations of the equilibrium point for the model are obtained. Examples are provided to demonstrate the proposed results. Our simple criterion to guarantee the existence of permanent oscillations is easy to check, as compared with predicting the regions of bifurcation.

References

1. Wirkus, S., Rand, R.: The dynamics of two coupled van der Pol oscillators with delay coupling. Nonlinear Dynam. 30, 205–221 (2002)
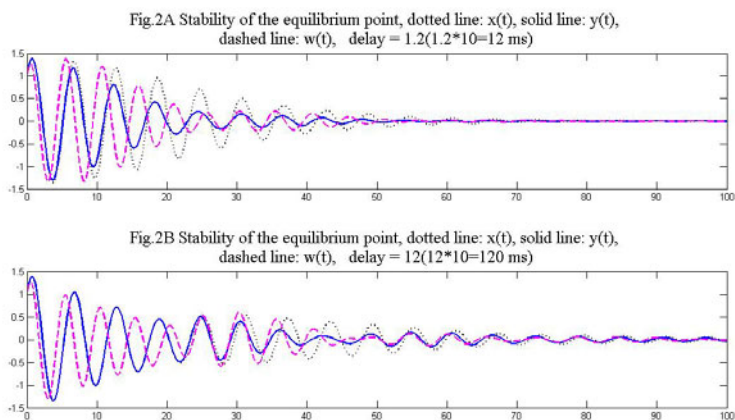2. Hirano, H., Rybicki, S.: Existence of limit cycles for coupled van der Pol equations. J. Differ. Equat. 195, 194–209 (2003)
3. Zhang, J.M., Gu, X.S.: Stability and bifurcation analysis in the delay-coupled van der Pol oscillators. Appl. Math. Model 34, 2291–2299 (2010)
4. Song, Y.L., Han, M.A., Peng, Y.H.: Stability and Hopf bifurcations in a competitive Lotka-Volterra system with two delays. Chaos Soliton Fract. 22, 1139–1148 (2004)
5. Yu, C.B., Wei, J.J., Zou, X.F.: Bifurcation analysis in an age-structured model of a single species living in two identical patches. Appl. Math. Model. 34, 1068–1077 (2010)
6. Li, X.Z., Wang, J., Ghosh, M.: Stability and bifurcation of an SIVS epidemic model with treatment and age of vaccination. Appl. Math. Model. 34, 437–450 (2010)
7. Rompala, K., Rand, R., Howland, H.: Dynamics of three coupled van der Pol oscillators with application to circadian rhythms. Commun. Nonlinear Sci. Numer. Simul. 12, 794–803 (2007)
8. Nagy, B.: Comparison of the bifurcation curves of a two-variable and a three-variable circadian rhythm model. Appl. Math. Model. 32, 1587–1598 (2008)

The Recursive Transformation Algorithms between Forest and Binary Tree

Min Wang

Computer Science Department, Weinan Teachers University, Weinan, Shanxi, China
wntcwm@126.com

Abstract. Analyzed in detail the storage structures of tree, forest and binary tree, introduced the design ideas of the recursive algorithms about transformation between the forests and the corresponding binary trees, gave the descriptions of the recursive algorithms in C, and then analyzed the algorithms and evaluated them from the two aspects of time complexity and space complexity.

Keywords: Tree; Forest; Binary tree; Recursive algorithm; Time complexity; Space complexity.

1   Introduction

Trees or Forests can take many forms of storage structures in a large number of applications, but many "Data Structure" materials introduced their storage structures mainly about the parents representation, the children representation and the child and brother representation. Binary tree is another tree structure, and its characteristic is that each node of it has at most two subtrees that are ordered [1]. Since binary tree is convenient for computer processing [2], the tree or forest can be converted at first into the corresponding binary tree, and then execute the relevant oprations. This paper will analyze and design the recursive algorithms of forest and binary tree transforming into each other, give the algorithm descriptions in C, and analyze and evaluate the algorithms from the two aspects of time complexity and space complexity, so as to play a guiding role in teaching the relevant chapters in "Data Structure" curriculum [3].

2   The Child and Brother Representation of Tree [3]

The child and brother representation of tree is also known as the binary tree representation or the binary linked list representation. That is the storage structure of the tree is the binary linked list. The two pointer fields, named *Firstchild* and *Nextsibling*, in each node of the linked list indicate respectively the first child and the next sibling of the node [1,3].

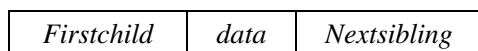The storage structure of the linked node is shown as Fig.1.

Firstchild	*data*	*Nextsibling*

Fig. 1. The node structure of the binary linked list of tree

The node type can be defined in C as follows:

```
typedef struct node{
  DataType data;
  struct node *Firstchild,*Nextsibling;
} CSNode, *CSTree; [1-3]
```

3   The Storage Structure of the Binary Tree [3]

For any binary tree, each node of it has only two children and one parent (root node without parent), and each node can be designed to include at least three fields: *data*, which is used to store the value of the node, *Lchild*, which points to the left child of the node, and *Rchild*, which points to the right child of the node. Its storage structure is shown as Fig.2.
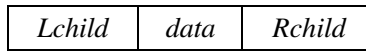
Lchild	*data*	*Rchild*

Fig. 2. The node structure of the binary linked list of the binary tree

The node type can be defined in C as follows:

```
typedef struct node{
  DataType data;
  struct node *Lchild,*Rchild;
} Node, *BTree; [2,3]
```

4   Transformations between Forest and Binary Tree

As the tree and the binary tree have the same binary linked storage structure, the binary linked list can be used as their relation medium. That is, given a tree, you can find one and only corresponding binary tree, and their storage structure are the same but only different in interpretation [1,3].

Forest is a collection of some trees. As the tree can correspond to a unique binary tree, the forest can also correspond to a unique binary tree [2,3].

4.1   Formalized Definition of Transformation from Forest to Binary Tree

Suppose that $F=\{T_1,T_2,\ldots,T_n\}$ is a forest, then the following rules will convert F into a binary tree $B=\{root,LB,RB\}$:

(A) If F is empty, that is $n=0$, B will be an empty tree;
(B) Otherwise, follow these steps to convert:

  (a)   The root of B (named *root*) is the root of the first tree of the forest ($ROOT(T_1)$);
  (b)   The left subtree of B (named *LB*) is a binary tree converted from $F_1=\{T_{11},T_{12},\ldots,T_{1m}\}$, which is the subtree forest of the root of T_1;
  (c)   The right subtree of B (named *RB*) is a binary tree converted from forest $F'=\{T_2,T_3,\ldots,T_n\}$ [1,3].

4.2   Algorithm Description about Transformation from Forest into Binary Tree

The binary tree *B* adopts the binary linked type *BTree* mention before, and the forest *F* adopts the aforementioned child and brother binary linked structure type *CSTree*. The description in C of the recursive transformation algorithm is as follows:

```
void TransForest(CSTree F, BTree *B)
{  if(!F)
       *B=NULL;
   else{
       (*B)->data=F->data;
       TransForest(F->Firstchild,&((*B)->Lchild));
       TransForest(F->Nextsibling,&((*B)->Rchild));
   }//End_if
}//End
```

4.3   Formalized Definition of Transformation from Binary Tree to Forest

Suppose that $B=\{root,LB,RB\}$ is a binary tree, then the following rules will convert B into forest $F=\{T_1,T_2,\ldots,T_n\}$:

(A) If *B* is empty, *F* will be an empty tree;
(B) Otherwise, follow these steps to convert:

(a)   The root of the first tree of the forest ($ROOT(T_1)$) is the root of *B* (named *root*);
(b)   The subtree forest (F_1) of the root of T_1 is converted from the left subtree of *B* (named *LB*);
(c)   The forest $F'=\{T_2,T_3,\ldots,T_n\}$ consists of the rest tree except T_1 is converted from the right subtree of *B* (named *RB*) [1].

4.4   Algorithm Description about Transformation from Binary Tree into Forest

The binary tree *B* and the forest *F* adopt the same structure type mentioned before, and the description in C of the recursive conversion algorithm is as follows:

```
void TransBinary(BTree B,CSTree *F)
{  if(!B)
       *F=NULL;
   else{
       (*F)->data=B->data;
       TransBinary(B->Lchild,&((*F)->Firstchild));
       TransBinary(B->Rchild,&((*F)->Nextsibling));
   }//End_if
}//End
```

4.5   Algorithm Analysis and Evaluation

The returned result of each recursive calling does not be saved, so it must be computed once more whenever needed, this leads to the time complexity of recursive functions actually depend on the times of recursive calling [3-5].

Function *TransForest()* transforms forest *F* into its corresponding binary tree *B*, and the function call starts from *F*. If *F* is not empty, the root of *B* will be the root of the first tree T_1 of *F*. The first recursive calling statement transforms the forest pointed by the field *Firstchild* of *F* into the left subtree of *B*, while the second one transforms the forest pointed by the field *Nextsibling* of *F* into the right subtree of *B*.

Function *TransBinary()* reverts binary tree *B* to its corresponding forest *F*, and the function call starts from *B*. If *B* is not empty, the root of *B* will be the root of the first tree T_1 of *F*. The first recursive calling statement converts the left subtree of *B* into the subtree forest of root node of T_1, while the second one converts the right subtree of *B* into the forest that consists of the rest tree except T_1.

Since there are two recursive calling statements in the function bodies of the two functions above, the times of recursive calling is actually the sum of the number of nodes in the forest and the number of null pointers. An *n* nodes binary linked list has $n+1$ null pointers, and then the total number of recursive calling is $2n+1$ times [3,5]. Regards the number (*n*) of nodes in the forest as the scale of the problem, and with the gradually increase of problem scale, the time complexity of the two algorithms are nearly *T(n)=O(2n+1)* [3].

In addition to the storage space used by the functions themselves, function *TransForest()* and *TransBinary()* introduced non assistant space, thus the algorithm space complexity of the two algorithms are constant order, that is *S(n)=O(1)*.

5   Conclusion

This paper analyzed in detail the procedure of transformation between the forests and the corresponding binary trees, introduced the recursive analyze ideas and the concrete design processes of the two algorithms, and thus played a guiding role in teaching the relevant chapters in "Data Structure" curriculum.

References

1. Yan, W., Wu, W.: Data Structures(C language edition). Tsinghua University Press, Beijing (2002)
2. Geng, G.: Data Structure—C Language description. Xi'an Electronic Science and Technology University Press, Xi'an (2005)
3. Wang, M.: The Recursive Algorithm of Converting the Forest into the Corresponding Binary Tree. In: 2011 International Conference on Computer Science and Information Engineering. Springer, Zheng Zhou (in press, 2011)
4. Wang, M., Li, J.: Analysis of Time Efficiency in Recursion Algorithm. J. Journal of Weinan Teachers University 18(5), 61–62 (2003)
5. Wang, M.: Non-Recursive Simulation of the Recursive Algorithm for Searching the Longest Path in Binary Tree. J. Science Technology and Engineering 10(6), 1535–1539 (2010)

Design of Software System of Mobile Robot with Mixed Programming Based on Eclipse + pydev

Yinbo Liu, Junwei Gao, and Dawei Liu

Automation Engineering College Qingdao University, Qingdao, China
`qdlyb_1987@163.com`

Abstract. To meet the needs of modular, cross-platform and portability of mobile robot software system, a software system was designed based on the eclipse + pydev environment, GUI of the mobile robot was developed by using pyqt. The software system was of cross-platform and portability by using mixed programming of C/C++ and Python and the efficiency of development was improved at the same time. The experiment of mobile robot shows that the system is stable, reliable and real-time, and is of scalability and cross-platform. It meets the needs of navigation for mobile robot in various environments.

Keywords: mobile robot, Python, mixed programming, SWIG.

1 Introduction

With the development of computer programming language, mixed language programming has become a popular approach to software development. Mixed-language programming refers to use two or more than two programming languages for application development, it is a popular approach to use scripting languages (such as Python, Tcl) mixed with compiled language (such as C/C++ or Fortran) [1] [2] [3]. The program developed by compiled language runs fast, but the development cycle is a little longer; while scripting language is convenient and flexible, the code is short, the efficiency of development can be improved, but it runs slowly. It is a good way to combine the advantages of the two languages properly and complement each other. It can build applications quickly and efficiently and also can maintain the same performance. Mobile robot software system developed using compiled languages can only running under the specific strategy in a specific environment. If the strategy needs to be modified after compiled, it has to modify the source code and then compile again, which is not good to meet the needs of the mobile robot running in various environments and is had to improve the control strategy. Python [4] is a scripting language of interpreted, object-oriented, dynamic semantics, beautiful syntax, and had provided a variety of open source extension modules. After 30-year development, it with Tcl, Perl together, has become the most widely used cross-platform scripting language. Python's syntax is simple. It only needs a small amount of code even to write a large-scale program and has a good integrated support. It is proper to be the code of the master control program. Using Python, C/C++ mixed

programming language, can improve the efficiency of robot software development and the cross-platform and portability of software systems [5] [6] [7] [8] [9]. Based on which the laser navigation mobile robot software system is designed in eclipse + pydev environment. GUI of the mobile robot is also developed by using pyqt. The efficiency of the development and cross-platform and portability were improved by using the mixed programming with C/C++ and Python.

2   Structure of Mobile Robot

The mobile robot with laser navigation is showed in Figure 1. The robot is of four-wheel, two-wheel drive with differential mode, two driving wheels arranged in the robot's front side both with rubber pneumatic tires, and of good adhesion and damping properties. Each of the driving wheels is driven by its own motor; engaged wheels are solid rubber casters, just as a support. With the laser range finder robot can acquire the perception of outside world with which the robot can complete its obstacle avoidance, navigation and so on. The laser range finder used is LMS200 which is produced by SICK. This laser range finder is a non-contact measurement system, and has advantages of high speed, high precision, wide measurement range, and so on. LMS200 laser range finder has a scanning range of 180°, adjustable scanning distance 0~80m, a resolution of 10mm, and its detection method is diffuse type. LMS200 has three adjustable scan interval models, 0.25°, 0.5° and 1°, and its response time is 53.33ms, 26.67ms and 13.33ms.
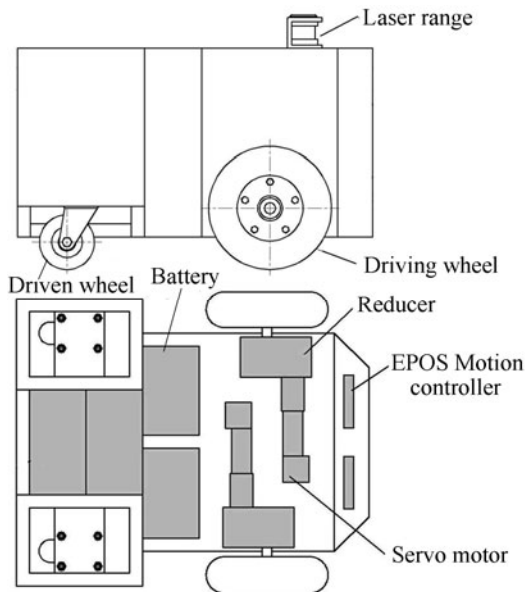

Fig. 1. Structure schematic diagram of the mobile robot

3 Mobile Robot Software System Design Based on Python + C/C++ Mixed Programming

3.1 Software Development Framework

The main point of mix programming of Python and C/C++ is to integrate. To import a module of C/C++ in Python, C/C++ code should be compiled by the GCC firstly, then by using SWIG or Boost, you can call it in Python interpreter.

Figure 2 shows the flowchart of mobile robot software system. In the design of software system multi-threading under PyDev for Eclipse is used. The entire system consists of a main process and two threading (environmental processing threading, motion control threading). The main process is responsible for the operation of the whole process, also responsible for obstacle avoidance sensor information access and GUI exchange working. To the two working threading, the environment processing threading is responsible for data processing and sending to the public information area, the date was read from the laser range finder; and according to environmental information from the public information area and obstacles information, the motion control threading control the mobile robot movement through movement controller of the system while the motion parameters were written in public information area by this threading.

To the whole software system Python and C/C++ mixed programming is used. To the modules of no special requirements on speed, such as GUI, serial communication, Python is used to be developing code; to the motion control module, since the motion controller EPOS only provided the interface under Windows, and the path planning process has a large amount of computing on the high speed requirements, C/C++ is used.

3.2 Software Interface Design

The main programming language is Python, while C/C++ is only a small part of the whole code, so we made C/C++ code an extended module and embedded it into Python. The interface can be designed in the following way.

Before programming with Python, C/C++, a development environment should be built. The program code we compiled is under GCC but it is developed under Windows which do not have it, we should install MinGW to give a GCC environment to Windows. MinGW provides a set of complete open source programming tool which is suitable for the development of native MS-Windows applications, and also MinGW includes a port of the GNU Compiler Collection(GCC), including C, C++, ADA and Fortran compilers, GNU Binutils for Windows(assembler, linker, archive manager) and make a good foundation for cross-hosted use. While in transforming DLL to Static Library pexport and dlltool should be downloaded. While integrating codes SWIG should be installed and C:\SWIG\bin should be added to your PATH environment.
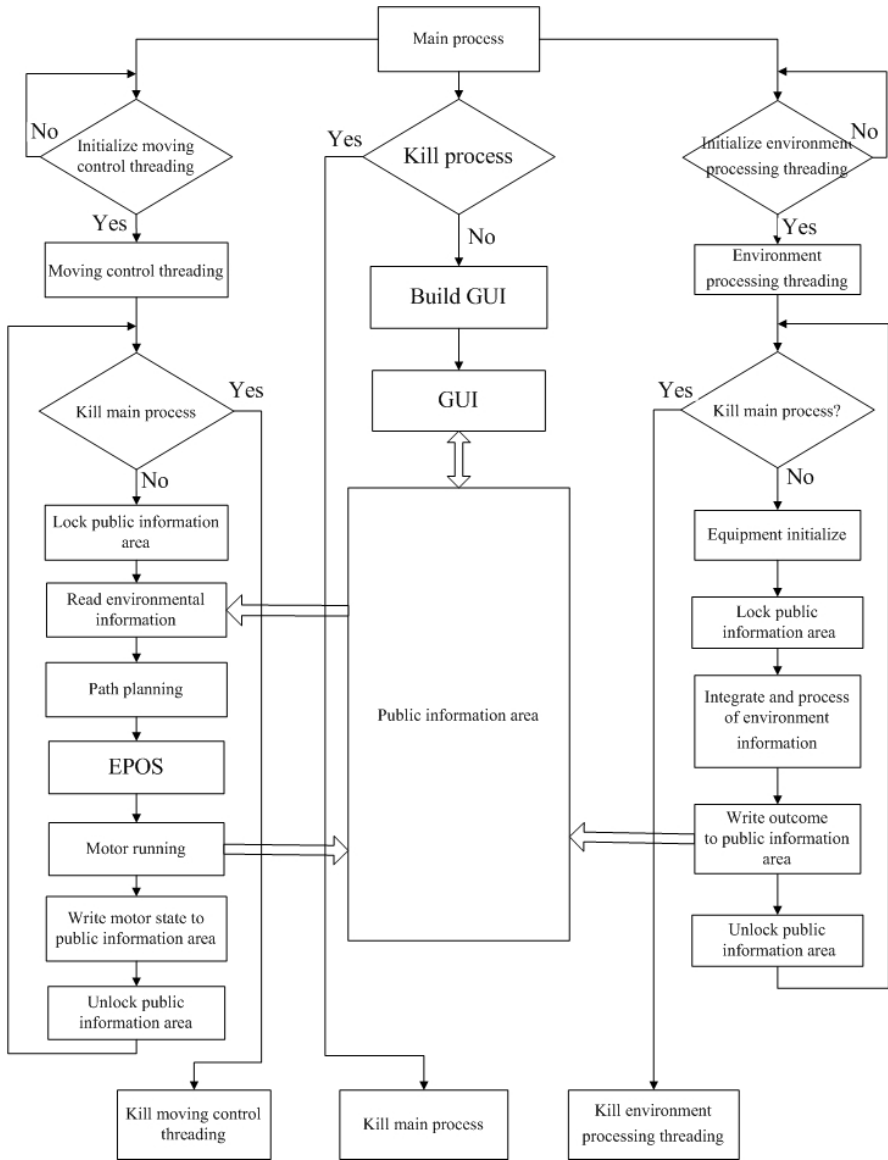
Fig. 2. The flowchart of mobile robot software system

By using C/C++ and Python mixed programming in Windows, SWIG was used to create C/C++ extensions in Python, to improve the cross-platform features. GCC compiler was used to compile C/C++ code, show as follows:

(1) To establish libpython26.a static library

In order to create Python extensions, a Python library is needed, but Python only gives a DLL which is available for Microsoft Visual C++ development, GCC

compiler requires a static library files, so python26.lib should be transformed into libpython26.a by using pexport, dlltool showed as follows:

```
pexports python26.dll > python26.def
dlltool -dllname python26.dll -def python26.def -
output-lib libpython26.a
```

Then copy the generated libpython26.a to the same directory with the python26.lib.

(2)To establish libEposCmd.a static library

Since the robot motion controller is using the EPOS, and EPOS does not provide Python API, in the development processing Python API can be made by using other language's API. In this paper C/C++ API was used to be transformed. The way is shown as follows:

```
pexports EposCmd.dll > EposCmd.def
dlltool -U -d EposCmd.def -l libEposCmd.a
```

Then copy the generated libEposCmd.a to the directory of mingw's lib.

(3) To build a scripting language interface motion.i

motion.i document is written according to C/C++. The program's motion.i document is shown as follows:

```
%module mymodule
%{
#include "motion.h"
%}
class Motion
{
        public:
                Motion();
                ~Motion();
                int init();
            int stop();
            int go_forward(int dis);
            int go_back(int dis);
            int set_speed(int v);
            int set_acceleration(int a);
            int set_deceleration(int a);
            int turn_right(double angle);
            int turn_left(double angle);
    };
```

3.3 Compile the Running Module

Since C/C++ extensions should be compiled as a DLL for Python before integrating to Python code, the commands are much more and complex. To create a scripting language module from C/C++ code a batch file is used which can make a remarkable improvement of the efficiency. The compiled document is shown as follows:

```
swig -python -c++ motion.i
g++ -c motion.c++
```

```
g++ -c motion_wrap.cxx -Ic:\python26\include
g++ -shared motion_wrap.o -o _motion.pyd -
Lc:\python26\libs -lpython26 -lEposCmd
pause
```

motion.py and _mymodule.pyd can be generated after running motion.bat. Then the programming work is finished. If there is not error, it can be introduced and run in Python interpreter.

```
> Import mymodule
> R = mymodule.Motion ()
> R.init ()
> R.go_forward ()
```

4   GUI Design

There are many GUI toolkits for Python, some common GUI toolkits including: tcl/tk, wxPython, PyGtk, PyQt, etc. by which GUI programming can be realized conveniently. To develop the GUI for the laser navigation of mobile robot PyQt is used.

PyQt is Python bindings for Qt cross-platform GUI/XML/SQL C++ framework. Qt is a cross-platform application and UI framework. It includes a cross-platform class library, integrated development tools and a cross-platform IDE. It also provides a rich set of widgets, with the property of object-oriented, easy to be expand, blocks programming and so on. Qt supports the full range of Windows, UNIX/X11-Linux, Sun Solaris, HP-UX, Digital Unix, IBM AIX, SGI IRIX.

As a module of Python, PyQt contains over 600 classes and nearly 6,000 functions and methods. It is a cross-platform toolkit can be running on all major operating systems including UNIX, Windows and Mac. PyQt is very fast, and is fully object oriented. In particular, it inherited Qt Designer in Qt. Qt Designer is a GUI-aided design tools which is provided by Qt. It largely reduce the workload of the user interface designed. Make developer of Qt develop GUI like Visual Basic programmers, which only needs a small amount of dragging and code to complete most of the working.

While developing GUI, the prototype of GUI can be designed in the Qt Designer, and then generate a file with .ui for extension, next execute pyuic4 test.ui> test_ui.py under the command line, using pyuic4 conversion tool in PyQt, a Python code can be generated from the .ui file. GUI can be established by running the file. Efficiency of GUI development can be greatly improved by directly writing the file while deep development.

According to the needs of Mobile robot control system, GUI consists of manual control and automatic control. Manual control adjust the start position and posture, including linear movement, steering, speed, acceleration of the robot; automatic control is used to accomplish obstacle avoidance and navigation walk relying on the internal program of the robot. Designed under the Qt Designer, the final generation of the GUI was shown in Figure 3.
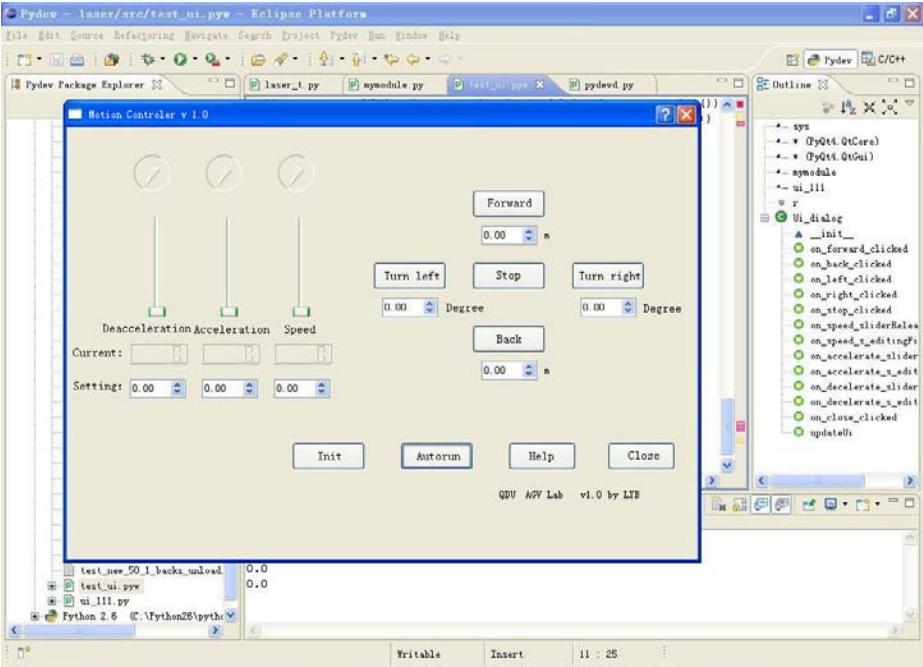
Fig. 3. GUI generated under Eclipse+pydev

Figure 4 shows the laser navigation mobile robots, the configuration of its industrial PC is of 2.8GHz, 1G memory. The robots can carry out environment accurately and stably with the speed of 1m/s, meet the needs of obstacle avoidance and navigation.

Fig. 4. The environment of experiment

5   Conclusion

(1) The function of mobile robot control system is improved to be openness and scalable by using Python and C/C++ mixed programming for development.
(2) Multi-threading method was used in laser navigation mobile robot, which is of a main processing, environment processing threading and motion control threading.
(3) PyQt toolkits was used for the development of GUI on mobile robot software system.

References

1. Beazley, D.M.: Automated scientific software scripting with SWIG. J. Future Generation Computer Systems 19(5 SPEC), 599–609 (2003)
2. Magoules, F., Putanowicz, R.: Visualization of large data sets by mixing Tcl and C++ interfaces to the VTK library. J. Computers and Structures 85(9), 536–552 (2007)
3. Hinsen, K., Langtangen, H.P., Skavhaug, O., Ødegård, Å.: Using B SP and Python to simplify parallel programming. J. Future Generation Computer Systems 22(1-2), 123–157 (2006)
4. Van Rossum, G., et al.: Python programming language. CWI, Department CST, The Netherlands (1994)
5. Blank, D., Kumar, D., Meeden, L., Yanco, H.: Pyro: A python-based versatile programming environment for teaching robotics. J. ACM Journal on Educational Resources in Computing 3(4) (2003)
6. Blank, D., Kumar, D., Meeden, L., Yanco, H.: The Pyro toolkit for AI and robotics. J. AI Magazine 27(1), 39–50 (2006)
7. Byungjoon, L., Hyunju, J., Gyun, W., Sungyoub, J., Joonkey, J.: Pyro implementation of swarm-bots exploring target objects in an area with irregular barriers. In: Proceedings - 2008 IEEE 8th International Conference on Computer and Information Technology, CIT 2008, pp. 670–675 (2008)
8. Kazanzides, P., Deguet, A., Kapoor, A.: An architecture for safe and efficient multi-threaded robot software. In: 2008 IEEE International Conference on Technologies for Practical Robot Applications, TePRA, pp. 89–93 (2008)
9. Yunha, J., Hyowoon, P., Sangjin, L., Mooncheol, W.: Development of a navigation control algorithm for mobile robots using d* search and fuzzy algorithm. Transactions of the Korean Society of Mechanical Engineers, A 34(8), 971–980 (2010); Language: Korean

Optimal Algorithms for Computing Policy-Conforming Paths in the Internet

Qixin Gao[1] and Lixin Gao[2]

[1] Northeastern University
Qinghuangdao, China
`gao263@sina.com`
[2] University of Massachusetts
Amherst, MA, USA
`lgao@ecs.umass.edu`

Abstract. Border Gateway Protocol (BGP) is an interdomain routing protocol that allows Autonomous Systems (ASes) to apply local policies for selecting routes and propagating routing information. These routing policies are typically constrained by the contractual commercial agreements between administrative domains. For example, an AS sets its routing policy so that it does not provide transit services between two of its providers. As a result, a route selected for a packet in the Internet may not be the shortest AS path. In this paper, we formulate two common routing policies in the Internet and the problem of computing routing policy conforming paths. We present optimal algorithms for computing the policy-conforming paths in the Internet and show the complexity of these algorithms. Understanding AS paths chosen in the Internet is critical to answer "what if" questions such as which ISPs an AS should peer with next in order to reduce the path length of the AS' customers to a content provider, or which ISP an AS should select as a provider in order to be "closer" to a popular content provider. Deriving AS paths in the Internet is also important for understanding how the global AS level topology evolution impacts the actual AS paths taken by packets.

Keywords: Border Gateway Protocol, Internet routing, routing policy.

1   Introduction

The Internet connects thousands of Autonomous Systems (ASes) operated by Internet Service Providers (ISPs), companies, and universities. Routing within an AS is controlled by intradomain protocols such as static routing, OSPF, IS-IS, and RIP. ASes interconnect via dedicated links and public network access points, and exchange reachability information using the Border Gateway Protocol (BGP) [1]. BGP is an interdomain routing protocol that allows ASes to apply local policies for selecting routes and propagating routing information, without revealing their policies or internal topology to others. These routing policies are typically constrained by the contractual commercial agreements between administrative domains. For example, an AS typically sets its routing policy so that

it does not provide transit services between two of its providers. As a result, a route in the Internet is determined by routing policies and not necessarily the shortest AS path in the Internet.

In this paper, we present two common routing policies and formulate the problem of computing policy-conforming paths in the Internet. The two common routing policies are described as follows. First, it is typical that an AS does not transit traffic between its providers or peers. This is referred to as no-valley routing policy. Second, it is common that an AS prefers its customer route over its provider or peer routes. This is referred to as prefer-customer routing policy. Third, it is common that an AS prefers its peer routes over its provider routes. This is referred to as peer-over-provider routing policy. Based on these two routing policies, we formulate the problems of deriving the shortest path that conforms the two policies, each of which progressively has more and more restricted routing policy. We prove that these computed paths are the shortest paths that conform to policy constraints, and provide the complexity of the algorithms.

Computing the policy-conforming routing paths in the Internet has several important implications. First, many protocol evaluation studies such as understanding routing protocol convergence speed [2] depend on the length of the actual policy-conforming AS path. Second, AS paths taken by an AS can affect services the AS receives. Important decisions such as ISP selection or peering AS selection may need to take actual AS paths into consideration. Computing policy-conforming AS paths can effectively quantify the tradeoffs between cost of ISPs and their reachability. Third, despite the common belief that AS-level topology becomes denser, it does not necessarily reflect that the packets in the Internet takes shorter AS paths. The impact of routing policies on the actual paths taken by packets is critical in understanding the impact of the evolution of AS-level topology on routes in the Internet. Most of the studies on the Internet path [3] focus on router-level path or on inferring AS-level paths from traceroute [4–6]. In order to understand the impact of ISP selection and AS-level topology, deriving actual AS-level paths is critical.

The remainder of the paper is structured as follows. Section 2 presents an overview of AS-level topology, commercial agreements, and common routing policies. In Section 3, we present an algorithm that computes the paths that conform to the no-valley routing policy. We then present an algorithm that computes the paths that conform the no-valley and prefer-customer routing policy, and an algorithm that conforms to no-valley, prefer-customer, and prefer-peer-over-provider routing policy. We conclude the paper in Section 4 with a summary.

2   Common Routing Policies

In this section, we first present AS-level topology and annotate the topology with commercial agreements. We then describe routing policies commonly deployed in the Internet.

2.1   Annotated AS Graph

The Internet consists of a large collection of hosts interconnected by networks of links and routers, which is partitioned into thousands of autonomous systems (ASes). An AS has its own routers and routing policies, and connects to other ASes to exchange traffic with remote hosts. A router typically has very detailed knowledge of the topology within its AS, and limited reachability information about other ASes. Since we mainly concern AS-level paths in this paper, we model the connectivity between ASes in the Internet using an AS graph $G = (V, E)$, where the node set V consists of ASes and the edge set E consists of AS pairs that exchange traffic with each other. Note that the edges of AS graph represent logical connections between ASes and do not represent the form of the physical connection.

Routing policies are constrained by the commercial contractual agreements negotiated between administrative domain pairs. These contractual agreements include customer-provider and peering. A customer pays its provider for connectivity to the rest of the Internet. A pair of peers agree to exchange traffic between their respective customers free of charge.

In order to represent the relationships between ASes, we use an *annotated AS graph* – a partially directed graph whose nodes represent ASes and whose edges are classified into provider-to-customer, customer-to-provider, and peer-to-peer edges. Furthermore, only edges between providers and customers in an annotated AS graph are directed. Figure 1 shows an example of an annotated AS graph. When traversing an edge from a provider to a customer in a path, we refer to the edge as a *provider-to-customer edge*. When traversing an edge from a customer to a provider, we refer to the edge as a *customer-to-provider edge*. We call the edge between two ASes that have a peer-to-peer relationship a *peer-to-peer edge*.
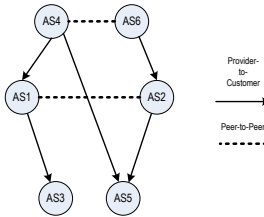
Fig. 1. An Annotated AS graph

2.2   Routing Policy

Routing policies typically conform to the commercial relationships between ASes. The commercial contractual relationships between ASes translate into the export rule that an AS does not transit traffic between two of its providers and peers. Formally, we define $customer(a)$, $peer(a)$, and $provider(a)$ as the set of customers, peers, and providers of a, respectively. We classify the set of routes in an AS into customer, provider, and peer routes. A route r of AS u is a *customer (provider, or peer) route* if the first consecutive AS pair in $r.as\_path$ has a

provider-to-customer (customer-to-provider, or peer-to-peer) relationship. More precisely, let $r.as\_path = (u_1, u_2, \ldots, u_n)$. If (u_1, u_2) is a provider-to-customer (customer-to-provider or peer-to-peer) edge, then r is a customer (provider or peer) route. An AS selectively provides transit services for its neighboring ASes. The selective export rule translates into *no-valley* routing policy. Intuitively, if we image that provider is always above its customers and two peering ASes are at the same level, then once an AS path goes down or remains at the same level, it does not go up or remain at the same level. Formally, the no-valley routing policy is defined as follows.

No-valley: In a no-valley AS path $(u_1, u_2, \ldots, u_n)$, there is i such that $0 \le i < n+1$ and for all $0 < j < i$, (u_j, u_{j+1}) is a customer-to-provider edge, (u_j, u_{j+1}) must be a provider-to-customer edge for any $i+1 < j < n$, and (u_{i+1}, u_{i+2}) can be either a peer-to-peer or provider-to-customer edge.

For example, in Figure 1, AS paths (1, 4, 6, 2) and (1, 4, 5) are no-valley paths while as_path (4, 5, 2) and (4, 1, 2, 6) are not no-valley paths. In addition to the no-valley routing policy, an AS typically chooses a customer route over a route via a provider or peer since an ISP does not have to pay its customer to carry traffic or maintain a traffic volume ratio between the traffic from and to a peer. Formally, we have a prefer-customer property for the import policy of AS a:

Prefer-customer: If $first(r_1.as\_path) \in customer(a)$ and $first(r_2.as\_path) \in priv\_peer(a) \cup provider(a)$, then $r_1.loc\_pref > r_2.loc\_pref$.

In addition to the prefer-customer property, an AS typically chooses a peer route over a provider route since an AS has to pay for the traffic its provider carries for it. Formally, we have a prefer-peer-over-provider routing policy:

Prefer-peer-over-provider: If $first(r_1.as\_path) \in peer(a)$ and $first(r_2.as\_path) \in provider(a)$, then $r_1.loc\_pref > r_2.loc\_pref$.

Therefore, we have two routing policies.

No-Valley Routing Policy: All ASes follow the selective export rule and therefore, all AS paths are no-valley paths. Furthermore, an AS chooses the AS path that is the shortest among all no-valley AS paths.

No-Valley-and-Prefer-Customer Routing Policy: In addition to the no-valley routing policy, all ASes follow the prefer-customer import policy. Furthermore, an AS chooses the AS path that is the shortest among all no-valley-and-prefer-customer AS paths.

3   Computing Policy-Conforming Paths

In this section, we present the algorithm to compute the path no-valley paths. To compute the shortest paths among all no-valley paths from all nodes to a single destination node, d, we propagate the paths to neighboring nodes starting with node d. We first propagate from customer to provider to derive the shortest customer paths. We then use the shortest customer paths to derive the shortest peer paths by propagating the customer path to a peer. Finally, we propagate customer and peer paths to a customer to derive the shortest provider paths. In the process of the path propagation, we maintain three shortest path lengths as follows.

- *Straight path length*: the length of the shortest straight path. *A straight path* is a no-valley path that contains provider-to-customer edges but does not contain any provider-to-customer or peer-to-peer edge. Note that a straight path can be announced to any neighbor, and therefore can be extended by any edge.
- *Step path length*: the length of the shortest step path. *A step path* is a no-valley path that first traverses a peer-to-peer edge and then traverses zero, one or more provider-to-customer edges. Note that a step path can be announced to a customer only, and therefore can be extended by a customer-to-provider edge.
- *Arc path length*: the length of the shortest arc path. *An arc path* is a no-valley path that contains zero, one or several customer-to-provider edges, followed by zero or one peer-to-peer edge, followed by zero, one or several provider-to-customer edges. Note that an arc path can be announced to a customer only and therefore can be extended by a customer-to-provider edge only.

Since we do not have prior information whether the shortest no-valley path is an arc, step or straight path, and the extension rules differ for different types of paths, we maintain the shortest arc, straight, and peer paths for each node.

In order to compute the shortest straight paths, we first compute the shortest customer paths by propagating the path from customer to provider. We then propagate the path from peer to peer to compute the shortest step paths. Finally, we propagate the path from provider to customer to compute the shortest arc path as well as the shortest no-valley paths. Note that provider or peer paths does not propagate to providers or peers. Therefore, we can finalize the no-valley paths after the propagating from providers to customers. We have the following outline for the two algorithms that compute paths conforming to the two common policies.

```
Input: Annotated AS graph G and destination node d
Output: policy-conforming AS paths from all nodes to node d
Phase 0: Initialization:
        Let node d be the selected node
        Set node d's straight path length to be 0
        Set all other nodes' straight, step, arc path lengths to infinity.
Phase 1: Compute shortest straight path
Phase 2: Compute shortest step path
Phase 3: Compute shortest arc path and policy-conforming path
```

We describe the algorithms for computing shortest customer paths, and shortest peer paths as follows.
Compute shortest straight paths:

```
1. while there is a selected node,
2.   Update the path length of providers of the selected node, i.e.,
     for each provider of the selected node,
3.       if the node does not have straight path length set or
         the current straight path length is larger than
```

```
                 selected node's straight path length +1
4.          set the straight path length to be
            selected node straight path length +1
5.     select a node with smallest straight path length among
       nodes that have not been selected
```

Compute shortest step paths:

```
1. for each node u whose straight path length is not infinity,
2.     for each of u's peer, v
3.         update the step path length of v to be min
           of straight path length of u +1 and step path length of v
```

3.1   Computing No-Valley Paths

To compute the no-valley paths, we compute the arc paths using the the shortest paths among straight, arc, and step paths as follows.

Computing No-Valley-Path:

```
1. Select the node with the smallest arc, step, or straight path length
2. while the selected path length is not infinity
3.         Set the no-valley path length of the selected node
           to be the shortest among its arc, step and straigh paths
4.         for each customer u of the selected node
5.             update the arc path length of u to be
               min of no-valley path length of selected node+1,
               step path length of $u$, and  arc path length of u
6.         Select the node with the smallest arc, step or straight path length
           among all nodes that have not been selected
```

3.2   Computing No-Valley-and-Prefer-Customer

In order to compute the no-valley-and-prefer-customer paths, we compute arc path as follows.

Computing No-Valley-Prefer-Customer-Path:

```
1. For each node,
       if its straight path length is not infinity
           Set its no-valley-prefer-customer path to be its straight path
       else
           Set its no-valley-prefer-customer path to be its peer path
2. Select the node with the smallest no-valley-prefer-customer path length
3. while the selected path length is not infinity
4.         for each customer u of the selected node
5.             Update the arc path length of u to be
               min of no-valley-prefer-customer path length of selected node+1,
               and  arc path length of u
6.             if the customer path length of u is infinity
                   Update the no-valley-prefer-customer path of u to be min
                   of no-valley-prefer-customer path and arc path of u
7.         Select the node with the shortest no-valley-prefer-customer path
           among all nodes that have not been selected
```

3.3   Computation Complexity

The above two algorithms traverse each edge of the annotated AS graph at most twice. Further, selecting nodes with shortest arc, step and straight path requires $N \log N$ time (if we use a heap to store the information of each node path length), where N is the number of nodes in the annotated AS graph. Therefore, it takes $O(E + N \log N)$ time to compute no-valley paths from all ASes to a destination AS, where N and E are the number of ASes and edges, respectively, in the annotated AS graph. For all pair AS paths, it takes $O(NE + N^2 \log N)$ time to compute AS paths from all ASes to all destination ASes.

4   Conclusions and Future Work

We describe common routing policies in the Internet and formulate the problem of computing the paths that conform to these routing policies. ISPs have incentive to conform to the two routing policies described and therefore it is important to understand how to compute the routing paths that conform to these routing policies. We present efficient algorithms for these computations and show the complexity of these algorithms. We show that our algorithms are efficent for large AS graph of the Internet.

References

1. Stewart, J.W.: BGP4: Inter-Domain Routing in the Internet. Addison-Wesley, Reading (1999)
2. Labovitz, C., Wattenhofer, R., Venkatachary, S., Ahuja, A.: The impact of Internet policy and topology on delayed routing convergence. In: Proc. IEEE INFOCOM (April 2001)
3. Tangmunarunkit, H., Govindan, R., Estrin, D., Shenker, S.: The impact of routing policy on Internet paths. In: Proc. IEEE INFOCOM (April 2001)
4. Mao, Z.M., Johnson, D., Rexford, J., Wang, J., Katz, R.: Scalable and accurate identication of as-level forwarding paths. In: IEEE INFOCOM (2004)
5. Morley, Z., Lili, M., Jia, Q., Zhang, W.Y.: On as-level path inference. In: ACM SIGMETRICS (2005)
6. Gao, L., Wang, F.: The extent of as path ination by routing policies. In: Proc. IEEE GLOBAL INTERNET (November 2002)

Design and Implementation of the LBS Interface for Personnel Positioning

Yanlan Yang, Hua Ye, and Shumin Fei

Southeast University, School of Automation,
Nanjing, China
{yyl,zhineng,smfei}@seu.edu.cn

Abstract. The realization of the personnel positioning base on LBS for the application is to make a socket based connection first and get the location information from the port of the LBS platform according to some interface specifications. To ensure the location service of the application stable and reliable, a short connection was proposed to solve the disconnection problem caused by network communication quality, and the asynchronous mode for data transportation was chosen to improve the real-time responsiveness of that interface. According to the specific needs for personnel locations, there are two ways to request location: calling the one or calling the group, which make the location services more flexible and convenient. The applying of this interface to a real application system for customer service management shows that the application system has a perfect interface to the LBS platform and obtains a fast and stable personnel positioning service.

Keywords: LBS, Personnel Positioning, Short Connection, Asynchronous Communication.

1   Introduction

In recent years, with the development of GPS technology and the improvement of communication network based on GSM/GPRS, the remote monitoring system for vehicles is growing at a speed which is quite unprecedented meeting different demands from various industries, such as traffic police scheduling, city logistics, taxi dispatching, etc. The mobile information management of vehicles indicates that the development of intelligent transport systems in our society become more sophisticated, which brings more urgent needs of mobile information management for people. Especially in the service sector, if both the service-related vehicles and personnel could be located, the integrated management of them would be possible in the remote monitoring system, which makes the scheduling work more efficient. However, there is still some difficulty in locating a person by GPS. Because the custom device with GPS module embedded should be made specially for human using, which must be portable and with long battery life. Although the existing mobile phone with GPS navigation can meet all the needs above, they are not widely used and lack of the function for real-time positioning data transmission. Therefore, the solution of personnel positioning based on GPS will cost a lot no matter in the development or the implementation.

The location based service (LBS) has established a new method for personnel positioning, which gets the position of the mobile equipment based on mobile communication base station and can transmit the positioning data to those authorized clients through mobile network [1]. As a matter of fact, mobile phones have been one of the portable necessary in the human life, so that a person's position can be easily found according to the positioning result of his mobile phone by LBS [2]. There are no extra costs of devices for positioning in this solution, and the real-time personnel positioning will be realized in the monitoring system based on LBS provided by the special operators. This paper first discusses the design of the LBS interface for personnel positioning and then makes the implementation to an existing monitoring system for vehicles to realize the integrated scheduling management of both vehicles and the personnel.

2   LBS Platform and Its Interface for Positioning

2.1   Overview of LBS Platform

As the mobile phone has become a necessity in our lives, the importance of LBS is coming out. The development momentum of LBS is very rapid due to its huge potential market. Many domestic mobile communication corporations have increased the development and promotion of their new business, taking advantage of the new international communication technology. They have gradually changed from providers of single voice services to mobile multimedia information services, and the LBS is one of the most important part of that [3]. More and more operators cooperate with the mobile communication company, launching their different LBS platforms providing the mobile users with integrated information services based on location.

The service provided by the platform locates the mobile equipment through moblie commucaition station and sends the positioning data to the geographic information system (GIS) for correction. The corrected result regarded as the final position is then sent through the mobile network to the client who requesets the location service [4]. In order to expand the business scope of LBS in the application, the LBS platform opens many interfaces for location service to support reliable coding work for different types of positioning request. Interfaces accepted by the LBS platform include message accessing as SMS/MMS, internet accessing, voice accessing like 1860 customer service center and the client accessing with JAVA/WAP [5].

2.2   Integration of LBS Business in the Application

The main purpose to design a LBS interface is to expand personnel positioning function in the remote GPS monitoring system. Here the LBS platform receives and responds to the positioning requests from the application side in the way of internet accessing, and the LBS platform is regarded as a server while the application side as a client (also known as the small platform). The small platform exchanges the data with the LBS platform by internet following a certain interface standard.

There are three rules defined by the LBS platform for small platform's accessing, and they are 1) Establish a socket connection between the LBS platform and the small platform; 2) the basic accessing process to the LBS platform for positioning services

is logging in first and then executing commands; 3) all data transmission is based on XML packets. The small platform must be in strict accordance with the message format to organize and parse the related packets, so that it can access to the LBS platform successfully and obtain the positioning services to realize the personnel positioning function by their phone number.

2.3   Structure of the Personnel Positioning System Based on LBS

The personnel positioning system based on LBS mainly provides useful spatial information for the remote command and scheduling of the sales and service personnel. The system regards mobile phones as its positioning equipment and the LBS platform as its positioning method, obtaining the object's position with the help of location-based services provided by the platform. Due to the fact that the LBS platform calculates the position by detecting the signal strength of cell phone and combining with the GIS information, the positioning accuracy of the system is decided by the distribution density of mobile station and the GIS functions provided by the LBS platform [6].

The personnel positioning system consists of four parts, cell phone (personnel), mobile network, positioning client and LBS platform. Fig. 1 shows the structure of the system.
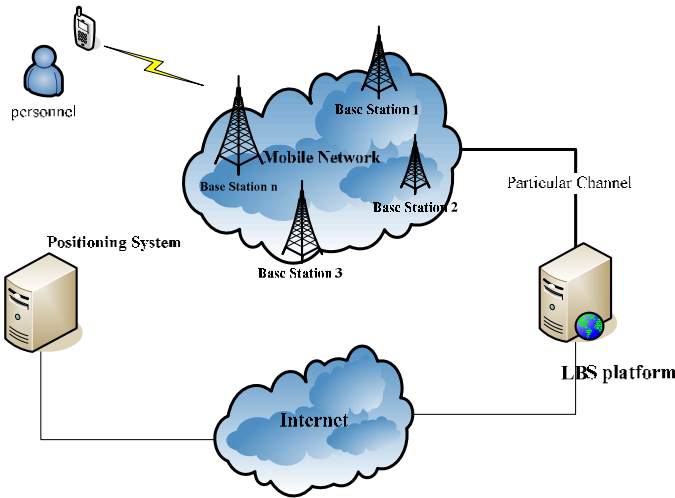

Fig. 1. Structure of the personnel positioning system based on LBS

3   Design of the LBS Interface for Personnel Positioning

According to the definition of the interface which applications use to apply LBS, when an application system requires personnel positioning from the LBS platform, it needs to send a log message to the platform firstly and wait for its identification authentication. If the authentication was successful, the command for positioning

could be sent. Considering that personnel positioning work involves something about privacy security, the positioning service emphasizes on the security control in the software designing.

The LBS interface for personnel positioning includes two parts, the communication interface to access the LBS platform and the functional interface for clients to call personnel positioning. The former focuses on the realization of the communications based on network, while the latter is designed for specific applications.

3.1   The Communication Interface for LBS Platform

As shown in Fig.1, LBS platform as a server is responsible for listening to connection requests from different applications and identifying their permissions to the platform. If the application is authorized, the platform will keep its connection online until it disconnects itself, and the locating requests from the application side will be accepted and answered in time during that period. In summary, the LBS platform has the following characteristics:

- LBS platform never disconnects the connection to the application side once it establishes.
- Each application side is only allowed to create one valid connection to the LBS platform at the same time.
- There is a 2-3 seconds delay when the application side gets the return information from LBS platform.

Considering the service performance of the platform above, the key points to design the LBS interface for the application side is all about the mode selecting on connection and data transmission.

Key Point 1: Short Connection to the LBS Platform
When the application side chooses the long connection mode to access to LBS platform, it is usually difficult for the platform side to catch the exception if the connection is suddenly broken by some objective reasons, such as network congestion or cable damage, unless the application as a client disconnects actively. Because the case of "pseudo-connection" exists in the platform server, the application side may fail to rebuild a new connection to the platform after its pre-connection is disconnected, limited by the condition that one single connection for one application. And the LBS platform can not keep providing location-based service for the application. If such situation continued, the function of personnel positioning in the application side would be disabled for a long time, which was fatal to a personnel monitoring system.

Therefore, the management of connections in the application side is necessary. With the actual needs for personnel positioning, the application usually submits the service request to LBS platform regularly. It is suggested to use a short connection mode when the application side begins its locating service, and disconnect the connection immediately after it has finished receiving the positioning data from LBS platform. The short connection mode makes the application side avoid losing the control of its usual connection to the LBS platform because of the low probability for abnormal network situations, which ensure the success of each positioning request. At

the same time, the phenomenon of "pseudo-connection" is no long also existed in the platform side so that each application can easily rebuild their connections and keep providing a stable and reliable positioning service based on LBS.

Key Point 2: Asynchronous Communication for Data Transmission
Because the application communicates with the LBS platform based on internet, the quality of network status affects directly the success of request sending or data receiving [7]. And the data transmission delay is the most common problem due to the poor network traffic. Meanwhile, the whole process for LBS platform to accept the positioning request and return back the positioning data is strictly controlled, which needs to take some treating time. Even in the case with a good network, it still needs to wait 2-3 seconds before getting the return information generally. Besides, the application side is a typical multi-threaded parallel processing system with a high demand for quick responses. As it still has other businesses to do in addition to providing location-based services, such as the data collection of mobile terminals based on GPS and transaction requests from the client, Therefore, it is strongly recommended to choose asynchronous communication during the data transmission between the LBS platform and the application.

In the asynchronous communication mode, there exist three separate threads in the whole process (Fig.2). Firstly, the application side sends an asynchronous request to start positioning in the thread 1 and creates the thread 2. Thread 2 stops until the positioning request has been sent. If the transmission is successful, thread 3 will be created to receive the positioning data in an asynchronous way, otherwise the application side will try to resend or report an error. Thread 3 is responsible for receiving the return data from the LBS platform, parsing the data and storing them into the database.
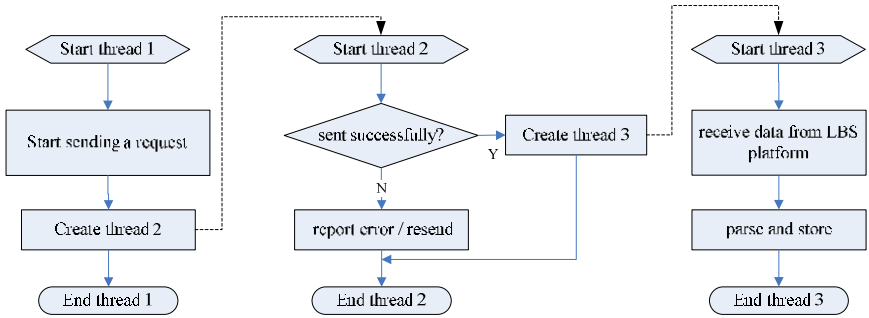

Fig. 2. There processing threads in the asynchronous communication mode

3.2   The Functional Interface for Personnel Positioning Service

Considering the factors in the application side, design of the interface for personnel positioning is mainly on the basis of the two following rules:

- Login to the LBS platform first and send positioning requests after identification is authorized.
- Each positioning request message can be used to locate one cell phone.

According to the actual demand for personnel positioning, two kinds of interfaces have been developed including the signal call and the group roll-call. The signal call do the positioning work once a time, and an independent session will be built when performing the signal call, while the group roll-call is for a group. When the group roll-call is executed, the positioning messages are sent one by one although the request with a group of phone numbers is submitted at one time. Compared to the single call, a series of positioning requests will be sent in the same session in the group roll-call, which makes the group roll-call own higher efficiency and network utilization. However, the signal call is more flexible and it can meet the need of real-time positioning.

Therefore, design of the LBS interface for personnel positioning on the application side adopts the strategy to provide positioning services, and that is mainly based on the group roll-call and takes the signal call as a complementary way. The group roll-call is executed regularly in order to update all of the personnel's position, which can be used to check personnel's history track. The time interval depends on the update frequency demanded by the system. When it is necessary, the application side will execute the signal call to check some particular person's latest position.

However, in order to ensure reliable positioning function the implementation of group roll-call is still based on the process of the signal call. That is, the network connection with LBS platform and the login status should be detected before the transmission when executing a group roll-call. If the connection and the login status are abnormal, the application side needs to reconnect or re-login. The process of group roll-call is shown in Fig. 3.

4   Implementation of the LBS Interface

The LBS interface for personnel positioning designed in this paper has been applied successfully into a remote monitoring system for a large enterprise, taking charge of location monitoring of the service personnel for the enterprise's customer service center. According to the requirements from customer service center, the system needs to monitor the personnel's historic positions during normal working period. Then the center can propose reasonable personnel scheduling solution based on the real-time distribution of them to supply the users a more timely and efficient service. Integrating the personnel positioning service into the monitoring system means a nationwide network for service personnel has been built, which enhances the scheduling ability of the center and improves the working efficiency of service personnel.

In the system for service personnel positioning, the group roll-call is executed per hour for gathering the position information of all service personnel. Because this function is performed regularly, the historic position of service personnel has been collected which can be used to check the personnel's working track. When the latest position of one target personnel is needed, the system executes the single call. Thus, the interfaces for the group roll-call or the single call are all necessary in the actual application. The Integration of the two types of interfaces can meet the needs of most applications.

Tests on connecting the application to the LBS platform have been performed, which verify the validity of the short connection mode to accessing the LBS platform.
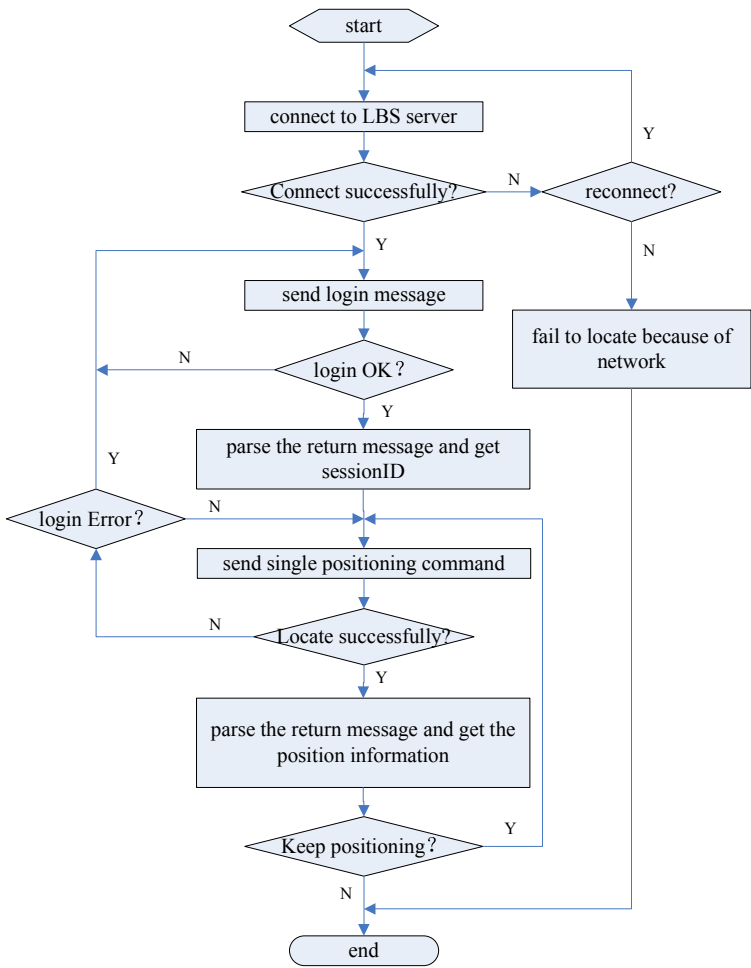
Fig. 3. Flow of group roll-cal based on LBS

Taking the group roll-call as an example, if a long connection mode is used, which means the application side doesn't end the connecting actively, missing of the network connection usually happens during the next roll-call when the executing interval is over 30 minutes. In this case, an error of reconnecting will be received on the application side if another request of a new connecting is sent to the LBS platform, which brings the failure of positioning further. However, if a short connection mode is used, the system sends a connection request to the LBS platform when necessary, and the connection will be ended by the application side actively when positioning information has been received successfully. At the same time, the system notifies the LBS platform to clear the current connection immediately. So the next positioning work will not be affected, which insures the application side provide continuous, reliable location based services.

5   Conclusions

The LBS interface for personnel positioning has implemented the connection between the application system for personnel positioning and the LBS platform. The application system takes the cell phone carried by the personnel as one kind of positioning devices, and it can acquire the personnel's latest position information through the LBS platform, which makes the management of personnel's position possible. In practice, the short connection mode and the asynchronous communication method used in the interface do improve the performance of the communication, which have also been proved to be effective in ensuring continuous and reliable positioning service.

References

1. Liu, L., Zhang, J.X., Tang, X.M., Li, W.W.: Research on architecture and key technologies of LBS. Science of Surveying and Mapping 32(5), 144–146 (2007) (in Chinese)
2. Wang, H., Yan, H., Ren, J., Bao, Q.: Design of Monitoring System for Vehicles Track on the Expressway Network Based on LBS. Journal of Chongqing Jiaotong University (Natural Science) 29(2), 261–264 (2010) (in Chinese)
3. Qi, P., Cai, J., Liu, W.P.: Design and Implementation of GIS in the LBS Platform. Science Technology and Engineering 9(6), 1438–1442 (2009) (in Chinese)
4. Wang, S., Min, J., Yi, B.K.: Location Based Service for Mobiles: Technologies and Standards. In: IEEE International Conference on Communication, Beijing (2008)
5. Dong, Z.N.: The Construction and Application of LBS Platform. Geomatics World 1(3), 19–22 (2003)
6. Zhu, S.M., Zhang, Q.J., Hou, L.S.: Design and Realization of the MLS System Based on Open Statand. Journal of Wuhan University of Technology 30(2), 329–331 (2006) (in Chinese)
7. Zheng, W.F., Yin, Z.T., Lu, H.B., Li, X.L.: LBS application in logistics management system. Science of Surveying and Mapping 34(3), 178–180 (2009) (in Chinese)

Finding Critical Multiple Paths
for Demands to Avoid Network Congestion[*]

Huawei Yang[1], Hongbo Wang[1], Shiduan Cheng[1], Shanzhi Chen[2], and Yu Lin[1]

[1] State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] State Key Lab of Wireless Mobile Communication, China Academy of
Telecommunication Technology, Beijing 100083, China
`huawei.g@gmail.com`

Abstract. Multi-path routing schemes have the inherent ability of balancing load between paths, and thus play a major role in traffic engineering for optimizing network distribution. The article proposes an algorithm of finding critical multiple paths, which determines paths between each pair of network nodes. The algorithm selects a small number of decisive paths, besides which few benefits can be obtained to balance load. Experiments on backbone networks with real traffic matrixes show the effectiveness of our algorithm in avoiding network congestion in terms of minimizing maximum link load.

Keywords: traffic engineering, congestion avoidance, multi-path routing, minimum cut.

1   Introduction

The Internet is now supporting many types of multimedia applications, with potentially high bandwidth demand. Typically, IP network providers adopt a strategy of bandwidth provisioning to accommodate increasing traffic. Nevertheless, the problem of network congestion has not been solved completely. Besides the congested links, the lightweight ones could be found everywhere due to the inefficient utilization of network bandwidth. A good approach for both better QoS and less congestion can be adopted by means of traffic engineering, which exploits bandwidth efficiently and postpones hardware upgrade.

Current routing mechanisms allow for some flexibility to implement traffic engineering algorithms. In OSPF/IS-IS network, a traffic flow arriving at the router is spitted equally between the links on the shortest paths to the destination. These

equal-cost multiple paths are constructed through carefully link weight settings. In MPLS network, arbitrary explicit paths are created before packets' forwarding. The traffic flows are classified into trunks which are carried on these paths between ingress and egress routers.

However, in those network environments stated above, several issues exist in modeling and implementing multiple paths. First, the optimal traffic distribution acquired from modeling of multi-commodity problem is not realistic. Second, periodical updates of routing schemes still cannot afford the dynamics of traffic. Third, the increase of network scale challenges routers' capabilities of computation and storage.

The article insists on that optimal traffic distribution is closely related to the locations of origin-destination (OD) routers, and that appropriate multiple paths between OD pairs can lift restrictions of above issues. To avoid network congestion, the article proposes an algorithm of finding critical multiple paths (hereafter abbreviated as FCMP), which determines paths between OD pairs to distribute traffic evenly. FCMP build these critical paths from links in minimum cuts, the potential bottlenecks in network. Balancing load over the network is expected via balancing traffic distribution over the critical paths.

The main contributions of this article include the following. (1) A new approach, especially as distinct from existing optimization methods, is proposed to solve multi-path problem. The way of graph theory is apt to locate bottlenecks related to OD pairs. (2) A new algorithm is brought forward to implement the solution and distribute traffic between critical paths. Those outside the set of critical paths share few responsibility for load balancing.

The rest of the article is organized as follows. We briefly review the state-of-the-art research related to our topic in Sec. 2. FCMP problem formulation and its algorithm implementation are detailed in Sec. 3, followed by network tests of real datasets from Europe and North American in Sec. 4. Then, we conclude and discuss future work on FCMP in Sec. 5.

2   Related Works

Routing optimization plays a key role in traffic engineering, finding efficient routes so as to achieve the desired network performance. With regard to routing implementation, today's intra-domain networks can be classified into two categories: OPSF/IS-IS and MPLS.

The article [1] draws an attention on popular intra-domain routing protocols such as OSPF and IS-IS, and reviews optimization techniques in networks operated with shortest path routing protocols. The general routing problem on optimal use of network resources is modeled as minimization of routing costs, on behalf of an objective function. The routing scheme must specifically follow the ECMP rule of the intra-domain routing protocols. As a result, link weights should be carefully configured, or even routing rules be relaxed, to approach the optimal traffic distribution [2, 3].

In sum, shortest path routing model pays attention on links rather than paths, and therefore ignores path bottlenecks which influence congestion ultimately. The algorithm

finding optimal weights depend on local search and an overall optimal traffic distribution may not be reached. Although new routing algorithms expect a better performance, the implementation is nontrivial.

The article [4] reviews MPLS forwarding scheme other than shortest path routing. In MPLS, traffic is sent along explicit paths and can be split arbitrarily over them. A generalized MPLS routing optimization can be formulated as a multicommodity flow problem, and can thus be solved using linear programming. The fundamental problem with MPLS is to compute routes and take interference estimation into consideration [5]. Recently, the oblivious property of routing problem attracts researchers' attention with no or approximate knowledge of traffic demands [6].

However, MPLS requires potentially huge number of paths, especially in a large-sized network, and that is impractical. Although the path number of an OD pair can be limited artificially, the reasoning behind path selection is fuzzy. In addition, the probability of paths interference could be decreased bypassing critical links, which should be considered across multiple demands.

Hence, the article propose FCMP algorithm to balance traffic distribution on bottleneck links, in an attempt to avoid network congestion. FCMP generate a small number of paths between any OD pair, and compute bottleneck links in a global view.

3   FCMP Algorithm

A routing specifies how to route the traffic between each OD pair across a given network. OSPF/IS-IS follows a destination-based evenly-split approach, and distributes traffic evenly on multiple paths with equal cost. The MPLS architecture allows for more flexible routing, and supports arbitrary routing fractions over multiple paths. The article [6] describes arc-routing and path-routing models corresponding to the two routing schemes separately. The optimization problems can be solved by a linear programming method.

Due to the rules enforced by protocols or the capabilities built in routers, it is nontrivial to achieve optimal traffic distribution using existing routing schemes. To decrease the hardness of multi-path routing, several problems must be addressed. First, the number of paths between an OD pair should be small enough to fit for routers. Second, the set of paths should play a decisive role in traffic distribution comparing to outsiders. Third, the links of paths potentially congested should be considered in a global view. In sum, critical multiple paths should be found between OD pairs.
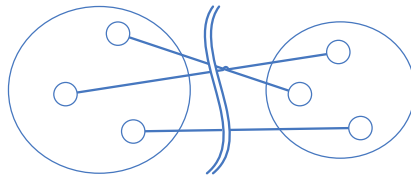

Fig. 1. A multicut is defined as a set of edges whose removal disconnects each source from its corresponding sink of demands

Our initial motivation is to find the potential bottleneck links. Network congestion could be controlled by means of traffic distributing over these links. To the case of multicommodity flow problem, the maximum flow is bound by minimum multicut. So, the links in minimum multicut are defined as the potential bottlenecks of the network in the article. Fig. 1 shows an example of multicut. Each commodity has its own source and sink, and multicut disconnects all the demand pairs. In a network, the capacity of link representing the weight, our problem asks for a minimum multicut.

The traffic demands should be routed along paths traversing bottleneck links in minimum multicut. These critical paths between OD pairs decide the final characteristic of network load. In a backbone network, the computed minimum multicut contains almost the same links as in the network, and could not be decomposed into subsets mapping to OD pairs. Therefore, the building of critical paths based on minimum cut is difficult.

In fact, for general networks, each commodity can be optimized separately using $1/k$ (where k is the number of demands) of the capacity of each edge [7]. This way, we can construct k networks each the same as the original one except for $1/k$ shrink of link capacity. For each one of these networks corresponding to a demand, the minimum cut defines the bottleneck location. Thus, our problem is resolved in the most basic cut problem, for which Ford and Fulkerson gave an exact algorithm [8].

To avoid network congestion, the article proposes FCMP algorithm to determine paths between OD pairs for traffic distribution. The key steps of FCMP algorithm are as follows. First, computing the minimum cuts related to each OD pair. Second, constructing multiple paths based on the minimum cuts. Here, the multiple paths between an OD pair are edge disjoint, and the number of paths is equal to the size of the minimum cut.

Fig. 2 shows a network demonstrating construction of critical paths between OD pair (2, 7). The minimum cut between OD pair (2, 7) are the set of links represented by {(5, 7), (6, 7)}. Then, we find two edge disjoint paths from source to sink, and they are (2, 3, 5, 7) and (2, 4, 6, 7).
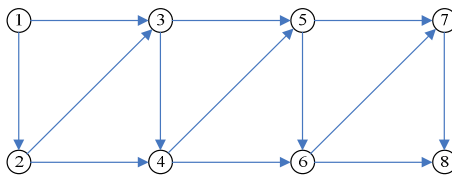

Fig. 2. An example network with 8 nodes is built. Supposedly, a traffic demand (2, 7) is routed through the network. FCMP selects paths (2, 3, 5, 7) and (2, 4, 6, 7) from available routes.

Corresponding to the network in Fig. 2, we illustrate the paths selected by FCMP algorithm in Fig. 3. Paths constructed from bottleneck links (5, 7) and (6, 7) back to source create opportunities to balance load on bottlenecks. It is obvious that FCMP algorithm select critical paths of small number from numerous available paths between OD pair.
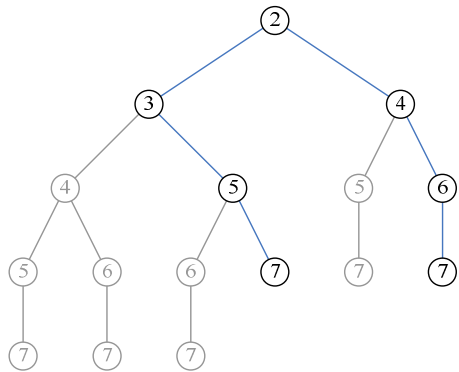
Fig. 3. FCMP algorithm selects 2 critical paths from 6 available paths between OD pair (2, 7). These paths are critical for load balance on bottleneck links.

The FCMP algorithm details in pseudo code listing below. Herein, the function for getting a minimum cut of a demand is supposed to be implemented using Ford-Fulkerson method. Shortest widest routing from ends of a link in minimum cut to source and sink of a demand constructs a path between an OD pair. The paths between an OD pair are assured to be edge disjoint.

```
program FCMP
{//assuming minimum cut between OD pair (i, j) is C_ij.
    set pathset = null;
    while(link l = nextlink(C_ij))
    {
        path p = shortestwidestpath(i, l);
        path q = shortestwidestpath(l, j);
        pathset += connect(p, q);
    }
}
```

4   Experiments

We do experiments in this section to verify performance of the FCMP algorithm. The selected backbone networks are Abilene and Geant, from North American and European separately. In those networks, traffic matrix [9, 10] captures are shown in Table 1.

Table 1. Traffic matrix datasets source information. Inner links are of concern to our experiments.

No.	Network	Network of nodes	Number of links	Duration	Sampling
1	Abilene	12	30	6 months	5 min
2	Geant	23	38	4 months	15 min

For comparison, OSPF routing algorithm commonly used in intra-domain network and a second routing algorithm we call it ODMP (an abbreviation for Origin-Destination Multi-Path) route the same traffic matrixes. OSPF routes traffic on shortest paths and allows even traffic split on next links. ODMP models an ideal routing scheme for even traffic distribution on all available paths between OD pairs. In the same way, FCMP routing algorithm distributes traffic evenly on found paths. For each experiment, we report both the maximum link load and the average link load collected throughout the network after traffic matrixes are routed by the algorithms.

Table 2. The two experiments carried on the two networks separately. The range of data source shown here are relative to corresponding dataset.

Exp.	Network	Purpose description	Source range	Sampling
I	Abilene	Performance contrast between light-load and heavy-load periods	21st week, 1333-1404	10 min
II	Geant	Performance production relative to average bandwidth consumption	2nd month, 1613-1648	15 min

Due to space limitations, we select two typical experiments carried on the two networks separately. The experiment descriptions and settings are shown in Table 2. In experiments, we first compute paths between OD pairs according to the routing algorithms, and then evenly distribute traffic flows among selected paths for each OD pair, and finally report the maximum link load and the average link load over the networks corresponding to each routing algorithm.

In experiment I, 36 traffic matrixes (lasting for 6 hours) are loaded via different routing algorithms, and the maximum link load of the network is computed. Fig. 4 depicts the degree of optimal traffic distribution of the algorithms across different traffic loadings. The middle section (about 7 traffic matrixes) of the curves gives a hint of heavy load, and here FCMP performs better than OSPF and ODMP, relative load decreases being 34.0% and 14.7% separately. The two ends of the experiment period indicate situations of light load, and there FCMP performs no less than OSPF. OSPF performs well in light load situation in Abilene, supposedly a result of long term adjusting of link weights.
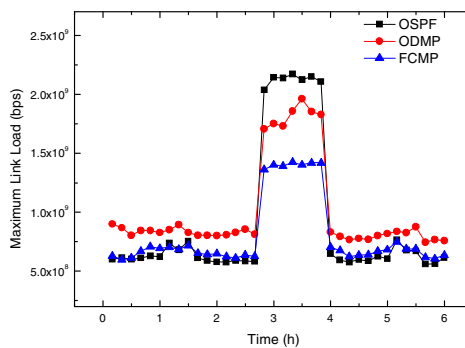

Fig. 4. A series of traffic matrixes are loaded via different routing algorithms. FCMP is superior to others in busy time, and is similar to OSPF in spare time.

In experiment II, 36 traffic matrixes (lasting for 9 hours) are routed, and Fig. 5 shows both the maximum link load and the average link load values at each traffic matrix point. The value of maximum link load describes optimism degree of traffic distribution, while the value of average link load expresses resource consumption for the optimism. In the testing period, FCMP acquires a load decrease of about 42.5%, at a cost of 47.5% bandwidth consumption. It is noticed that the maximum link load decreases by 1.19Gbps, while the average link load increases by 124Mbps.
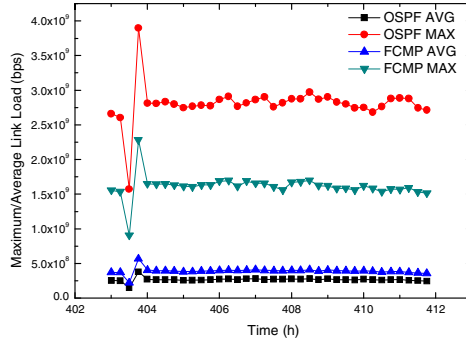

Fig. 5. FCMP acquires a large scale decrease of network congestion; meanwhile requires a small size increase of bandwidth consumption

5   Conclusion

With the development of Internet, traffic demands challenge the capabilities of ISPs. In the area of multi-path routing, FCMP provides a new method to balance load between critical paths, and therefore network congestion is avoided. FCMP determines a small number of paths between OD pairs, feasibly being implementable in current routers. FCMP computes a set of widest paths derived from minimum cuts, reserving bandwidth as much as possible for future demands. Experiments on backbone networks verify good performance on traffic distribution.

We also note that FCMP should be improved to fit in different situations. For example, in a network with link bandwidth changing rapidly, low capacity links should be cut. In other situations, varying in traffic matrixes and paths interference should be taken into consideration.

References

1. Altin, A., Fortz, B., Thorup, M., Ümit, H.: Intra-domain traffic engineering with shortest path routing protocols. 4OR 7(4), 301–335 (2009)
2. Sridharan, A., Guerin, R., Diot, C.: Achieving near-optimal traffic engineering solutions for current OSPF/IS-IS networks. TON 13(2), 234–247 (2005)
3. Xu, D., Chiang, M., Chiang, R.J.: DEFT: Distributed Exponentially-Weighted Flow Splitting. In: 26th IEEE International Conference on Computer Communications, pp. 71–79. IEEE Press, New York (2007)

4. Wang, N., Kin, H.O., Pavlou, G., Howarth, M.: An overview of routing optimization for internet traffic engineering. Communications Surveys Tutorials 10(1), 36–56 (2008)
5. Kodialam, M., Lakshman, T.V.: Minimum interference routing with applications to MPLS traffic engineering. In: Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies, pp. 884–893. IEEE Press, New York (2000)
6. Li, Y., Bai, B., Harms, J., Holte, R.: Multipath oblivious routing for Traffic Engineering - stable and robust routing in changing and uncertain environments. In: Mason, L.G., Drwiega, T., Yan, J. (eds.) ITC 2007. LNCS, vol. 4516, pp. 129–140. Springer, Heidelberg (2007)
7. Leighton, T., Rai, S.: Multicommodity max-flow min-cut theorems and their use in designing approximation algorithms. J. ACM 46, 787–832 (1999)
8. Ford, L.R., Fulkerson, D.R.: Flows in Networks. Princeton University Press, Princeton (1962)
9. http://www.cs.utexas.edu/~yzhang/research/Abilene-TM/
10. Uhlig, S., Quoitin, B., Lepropre, J., Balon, S.: Providing public intradomain traffic matrices to the research community. SIGCOMM Comput. Commun. Rev. 36, 83–86 (2006)

A Short-Wave Communication System Based on Fountain Codes

Rui-Na Yin and Ke-Bin Jia

Beijing University of Technology
100124 Beijing, China
`yinruinabjut@163.com`

Abstract. Fountain codes are a new class of ratelss codes with low encoding and decoding complexity and have broad prospects in engineering applications. On the basis of the introduction and analysis of two typical fountain codes, this paper puts forward the proposal that fountain codes can be used in the short-wave communication and also designs the short-wave communication system based on Raptor codes. This system can improve the transmission efficiency and reliability of the short-wave communication due to the rateless property of fountain codes.

Keywords: Short-wave communication, LT codes, Raptor codes, BP.

1   Introduction

Short-wave is the radio wave within the frequency ranges of 3-30MHz. It is transmitted mainly through the sky wave which is radiated to high-altitude, reflected or refracted to the ground by the ionosphere of the sky [1]. Short-wave communication is the most ancient radio communication and has the advantages of good flexibility and low cost. Compared with satellite communication and wire communication, the ionosphere used in the short-wave communication is not vulnerable to Man-made destruction. Therefore, short-wave communication is the best or even the only means of communication in unexpected circumstances, especially in wartime or emergency situations. In many countries, short-wave communication network is a strategic communication network. The research on short-wave communication is of great significance.

Short-wave is transmitted by the ionosphere, while the height and density of the ionosphere are susceptible to weather factors, so the stability of short-wave communication is poor and the noise is strong in the channels. Data packet loss in transmission is quite serious, leading to low transmission efficiency.

Fountain codes [2] [3] are a class of rateless codes. The number of encoding symbols is potentially limitless. Furthermore, encoding symbols can be generated as few or as many as needed. No matter how many symbols are lost in transmission, the decoder can recover an exact copy of the original data once receiving a sufficient number of correct symbols. In recent years, fountain codes have been widely applied in multimedia broadcasting service of 3G network because retransmission is not

needed. We can also improve the efficiency of short-wave communication by using fountain codes' advantage of no retransmission.

2 Typical Fountain Codes

John Byers and Michael Luby etc put forward the concept of digital fountain for large-scale data distribution and reliable broadcast application in 1998. In 2002, Michael Luby proposed Luby Transform (LT) codes [4] which are the first class of fountain codes and Shokrollahi introduced Raptor codes [5] on the base of LT codes in 2006.

2.1 LT Codes

LT codes are the first practical realization of fountain codes. The length of symbols generated from original data can be arbitrary and the encoding and decoding complexity of LT codes is low.

A   Encoding

If the original data consists of k input symbols (bits or bytes, for example), each encoding symbol is generated independently from the exclusive-or of different original symbols [6]. The LT encoding process is as follows.

- Select randomly an integer $d \in (1, \ldots, k)$ as the degree of the encoding symbol from a degree distribution $\rho(d)$.
- Choose uniformly at random d distinct original symbols and generate an encoding symbol the value of which is the exclusive-or of them.
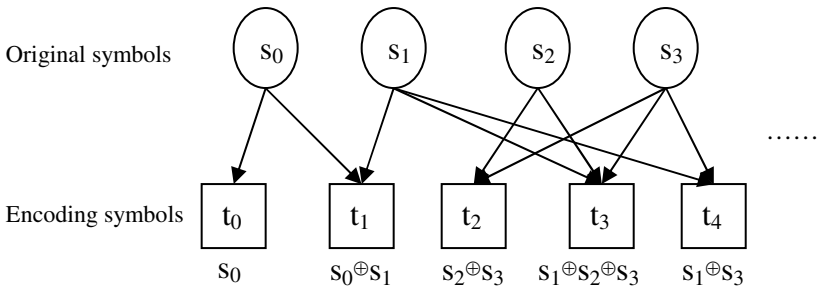- Go to the step 1 until the encoding symbols are as many as needed.

Fig. 1. Encoding graph of LT codes

B   Decoding

The belief-propagation (BP) decoding is the inverse of LT encoding, and the process is as follows.

- Find an encoding symbol t_n that is connected to only one original symbol s_k . If t_n doesn't exit, the decoding can not be continued.
- Set $s_k = t_n$, so s_k can be recovered immediately since it is a copy of t_n .
- Set $t_i = s_k \oplus t_i$ such that t_i is any other encoding symbol that is connected to s_k .
- Remove all edges connected to s_k and the degree of t_i is decreased by one.
- Go to step 1 until all of the original data are recovered.

C   LT Degree Distributions

The degree distribution is the key factor affects the LT encoding and decoding performance. We should pay attention to the following three aspects when designing $\rho(d)$.

- The encoding symbol that is connected to only one original symbol must be found constantly to ensure success of the LT decoding.
- The average degree of the encoding symbols is as low as possible to reduce the complexity of LT codes. The average degree is the number of symbol operations on average it takes to generate an encoding symbol.
- Some encoding symbols must have high degree to make sure that each of the original symbols has been chosen to generate the encoding symbol at least once.

Two typical LT degree distributions are the Ideal Soliton distribution and Robust Soliton distribution. If the original data consists of k input symbols, the Ideal Soliton distribution is as follows.

$$\rho(d) = \begin{cases} \dfrac{1}{k} & d = 1 \\[2mm] \dfrac{1}{d(d-1)} & d = 2,3,\ldots,k \end{cases} \tag{1}$$

The Ideal Soliton distribution works perfectly if the expected behavior of the LT process is the actual behavior. There is always exactly one encoding symbol the degree of which is one in the ripple, so that exactly one encoding symbol is released and an original symbol is processed each time. However, the Ideal Soliton distribution works poorly in practice because the expected ripple size is one, and even the smallest variance leads to failure of the LT decoding.

The Robust Soliton distribution adds $\tau(d)$ to the Ideal Soliton distribution for improvement of the LT codes performance. Let

$$S = c \ln(\frac{k}{\delta})\sqrt{k} \tag{2}$$

Define

$$\tau(d) = \begin{cases} \dfrac{S}{kd} & d = 1,2,\ldots,\dfrac{S}{k}-1 \\[2mm] \dfrac{S}{k}\ln(\dfrac{S}{d}) & d = \dfrac{S}{k} \\[2mm] 0 & d > \dfrac{S}{k} \end{cases} \qquad (3)$$

The Robust Soliton distribution is defined as follows.

$$u(d) = \frac{\rho(d)+\tau(d)}{\sum_{d}(\rho(d)+\tau(d))} \qquad (4)$$

The parameter δ is the allowable failure probability of decoding for a given number k input symbols. Another new parameter c is a constant which satisfies $c > 0$. The supplement of δ and c makes the expected ripple size is about $\ln(k/\delta)\sqrt{k}$. The Robust Soliton distribution ensures the expected ripple size is large enough in the decoding so that it has a higher success rate of LT process in practice.

2.2   Raptor Codes

In the LT process, the k original symbols can be recovered from about $k + o(\sqrt{k}\ln^2(k/\delta))$ encoding symbols with the allowable failure probability δ by on average $o(\ln(k/\delta))$ symbol operations for each encoding symbol. It implies that LT codes can not be processed with constant cost if the number of collected encoding symbols is close to the number of original symbols [5]. In addition, all the original symbols can be obtained only when the LT decoding is completely successful. The Raptor codes solve these problems by the supplement of precoding.
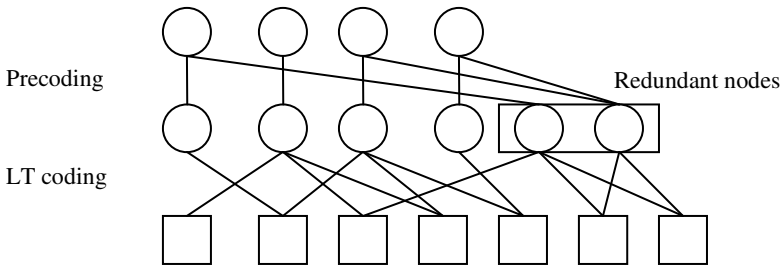

Fig. 2. Encoding graph of Raptor codes

The encoding of the Raptor codes is divided into two steps. First to encode the input symbols using a traditional erasure correcting code such as LDPC code to append the redundant symbols, and then generate the output symbols from the pre-coded input symbols by LT codes. Corresponding to the encoding, LT decoding is

firstly used to recover a constant fraction of the original symbols. Then all the original symbols can be recovered completely by the error-correction ability of the traditional erasure correcting code.

The cost of Raptor codes is lower than LT codes. For a given integer k and any real $\varepsilon > 0$, $k(1+\varepsilon)$ encoding symbols should be connected to recover all of the original symbols in the Raptor codes. Each encoding symbol is generated by on average $o(\ln(1+\varepsilon))$ symbol operations.

3   The Short-Wave Communication System Based on Fountain Codes

We have known that fountain codes have low encoding and decoding complexity with the advantage of no retransmission through the above introduction. Therefore, the fountain codes can be also used in the short-wave communication in order to obviously improve the transmission efficiency and reliability. We design a short-wave communication system based on fountain codes, which is given in Fig. 3.
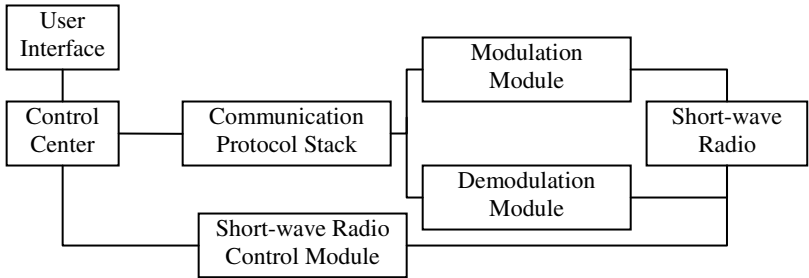

Fig. 3. A short-wave communication system based on fountain codes

The system shown in Fig.3 consists of seven modules. The communication between modules is realized by the socket, transferring the instructions and file data.

Each module is responsible for its own function and the coupling between these modules is low. The modular construction is convenient for the development and maintenance of the system. The function of each module is as follows.

- The user interface is responsible for the man-machine interaction. We can configure the working parameters for all the modules and send the instructions through the user interface in the transmission. The current working state is also displayed in it.
- The control center analyzes instructions and data, and then sends them to the corresponding module.
- The communication protocol stack is responsible for the encoding and decoding of fountain codes, encapsulation of the encoded data, generation of the feedback information and adjustment of the sending rate and number of data in two-way communication. The Raptor codes are suitable for this system

for its lower complexity and higher success probability of decoding compared to LT codes. According to the characteristics of fountain codes, the decoder can recover all the original data as long as enough correct encoding symbols are collected, no matter how much loss of data in transmission.

- The modulation module changes the carrier frequency of the data to suit transmission channel. The demodulation is the reverse of modulation.
- Current working state and working parameters of short-wave radio such as frequency and power are set by the short-wave radio control module.
- The sender transmits the modulated signal by the short-wave radio. And the radio in the receiver receives data at the same frequency.

Communication can be one-way or two-way in this system. The sender does not consider channel condition and sends all of the encoding data as a fixed rate when using one-way communication. Two-way communication is more difficult. However, it is more accurate. Fewer mistakes occur and fewer problems arise. Data is sent for several times in two-way communication. The receiver feeds back the information of this receiving process, including the accuracy and SNR. The sender uses the feedback information to adjust the sending rate and packet number for the rest of encoded data so that two-way communication has better energy efficiency and better channel utilization. The sender stops encoding when receiving the feedback information that all the original symbols have already recovered, and this transmission process finishes.

4   Conclusion

The research on short-wave communication still has great significance because it plays an important role in the emergency situation. A short-wave communication system based on fountain codes is given in this paper after the introduction of fountain codes. This system can overcome the disadvantages of low transmission efficiency and reliability in short-wave communication and has a great practical value.

References

1. Zhang, D.B., Huang, J.-M., Deng, Z.L.: Planner Spiral Antennas Applied on Short-Wave Communications. In: Proceedings of 5th International Conference on Wireless Communications, Networking and Mobile Computiong, pp. 1–4 (2009)
2. Byers, J.W., Luby, M., Mitzenmacher, M.: A Digital Fountain Approach to Asynchronous Reliable Multicast. IEEE J. on Selected Areas in Communications, Special Issue on Network Support for Multicast Communications (2002)
3. Byers, J.W., Luby, M., Mitzenmacher, M., Rege, A.: A Digital Fountain Approach to Reliable Distribution of Bulk Data. In: Proceedings of ACM Sigcomm 1998, pp. 56–67 (1998)
4. Luby, M.: LT Codes. In: Proceedings of 43rd Annual IEEE Symposium Foundations of Computer Science (FOCS), Vancouver, pp. 271–280 (2002)
5. Shokrollahi, A.: Raptor Codes. IEEE Trans. Inf. Theory 52, 2551–2567 (2006)
6. Ahmad, S., Hamzaoui, R., Al-Akaidi, M.: Unequal Error Protection Using LT Codes and Block Duplication. In: Proceedings of 9th Middle Eastern Simulation Multiconference, pp. 104–108. EUROSIS-ETI, Ghent, Belgium (2008)

Logistic Regression Parameter Estimation Based on Parallel Matrix Computation

Zhen Liu and Meng Liu

Web Science Center, School of Computer Science and Engineering, University of Electronic Science and Technology of China 610054 Chengdu, P.R. China
quake.liu0625@gmail.com, lmaz@163.com

Abstract. As a distributed computing framework, MapReduce partially overcomes centralized system's limitations about computation and storage. However, for matrix computation, there is a paradox between distributed data storage and intensive-coupled computing. To solve this problem, new approaches for matrix transposition and multiplication with MapReduce were brought forward. By applying a new model based on parallel matrix computing methods, the bottleneck of computing for logistic regression algorithm was overcome successfully. Experimental results proved that the new computing model can achieve nearly linear speedup.

Keywords: logistic regression, matrix computing, Hadoop, MapReduce.

1   Introduction

At present time, computing performance of traditional machine learning methods needs to be improved in massive data mining in the zone of aerospace, biomedical science, Cyberspace, etc. Although computer's hardware technology has been developing rapidly, one desktop still does not meet the need to process very huge information. Parallel computing and distributed computing who utilize multiple processors or a batch of computers to compute simultaneously is a cheap and effective solution to adapt such information processing requirement. In this area, MapReduce is a promising model for scalable performance on shared-memory systems with simple parallel code[1] which is initially proposed by Google. Many algorithms have been implemented successfully with the MapReduce framework such as Genetic Algorithm[2], Particle Swarm Optimization[3] etc. Sameer Singh and Jeremy Kubica[4] presented a parallelized algorithm for feature evaluation that is based on the MapReduce framework when they examine the problem of efficient feature evaluation for logistic regression on very large data sets. The new algorithm is scalable by parallelizing simultaneously over both features and records. Tamer Elsayed, Jimmy Lin and Douglas W. Oard[5] presented a MapReduce algorithm for computing pairwise document similarity in large document collections. They derived an analytical model of the algorithm's complexity and provide an example of a programming paradigm that is useful for abroad range of text analysis problems.

In this paper, we aim to investigate how to improve the computing performance of Logistic Regression algorithm, which is a classic regression analysis algorithm widely

used in many commercial statistical systems, on a distributed computing platform based on Map/Reduce framework. The key issues mainly are to solve the computation bottleneck of regression coefficients and correspondence statistics which are related to complicated matrix computation when matrix grows very large. There are various distributed computing platforms and parallel programming paradigm available such as CloudBLAST[6], Kahn[7] process networks, etc. We finally chose the open-source platform Hadoop as our distributed computing platform. The Hadoop platform has its own distributed file system-HDFS and distributed computing framework MapReduce. Based on this platform, we can make the program execute in parallel mode by breaking a big problem into many small problems, which could be handled in parallel by the platform, thus improve the speed of computing.

2　Matrix Computation Process with MapReduce

The transposition of a matrix $A_{m \times n}$ is to form a new matrix $A^T_{m \times n}$ by exchanging rows and columns. We propose a solution to process the matrix transposition as a MapReduce job. Firstly, store the large-scale matrix which needs to calculate in a text file as the input of the Map function. The mapper reads the matrix from the file, takes the line number as the input key and corresponding elements of this line as the value. Each term in the index is associated with the i-th row, the j-th column and corresponding element. The mapper, for each element in the matrix, emits key tuples that interchange the i-th row and the j-th column as the key and the corresponding element as the value. The MapReduce runtime automatically handles the grouping of these tuples, then the reducer generates the pairs and then writes out to disk. An example can be illustrated as Figure 2.

Suppose a matrix $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, then $A^T = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}$.
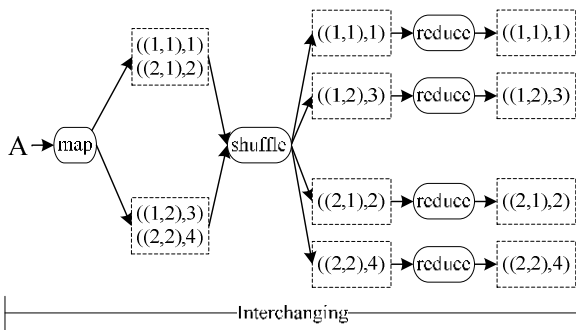

Fig. 2. Computing the transposition of a supposed matrix A

As for matrices multiplication, If there exist two matrices $A_{m \times n}$ and $B_{n \times p}$, then their matrix product AB is $m \times p$ matrix whose elements are given by the inner

product of corresponding row of $A_{m \times n}$ and the corresponding column of $B_{n \times p}$. Here, we propose an efficient solution for the matrix multiplication problem which is described as two separate MapReduce jobs (an instance illustrated in Figure 3). Before implementing the multiplication, we needs to transpose the matrix $A_{m \times n}$ so that it can be read by rows from the file conveniently.

(1) Indexing: Mapping over the file, the mapper, for each element in the matrix, emits the i-th row as the key, and a triple consisting of the name, the j-th column and the element as the value. The reducer transmits the intermediate key/value pairs to the next mapper without any treatment.

(2) Cross Multiplication: Multiplying the element in the matrix $A^T_{m \times n}$ and corresponding element in the $B_{n \times p}$ in intermediate value of the same key, the mapper generates key tuples with new i-th row and new j-th column, and generates the product by multiplication of values. Then reducer sums up the products.

Suppose two matrices $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, B = \begin{pmatrix} 2 & 3 \\ 4 & 5 \end{pmatrix}$

$$AB = \begin{pmatrix} 1 \\ 3 \end{pmatrix} \times \begin{pmatrix} 2 & 3 \end{pmatrix} + \begin{pmatrix} 2 \\ 4 \end{pmatrix} \times \begin{pmatrix} 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 6 & 9 \end{pmatrix} + \begin{pmatrix} 8 & 10 \\ 16 & 20 \end{pmatrix} = \begin{pmatrix} 10 & 13 \\ 22 & 29 \end{pmatrix}$$
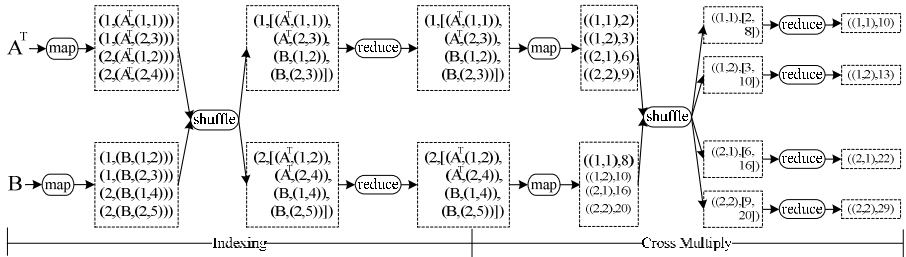

Fig. 3. Computing the multiplication of matrix A and B

3   MapReduce for Logistic Regression

In statistics, Logistic Regression is used for prediction of the probability of occurrence of an event by fitting data to a logistic curve. It is a generalized linear model for determining the relationship between predictor variables and a dichotomously coded dependent variable. The common method of fitting logistic regression models, namely maximum likelihood method, has good optimality properties in ideal settings, but is extremely sensitive to bad data[8]. To calculate Regression coefficients has a better alternative through Newton-Raphson method. In the followings passage, we will give that how to calculate regression coefficients on the Hadoop platform with the Newton-Raphson method by matrix transformation.

Suppose an event, the probability of occurrence depends on a number of independent variables $(x_1, x_2, ... x_p)$,

$$P(y_i = 1) = \frac{\exp(\beta_0 + \beta_1 x_1 + ... \beta_p x_p)}{1 + \exp(\beta_0 + \beta_1 x_1 + ... \beta_p x_p)} \quad (1)$$

Then, we define that the relationship between variables and the probability of the incident is in line with multiple logistic regression. By logit transformation, logistic regression can be turned into a linear regression to estimate parameters.

$$Logit(P) = \ln[P / (1 - P)] = \beta_0 + \beta_1 x_1 + ... \beta_p x_p \quad (2)$$

We discuss in detail the simple case, namely two-class issue. It is convenient to code the two-class y_i via a 0/1. Let $P(y_i = 1) = \pi_i$, and $P(y_i = 0) = 1 - \pi_i$, the likelihood function for N observations is[9]

$$L = \prod_{i=1}^{n} \pi_i^{y_i} (1 - \pi_i)^{1 - y_i}, i = 1, 2 ... n \quad (3)$$

The log-likelihood can be written as

$$l = \sum_{i=1}^{n} [y_i \log(\frac{\pi_i}{1 - \pi_i})] + \sum_{i=1}^{n} \log(1 - \pi_i) \quad (4)$$

$$l(\beta) = \sum_{i=1}^{n} [y_i \beta^T x_i - \log(1 + e^{\beta^T x_i})] \quad (5)$$

Where $\beta = (\beta_0, \beta_1, \beta_2 ...)$. We assume that the vector of inputs x_i includes the constant term 1 to accommodate the intercept. To maximize the log-likelihood, we set its derivatives to zero. These score equations are

$$p(x_i; \beta) = \frac{e^{\beta^T x_i}}{1 + e^{\beta^T x_i}} \quad (6)$$

$$\frac{\partial l(\beta)}{\partial \beta} = \sum_{i=1}^{n} x_i (y_i - p(x_i; \beta)) = 0 \quad (7)$$

There are $p + 1$ nonlinear equations within equation (7) since β is a $p + 1$ vector. As the first component of x_i is 1, the first score equation specifies that

$$\sum_{i=1}^{n} y_i = \sum_{i=1}^{n} p(x_i; \beta) \quad (8)$$

To solve the score equations, we use the Newton-Raphson method, which requires the second-derivative or Hessian matrix

$$\frac{\partial^2 l(\beta)}{\partial \beta \partial \beta^T} = -\sum_{i=1}^{n} x_i x_i^T p(x_i; \beta)(1 - p(x_i; \beta)) \tag{9}$$

Started with β^{old}, a single Newton update is

$$\beta^{new} = \beta^{old} - \left(\frac{\partial^2 l(\beta)}{\partial \beta \partial \beta^T}\right)^{-1} \frac{\partial l(\beta)}{\partial \beta} \tag{10}$$

Where the derivatives are evaluated by β^{old}.

Let y denote the vector of y_i values, X the $N \times (p+1)$ matrix of x_i values, p the vector of fitted probabilities with ith element $p(x_i; \beta^{old})$ and W a $N \times N$ diagonal matrix of weights with ith diagonal element $p(x_i; \beta^{old})(1 - p(x_i; \beta^{old}))$. Then we have

$$\frac{\partial l(\beta)}{\partial \beta} = X^T(y - p) \tag{11}$$

$$\frac{\partial^2 l(\beta)}{\partial \beta \partial \beta^T} = -X^T W X \tag{12}$$

The Newton step is thus

$$\beta^{new} = \beta^{old} + (X^T W X)^{-1} X^T(y - p) \tag{13}$$

It seems that $\beta = 0$ is a good starting value for the iterative procedure, although convergence is never guaranteed. Typically the algorithm does converge, since the log-likelihood is concave, but over-fitting may occur.

So the solving process turns out to be the matrix computation: $X^T W X$ and $X^T(y - p)$. The column vector $(y - p)$ can be seen as a $N \times 1$ matrix. When the dataset is very large, computing large-scale matrix will be nearly impossible. Therefore, we deploy the computing procedure on Hadoop platform to solve the problem through Map/Reduce framework proposed in Section 2.

At the Map phase, the platform estimate the memory and other resources consumption, specified each DataNode the number of mapper which can be initialized. At first, the mapper read the large sample file by line number, take the line number as the input key and corresponding elements of this line as the value. The next step is to calculate the gradient vector $X^T(y - p)$ and the negative Hessian matrix $X^T W X$ with elements of each line, where the last element of this line is just

dependent variable y_i; the rest is independent variables x_i. Mapping over the file, the mapper, for each line, emits the constant term C as the key, and a tuple consisting of the gradient vector and the negative Hessian matrix as the value, then output the intermediate key/value pairs to the reduce phase. The process will continue until all map tasks are completed. Finally, the reducer sums up all the values to perform the update for β in accordance with the Newton step expressed in Equation 13.Thus the MapReduce jobs process iteratively until the algorithm result is convergent (illustrated in Figure 4).
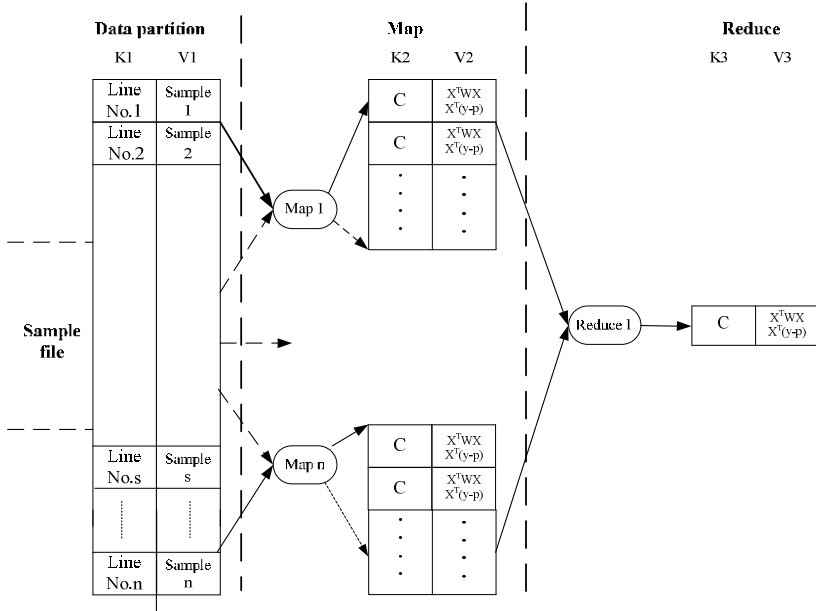

Fig. 4. MapReduce model for Logistic Regression

4 Experiment Results and Analysis

In our experiments, we use Hadoop version 0.20.0, an open-source Java implementation of MapReduce, running on a cluster with 9 machines (1 master, 8 slaves). Each machine has an INTEL Dual-core 2.6GHz processor, 4GB memory, 300GB disk, and Red Hat Enterprise Linux 5 operating system. The KDD Cup 1999 data set is used as the experimental sample set. It contains more than 4 million lines of data records about computer network intrusion detection. Each record contains 42 attribute fields. We just utilize 38 attribute fields with double type. In the data partitioning phase illustrated in Figure 4, we partition samples into groups according to two basic principles i.e., assigned mapper numbers should be the integral multiple number of machine nodes and partitioned task is equal to each other such that all processors fulfill task at the same time. That means the most proportion of run-time

should be spent in the computation process, rather than frequently initialize the mapper. Thus the total run-time will be the least. As the paper mainly compare the run-time between stand-alone and Hadoop platform, so we just ensure the calculated result is sound but not to discuss the accuracy and recall ratio. The data set are sampled into subsets of 10, 20, 30, 40……100 percent. The DataNode number is divided into 2,4,6,8 nodes. The maximum iterating times of MapReduce jobs is 5. The convergence factor of algorithm is 0.001. In order to compare the performance, when DataNode number and data set is fixed, we define the average time T_a as running time of the Hadoop platform at current DataNodes and data set, T_s as the stand-alone and Speedup T_s / T_a as an important criterion to measure our algorithm's superiority.

As the calculation process is based on each line of the sample file, it is equivalent to assign the calculation on N nodes, so that the speedup should be the number of DataNode N in theory. In the ideal case, speedup should be linearly related to the number. From the Figure 5 we can see that with the increase in the DataNodes, the speedup increase almost linearly when processing the data set in 10 percent and in 100 percent.
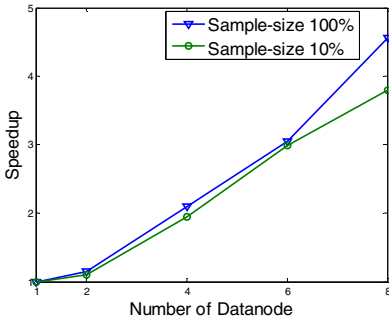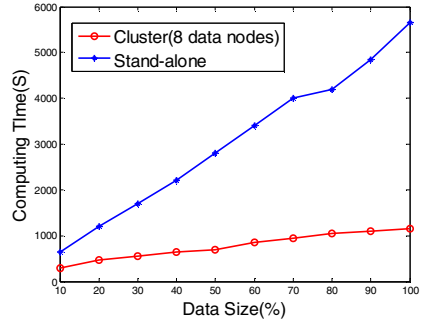

Fig. 5. Speedup of new model

Fig. 6. Running time for subsets of KDD Cup 1999 data set

Figure 6 shows the running time of the parameter estimation for different dataset sizes while the experiments are performed both on stand-alone and on 8-DataNode Hadoop platform. Empirically, no matter on which testing platform, we find that running time increases linearly with the data size, which is an approximate property, but the run-time is increasing much slower on cluster than on stand-alone. When the data size reachs 100 percent, the run-time of cluster is nearly one sixth of stand-alone's.

5   Summary

In this paper, we mainly presented two MapReduce methods for computing large-scale matrix transposition and matrix multiplication and solved the regression

parameters of logistic regression on large data sets by applying new matrix computation methods into a distributed computing model. Experimental result shows that our algorithm performs very well on the Hadoop platform. In addition, our work provides a useful programming paradigm for massive matrix operation to solve common statistical analysis issues. In the near future, we consider to keep proposing more parallel matrix computing methods with MapReduce framework, such as inversing a matrix and computing a matrix's eigenvalues and eigenvectors, etc.

References

1. Cheng, T.C., Sang, K.K., Lin, Y.A., Yu, Y.Y., Bradski, G., Andrew, Y.N., Olukotun, K.: Map-Reduce for Machine Learning on Multicore. In: Neural Information Processing Systems Conference, pp. 281–288 (2006)
2. Chao, J., Vecchiola, C., Buyya, R.: MRPGA: An Extension of MapReduce for Parallelizing Genetic Algorithms. In: IEEE Fourth International Conference on eScience, pp. 214–221. IEEE Press, New York (2008)
3. McNabb, A.W., Monson, C.K.,, Seppi, K.D.: Parallel PSO using MapReduce. In: IEEE Congress on Evolutionary Computation, pp. 7–14. IEEE Press, New York (2007)
4. Singh, S., Kubica, J., Larsen, S., Sorokina, D.: Parallel Large Scale Feature Selection for Logistic Regression. In: 9th SIAM International Conference on Data Mining, pp. 1165–1176. SIAM Press, Philadelphia (2009)
5. Elsayed, T., Lin, J., Douglas, W.O.: Pairwise Document Similarity in Large Collections with MapReduce. In: 32nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval, pp. 155–162. ACM Press, New York (2009)
6. Matsunaga, A., Tsugawa, M., Fortes, J.: CloudBLAST: Combining MapReduce and Virtualization on Distributed Resources for Bioinformatics Applications. In: IEEE Fourth International Conference on eScience, pp. 222–229. IEEE Press, New York (2008)
7. Vrba, Z., Halvorsen, P., Griwodz, C., Beskow, P.: Kahn Process Networks are a Flexible Alternative to MapReduce. In: 11th IEEE International Conference on High Performance Computing and Communications, pp. 154–162. IEEE Press, New York (2009)
8. Pregibon, D.: Logistic Regression Diagnostics. The Annals of Statistics 9, 705–724 (1981); IMS Production, Philadelphia
9. Friedman, J., Hastie, T., Tibshirani, R.: The Elements of Statistical Learning- Data Mining, Inference and Prediction. Springer, Heidelberg (2009)

Web Service Response Time Monitoring: Architecture and Validation

Sara Abbaspour Asadollah and Thiam Kian Chiew

Department of Software Engineering, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
spour@siswa.um.edu.my, tkchiew@um.edu.my

Abstract. Web services are used in many Web applications in order to save time and cost during software development process. To peruse Web service response time, a suitable tool is needed to automate the measurement of the response time. However, not many suitable tools are available for automatic measurement of response time. This research is carried out in the context of quality of Web services in order to measure and visualize Web service response time. The method proposed in this research for accomplishing this goal is based on creating a proxy for connecting to the required Web service, and then calculating the Web services response time via the proxy. A software tool is designed based on the proposed method in order to guide the implementation that is still in progress. The tool can be validated through empirical validation using three test cases for three different Web service access situations.

Keywords: Web Service, Web method, performance, response time.

1 Introduction

Nowadays, the Internet is an important phenomenon in human life and the number of its users is growing fast. It supports human interactions and connections with information and data in textual and graphical styles. It provides many services for its users. Web services are one of the recent important innovations in software that bring many consequences in software design and implementation. Web services are used in many Web applications that provide services such as searching and buying goods with the best quality and price, booking and coordinating plane tickets or hotel rooms, reading online newspapers and books, transferring files, and many more. The services are provided through Web sites and Web services. However, since quality is becoming an important issue in software, the Web sites and Web services should be monitored in order to provide high-quality services.

Monitoring is defined as the process of data extraction during program execution [1]. There are a number of tools for monitoring Web sites and Web services; some of them monitor hardware, others monitor software, and there are some tools that monitor both hardware and software (hybrid monitors) [2]. Monitoring Web sites and Web services enables users and developers to identify their features in order to compare them and select the best ones to use. Moreover, after monitoring, users can also recognize the current and potential problems of Web sites and Web services.

Then, these users will be able to solve/avoid these problems in order to produce higher-performance applications and reduce weaknesses of their products.

Measuring response time of Web services facilitates finding and correcting the cardinal and fundamental problems that affect response time. The ability to rectify problems quickly and improve Web services response time encourages Web developer to use these Web services. Monitoring Web service response time helps users to select better Web services in times of their response time.

2   Background

The Internet is an important and huge source of information that affects human lives. Different types of information on the Internet such as text, graphics, images and multimedia increase the attention of different kinds of users in order to work with the Internet. Such information is usually stored on servers. Software developers develop Web applications and Web services for users to access this information.

Web services and Web applications have similarities and differences between each other. Web applications are designed for browsers (standalone applications) while Web services are designed to be (re)used applications. Since Web services are always used by other applications, they do not need to have user interfaces [3]-[4]. As a result, when a Web application is designed to use a Web service to fulfill some of its functionalities, the Web application response time will be dependent on the Web service response time.

Response time of a Web service is defined as the sum of transmission time and processing time. Processing time is measured as the time for processing a request. In the context of Simple Object Access Protocol (SOAP), processing time is the period from the point where a SOAP message arrives at the engine, until a corresponding SOAP response message is sent using a reply activity [5]. Meanwhile, Transmission time is the time from when client sends the request until server receives it, plus the time from when the server sends the response until client receives it. As a result, response time is the time needed to process a query, from the moment of sending a request until receiving the response [6].

The performance of a Web service is considered as an important issue for its users [7]. If a user feels that the performance of the service he/she uses is poor (like long response time), then he/she will try to find another service with better performance. Since Web service monitoring, calculates the response time and analyzes its results, then users will be able to make suitable decisions about choosing the best Web service that conforms to their requirements.

One way to prove the abilities of Web services is using the tools for checking their performance, especially response time. This research presents a method to measure Web service response time, and a designed tool based on the presented method. This tool is useful for Web service providers to prove the ability and the performance (short response time) of their services to their existing customers, and encourage them to use or continue using these Web services. The tool will also enable potential customers (usually Web application designers) to select and use suitable Web service. Another benefit of the tool is that it facilitates testing Web services after they are implemented. It is useful for Web service designers, developers, and testers to find out the response time of the Web service in order to identify critical performance points.

3   Related Work

Usually, Web users measure the performance of Web applications with respect to time (Response time). As mentioned above, one aspect affecting the response time of Web applications is the response time of the Web services used in these Web applications. Thus, the response time of Web services needs to be measured and monitored.

Response time for the Web service is "*the time needed, to process a query from sending the request until receiving the response*" [7]. Repp et al. divided the Web service response time into three parts, which are network transport time, task time, and stack time. By this definition, Repp et al. (2007) defined the Web service response time as follows:

$$T_{response}(WS) = T_{task}(WS) + T_{stack}(WS) + T_{transport}(WS) \qquad (1)$$

Where:

- T_{task} is the time for processing the request (message) in both end-points and intermediate systems. It is the largest part of the response time.
- T_{stack} is "*the time from traversing the protocol stacks of source destination and intermediate system*".
- $T_{transport}$ is the network transport time.

Another method for measuring Web service response time is provided by Cardoso et al. (2004). He defined the task response time (T_{task}) as the time that an instance (object created at runtime) takes to be processed by a task, composed of two major components, which are delay time (DT) and process time (PT).

$$T_{task} = \text{Delay } T_{task} + \text{Processing } T_{task} \rightarrow T_{task} = DT_{task} + PT_{task} \qquad (2)$$

Where:

- DT is the non-value added time taken for processing an instance by a task.
- PT is the time that it takes for processing a workflow instance in a task. In other words, it is the whole time that a task needs to process an instance. DT consists of queuing delay time (QDT), and task setup delay time (SDT).

$$DT_{task} = QDT_{task} + SDT_{task} \qquad (3)$$

Where:

- QDT is the waiting time for an instance in queue until its processing starts. There are different methods to put a task in a queue on the server side, such as First In First Out (FIFO) and Server In Random Order (SIRO). The reason for engendering queue on the server is that a number of requests that arrive from the clients could be huge, and the server needs to process and respond to all of them. Therefore, the server places these requests into a queue and processes them accordingly.
- SDT is the waiting time for an instance until the task related to this instance setup on the server completely and instance processing starts.

As mentioned above, $T_{transport}$ (network time) is another factor that is considered in calculating the response time. Cahoon et al. (2000) presented the transport time as the amount of time that a message spends on the network. Thus, it can be calculated based on the message size and the network bandwidth by using the following formula:

$$T_{transport} = Size \times (8 / Speed) \tag{4}$$

Where:

- *Size* is the number of bytes in the message.
- *Speed* is the bandwidth of network in bits per second.

4   Monitoring Web Service Response Time

The proposed method for measuring and monitoring the response time for a Web service consists of two stages: running Web services, and monitoring the response time for each Web service.

The first stage of this method is accomplished through running Web methods of Web services. This task needs four inputs: Web service address, Web method name, time duration for running the Web method, and the number of calls for running the Web method of that Web service. After setting these inputs, a set of parameters is needed to call the Web method. Then, a factory creates suitable value for each parameter of the Web method to be passed for calling the Web method. Once these values are defined, a request is sent to the Web service in order to run its Web method. Before sending the request, the current date and time are saved, and after receiving the response from Web service, the date and time are saved again. The response time of the Web method is calculated by subtracting the *sending request time* from the *receiving response time*. Finally, the values such as *Web service name*, *Web method name*, *request date*, *request time*, *response date,* and *response time* are recorded. This process is repeated according to the running duration defined earlier in order to create more records to be used in the second stage of the method.

The second stage of this method aims to monitor the response time of the Web service. This is fulfilled by using the recorded data from the first stage. The input values for this part are Web Service name, Web method name, and monitoring time interval, i.e. the starting and ending date and time for monitoring. Then, all records belonging to that Web method are selected and filtered according to the inputs. These records represent the response times of the monitored Web method.

In order to apply this method, a software tool is proposed. This tool is designed based on the proposed method. Fig. 1 shows the architecture of the proposed tool.

In this architecture, the client and server are connected via network and they communicate with each other using Hyper Text Transfer Protocol (HTTP). HTTP transaction consists of two sections: a request from a client to a server, and a response from the server to the client [10].

In this architecture, UI calls a method of a Web service, and then the proxy serializes the parameters of the method to the .Net framework. After that, .Net framework sends them by a SOAP message to HTTP through the Internet. The Web service returns the result of calling the method. This response is serialized into a SOAP message and is passed through IP, TCP, HTTP, and .Net framework. Finally, the proxy diserializes the response and returns the value to the UI.

Using this architecture, two main functionalities can be achieved, (4.1) setting and running a Web service, and (4.2) monitoring and generating reports.

4.1 Setting and Running a Web Service

Calculating and recording the Web service response time is accomplished by setting, then running a Web service module. This module can be decomposed into three sub-modules. A sub-module for parsing the description document of a Web service (WSDL) is needed. It shall extract the useful information from the document in order to use this information for calling the desired Web method of any Web service. The second sub-module is needed to invoke a desired Web method of a Web service. Finally, another sub-module is needed for recording the obtained information to be analyzed during the monitoring process.

4.2 Monitoring and Generating Reports

This module shall be used for reporting the measured values of Web service response time. It is composed of two sub-modules, one for loading the saved data from the data storage, and another one for generating useful reports to monitor the desired Web service.

5 Method and Technique Validation

The validation of this research can be done via three test cases and two test Web services. After implementing a software tool based on the proposed method, the tool can be validated via these test cases and Web services by calculating the response time manually and automatically. One of these Web services will be used for finding the response time of its Web methods manually (manual testing), and the other one for automatic testing. The manual response time measurement will be done by the user while the automatic response time calculation will be accomplished via the proposed tool. Test cases were designed in order to test the three parts of response time (processing time, transporting time and queuing time).

The purpose of the first test case is measuring the processing time. For the first Web service (manual testing), there will be some code added to its Web methods for measuring the processing time of each Web methods in order to compare its results with the ones that will be obtained from the proposed tool during automatic testing. If these two sets of results are similar to each other, then it proves that the proposed tool for measuring the processing time works correctly.

The second test case will measure the processing time and transporting time together by uploading the test Web services on another system that is accessible from the user system. Then, the processing time and transporting time will be measured for the test Web services both manually and automatically. The result of manual testing and automatic testing will be compared together to check the accuracy of the proposed tool.
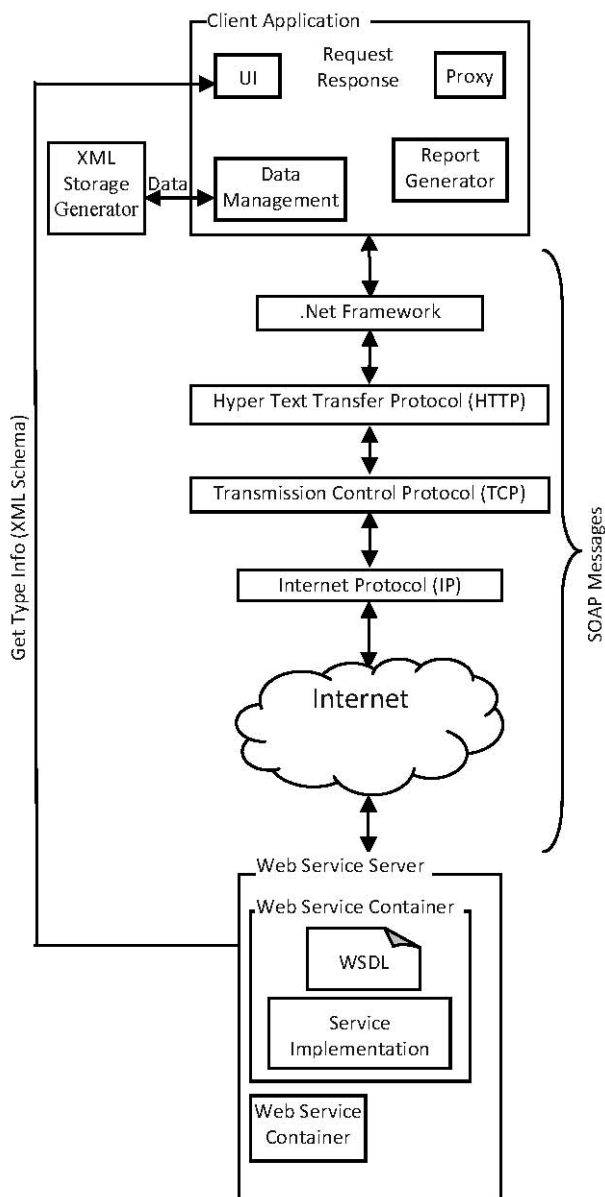
Fig. 1. Architecture of the designed tool for monitoring Web service response time

Finally, for the last test case, two users will call a Web method of the Web service at the same time. This technique will cause queuing time for the Web services. After running each test case, the obtained results of the manual testing and automatic testing will be compared with each other to validate the proposed tool.

6   Conclusion and Work in Progress

Web services are required by other applications in order to fulfill some of the functionalities of the Web applications. Measuring and monitoring the response time of Web services are important since users look for Web services with high quality performance, especially the Web services with short response time. One way to prove the abilities of Web services is using the tools for checking their performance, particularly response time. This paper presented a method and proposed an architecture for a tool to measure and monitor the response time of Web services. This tool is useful for Web service designers, developers, and testers to find out the response time of the Web service in order to identify critical performance points. Moreover, it enables the Web service providers to prove the ability and the performance (short response time) of their services to their existing customers, and encourage them to continue using these Web services. This tool will also enable potential customers (usually Web application designers) to select and use suitable Web services. The next step of this research is to implement and test the designed tool.

References

1. Chiew, T.K.: Web page performance analysis, PhD thesis, University of Glasgow (2009)
2. Haban, D., Wybranietz, D.: A Hybrid Monitor for Behavior and Performance Analysis of Distributed Systems (PDF). IEEE Transactions on Software Engineering 16, 197–211 (1990)
3. Killea, P.: Web Performance Tuning. O'Reilly, Sebastopol (1998)
4. Alonso, G., Casati, F., Kuno, H., Machiraju, V.: Web services: concepts architectures and applications. Springer, Heidelberg (2004)
5. Pautasso, C.: Emerging Web Services Technology: Wewst 2007, Halle (Saale), Germany. Birkhauser, Basel (2008); Selected Revised Papers
6. Pautasso, C., Bussler, C.: Emerging Web Services Technology. Springer-Verlag New York Inc., Secaucus (2007)
7. Repp, N., Berbner, R., Heckmann, O., Steinmetz, R.: A cross-layer approach to performance monitoring of web services. In: Proceedings of the Workshop on Emerging Web Services Technology (2007)
8. Cardoso, J., Sheth, A., Miller, J., Arnold, J., Kochut, K.: Quality of service for workflows and web service processes. Web Semantics: Science, Services and Agents on the World Wide Web 1, 281–308 (2004)
9. Cahoon, B., McKinley, K.S., Lu, Z.: Evaluating the performance of distributed architectures for information retrieval using a variety of workloads. ACM Transactions on Information Systems (TOIS) 18, 1–43 (2000)
10. Grove, R.F.: Web-Based Application Development. Jones & Bartlett Pub., USA (2009)

A Simulating Model of NGN Based on CPN Tools

Yiqin Lu, Fang Fang, and Runqing Quan

School of Electronic and Information Engineering
South China University of Technology, Guangzhou, China
`ncdirector@scut.edu.cn`

Abstract. The next generation network (NGN) is the mainstream framework of the existing telecomm networks. NGN is a service-driven network. To simulate its service-supporting environment, an service-oriented simulating model is presented based on CPN Tools, the modeling, analyzing, simulating platform of colored Petri net (CPN). The model employs the hierarchical feature of CPN and the skeleton of object-oriented CPN. To reflect the transitional characteristic of the existing network, it contains the fields of intelligent networks and NGN, which are connected with NGW. The main kinds of functional entities of the two fields are modeled as pages representing objects, while the protocols as the messages between the objects. The model can be used for studying the service creation, running and interaction in the existing telecom networks.

Keywords: NGN, softswitch, intelligent network, colored Petri net, CPN Tools.

1   Introduction

NGN (the next generation network) is the emerging telecom network, in which the core transport network is an IP network, and the functionalities of transport, control and service separated from each other. Therefore the service design can be done by the third-party, who need not know much about the technical details of a telecomm network [1-3]. Up to now, the core networks of the telecom operators are all IP transport network based on softswitch or MSC (mobile switch centers) Server. For example, Guangdong Telecom Co. Ltd. had finished the intelligent reform of backbone network in 2006. An IP-based transport network from tandem layer had been built. Softswitches and SHLRs (smart home location registers) are added in the control layer, while ASs (application servers) are used in service layer. Therefore, a NGN-based framework is constructed. Some existing services are moved to the new framework, and all the new value-added services will be developed on it [1].

NGN is a service-driven network. To study the creation, running, testing of service in a NGN, a simulating model of NGN is proposed based on CPN Tools. Developed in Danmark University, CPN Tools is a platform of modeling, analysis and simulation of Colored Petri net [4-7]. In the model, the main functional entities of NGN are abstracted and the modular design is finished, so that a supporting environment of NGN services are constructed, where the creation, running, testing, simulation and interaction detection of service can be studied [8-14].

2   NGN and CPN Tools

2.1 NGN

The NGN network is based on a 4-layer architecture, namely Access, Transport, Control, Service [1]. In access layer, the existing telecom networks or user terminals can be connected to the network through different kinds of gateway, such as signaling gateway (SG), trunk gateway (TG), network access server (NAS), and access gateway (AG), etc. The core transport network is an IP data communication network, which are composed with data communication switches and router. The connection of a call or session is carried out by softswitches (SSs) or MSC Servers in the control layer. The services are running in application servers (ASs) in the service layer. Besides the AS, there may be many other servers in the service layer, such as AAA server, network management server (NMS), etc. Standard protocol and application programming interface (API) are provided to the third-party for the service developing, which brings an open service supporting environment.

2.2 CPN Tools

CPN Tools [4] are a set of software tools for the modeling, simulating and analysis of CPN [5,6]. It provides an edition platform for construction of CPN. Where, a CPN can be created and modified. There are facilities for syntax checking and state space analysis of a created CPN. Besides, CPN can be simulated with given initiate marking. The official web pages of CPN Tools can be found in [4].

3   The Overall Frame of the Model

The overall structure of the model is shown in Fig. 1. The followings describe the main features of the frame.

- *Multiple Layered Structure.* CPN Tools support the hierachical feature of CPN by utilizing substitution transitions [4]. In an intricate net, to simplify the graphical expression, a piece of net structure can be represented by a single transition in the upper layer, which is called 'substitution transition'. Therefore, a complicated system can be modeled in a modular way. The top page of NGN is showed in Fig.1.

- *Object-oriented (OO) Modeling.* Object-orientation is a popular technology for structuring specification, modeling, analysis of a large system. A kind of CPN called the object-oriented CPN (OOCPN) uses the method of OO modeling to construct a CPN [7]. According to object-orientation, an object encapsulates its state and behavior. The state of an object's state can only be changed by sending a message to invoke one of its methods (services). In an OOCPN, an object is a marked net page, variables are transformed to places, and methods to transitions. The object receives and sends messages using the two places: in_pool and out_pool. In our model, a functional entity or a feature can be encapsulated as an object, and the signalings between two entities, or the signalings between an entity and a feature can be specified as the messages transporting between two objects.

- *The Abstraction of the Functional Entities*. With the multiple layer structure and the OO modeling method, the functional entities of a NGN can be modeled as a page, representing an object. However, in an upper layer, it is abstracted as a substitution transition. Therefore, a concise view of the whole network can be gotten (Fig.1).
- *The Combination of NGN and PSTN*. The existing telecom network is a combination of NGNs and intelligent networks (INs), which are based on PSTN (public switch telephone network) or PLMN (public land mobile network). The two networks are connected by NWG (network gateway). To reflect the fact of the existing telecom network, the model includes two fields. One is the field of IN, another is the field of NGN. The functional entities in the field of NGN include ASs, SSs, routers, and SIP (session initiation protocol) terminals, etc. while those in the field of IN include service control points (SCPs), service switch points (SSPs), intelligent peripherals (IPs), tandem switches (MSs), local switches (LSs), gateway switches (GWs), MSC Servers, and SHLRs, etc. The whole structure of the existing network can be model as the top page of the model, which is shown in Fig.1.
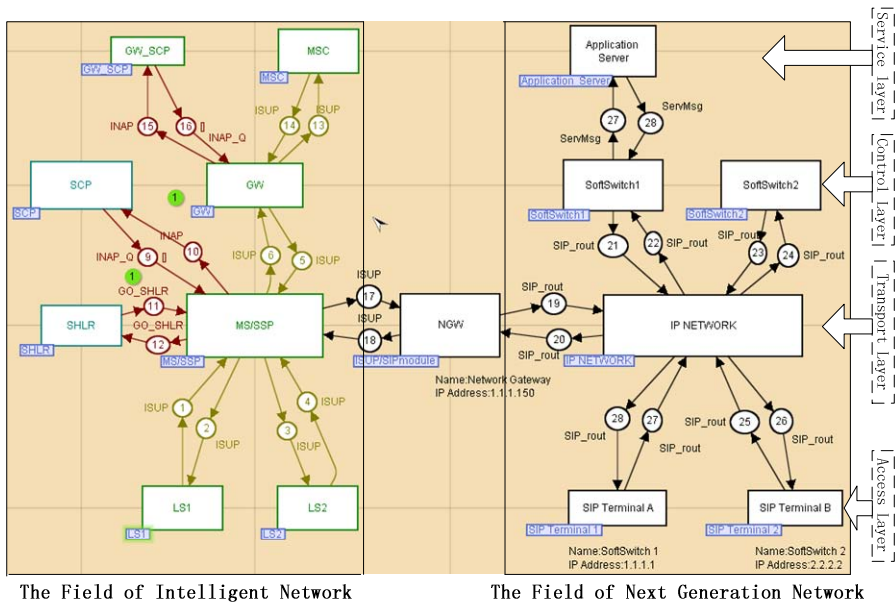

Fig. 1. The top page in the CPN model of NGN

- *Feature Integration*. A feature is treated as an object and specified as a page. When the feature is integrated into the network. The page is added into the model by inserted a substitution transition in the page of AS.

4   NGW

NGW is the bridge between an IN and a NGN. The functionality of NGW concerned in the paper is the translation between the signalings in the IN field and in the NGN field. As shown in Fig.2, there are two modules in the page of NGW, which are named SIP2ISUP and ISUP2SIP.

A SIP2ISUP module translates a SIP message in the NGN field into ISUP signaling in the IN filed, while the ISUP2SIP module forms a SIP message from the ISUP signaling.
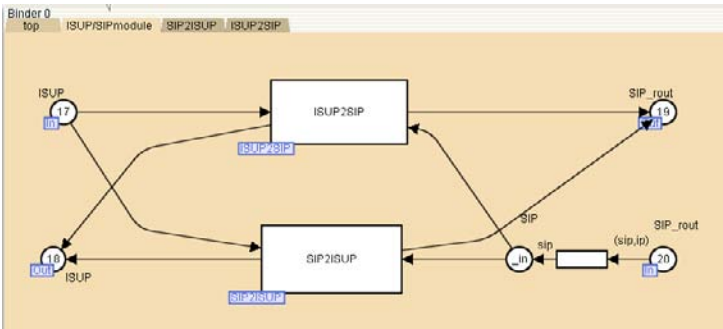

Fig. 2. The CPN model of a NGW

5   The Field of Intelligent Network

Intelligent network provides a service supporting environment based on framework of the PSTN or PLMN. It supports the protocol of INAP (intelligent network application part). Most of the existing INs are in the stages of CS-1 (capability set one), some of them are in the stage of CS-2 (capability set two). The followings are the main functional entities of the model [12].

- *SCP*. SCP is server where a feature runs. It communicates with SSP with INAP.
- *SSP.* In the existing network, a SSP is often a MS which supports INAP. A feature is triggered in a SSP.
- *SHLR.* A SHLR is an independent entity in a PSTN. It contains the attribute datum of the end users, which is something of the HLR (home location register) in PLMN. A SSP often obtains the service code from SHLR, which is used to invoke the service logic in SCP.
- *LS.* A LS is the access switch of the end user.
- *GW.* A GW is the exchange forwards a call across the different networks.

6   The Field of NGN

6.1   Softswitch (SS)

SS realizes the call control function, which is separated from a switch in a PSTN. The call control includes the establishment, maintain and release of a call. A SS communicates with an AS with SIP messages. A module called O_SIP is designed to handle the SIP messages from a caller and a module called T_SIP to handle the SIP messages to a callee (Fig.3).

In Fig.3, the basic call state module (BCSM) is employed, which is a concept used in an IN. In BCSM, a feature is triggered in detecting point (DP) [15].
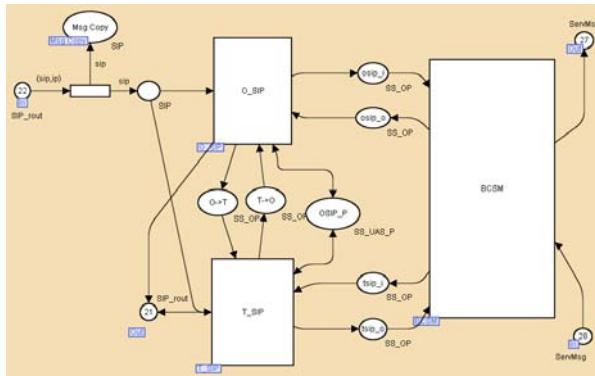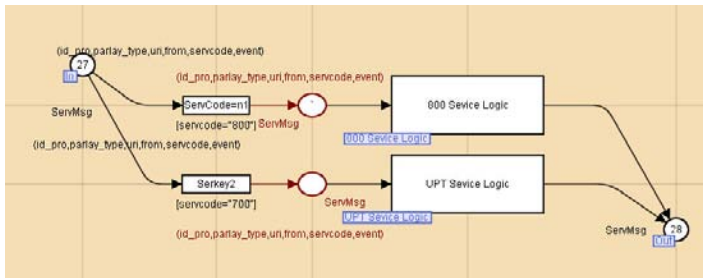

Fig. 3. The CPN model of a softswitch (SS)

Fig. 4. The CPN model of an application server (AS)

6.2   Application Server (AS)

The application server contains the service logics of different features. When a feature is triggered in SS, a SIP message is sent to the AS. According to the service code, the corresponding service logic is invoked. Fig.4 shows two features. One is 800 with the service code of 800, another is UPT (universal personal telecommunication) with the service code of 700 [16]. The service codes are expressed as a guard of the transitions.

6.3   SIP Terminal

The structure of a page of SIP terminal module is similar to that of a LS. There are two parts of the page (Fig.5). One is the module of 'Calling Party', modeling the caller role of the terminal; another is the module of 'Called Party', modeling the callee role of the terminal [17-19].
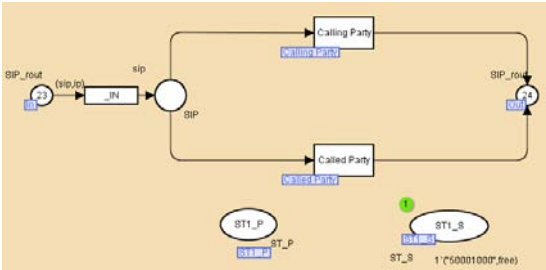

Fig. 5. The CPN model of a SIP terminal

7   Conclusions

NGN is the mainstream framework of the telecom network, though the services provided by IN may be remained in the existing telecom network. In this paper, the above characteristic of the existing telecom network structure is model based on CPN Tools. The skeleton of OOCPN is employed in using the hierarchical feature of CPN. The main kinds of functional entities of the two fields and the features are modeled as pages representing objects, while the protocols as the messages between objects. The behaviors of the network can be studied by using the simulation facility of CPN. With the model, the service creation, running and interaction in the existing telecom networks can be studied.

References

1. Lu, Y., Yue, G., Wang, J.: Detecting Intention-Violation Feature Interaction in NGN Based on Feature Re-presentation. Journal of Networks 5, 603–612 (2010)
2. Lu, Y., Yue, G., Wang, J.: An Algorithm for NGN Feature Interaction Detection. In: ISCST 2009, pp. 510–513 Huangshan (2009)
3. Lu, Y., Yang, X., Fang, F., Wang, S.: An Implementation of On-line Management of Livelock Type Feature Interaction in NGN. In: 3rd IEEE International Conference on Computer Science and Information Technology, Chengdu (2010)
4. CPN Tools for Color Petri Nets, http://cpntools.org/
5. Jensen, K.: A Brief Introduction to Colored Petri Nets,
   http://www.daimi.au.dk/~kjensen/

6. Jensen, K.: Colored Petri Nets: Basic Concept. Monographs in Theoretical Computer Science. Springer, Heidelberg (1992)

7. Buchs, D., Guelfi, N.: CO-OPN: A Concurrent Object Oriented Petri Net Approach. In: 12th International Conference on Application and Theory of Petri Nets, Gjern, Denmark, pp. 432–454. IBM Deutschland (1991)

8. Lu, Y., Cheung, T.Y.: Feature Interactions of the Livelock Type in IN: A Detailed Example. In: 7th IEEE Intelligent Network Workshop, pp. 175–184. Bordeaux (1998)

9. Lu, Y., Wei, G., He, Q.: A Temporal Colored Petri Net Model for Telecommunication Feature Integration. Journal of South China University of Technology(Natural Science Edition) 30(1), 27–33 (2002)

10. Lu, Y., Wei, G., Ouyang, J.: A colored Petri Nets Based Model of Features Integration in Telecommunications Systems. Journal of China Institute of Communications 20(6), 69–76 (1999) (in Chinese)

11. Lu, Y., Wei, G., Ouyang, J.: Detecting and Managing Feature Interactions in Telecommunications Systems by Invariant-Preserving Transformations of Colored Petri Net. Journal of China Institute of Communications 20(7), 55–58 (1999) (in Chinese)

12. Wang, J., Lu, Y., Li, W.: Telecommunication Services Modeling Based on CPN Tools and Its Application. Computer Engineering 32(14), 221–223 (2006) (in Chinese)

13. Cheung, T.-Y., Lu, Y.: Detecting and Resolving the Interaction between Telephone Features Terminating Call Screening and Call Forwarding by Colored Petri Nets. In: 1995 IEEE Int. Conf. Systems, Man and Cybernetics, pp. 2245–2250. Vancouver (1995)

14. Lu, Y., Wei, G., Cheung, T.-Y.: Managing Feature Interactions in Telecommunications Systems by Temporal Colored Petri Nets. In: ICECCS 2001, pp. 260–270. Skovde (2001)

15. Distributed Functional Plane for Intelligent Network CS-1, ITU-T Recommendation Q.1214, Geneva (1993)

16. Jackson, M., Zave, P.: Distributed Feature Composition: A Virtual Architecture for Telecommunications Services. IEEE Trans. Softw. Eng. 24, 831–847 (1998)

17. SIP Servlets Specification, `http://www.ietf.org/internet-drafts/draft-peterbauer-sip-servlet-ext-00.txt`

18. Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., Schooler, E.: IETF RFC 3261. SIP: Session Initiation Protocol, p. 8, 17–18, 26–29, 122 (2002)

19. Rosenberg, J., Schulzrinne, H., Huitema, C., Gurle, D.: IETF RFC 3428: Session Initiation Protocol (SIP) Extension for Instant Messaging (2002)

20. Blom, J., Jonsson, B., Kempe, L.: Using Temporal Logic for Modular Specification of Telephone Service, pp. 197–216. IOS Press, Amsterdam (1994)

21. Thomas, M.: Modelling and Analysing User View of Telecommunication Service, pp. 163–176. IOS Press, Montreal (1997)

Simulation Analysis for Information Resource Allocation of Express Company Based on Fractal

Ning Chen[1], Xueyan Zhang[2], and Wenrui Hao[3]

[1] School of Transportation and Logistics, Southwest Jiaotong University,
Chengdu, P.R. China 610031
Tel.: （86）13388197917
chenning@home.swjtu.edu.cn
[2] School of Transportation and Logistics, Southwest Jiaotong University,
Chengdu, P.R. China 610031
Tel.: （86）028-87602002
xyz@home.swjtu.edu.cn
[3] School of Transportation and Logistics, Southwest Jiaotong University,
Chengdu, P.R. China 610031
Tel.: （86）15198281449
420760500@qq.com

Abstract. Nowadays, logistics informationization develops by leaps and bounds. By means of Internet of Things (IOT), modern logistics industry, especially express company is able to obtain and process the information resources timely, accurately and integrally, which is becoming the key way to fulfill various business tasks to meet customers' demands. So, first of all, some important issues concerning to business flow processing for express company are presented. And then, in view of the information demands of express company, the modified Co-shared Information Resource Fractal Unit (CIRFU) and such improved model as Re-constructed Resource Optimization Allocation (RROA) are presented. Furthermore, some key problems relating to the model are analyzed. Last but not least, a case study—numerical simulation is given to explain the function of such model applied to express company.

Keywords: numerical simulation, fractal information resource allocation, express.

1 Background of Research

This paper analyzes the method of co-shared information resource allocation and its application to express company. With the rapid development of IT technologies and widespread application of Internet of Things (IOT), more and more industries wish to fulfill their business processes via Internet by virtue of useful information resource allocations. How to find and organize co-shared information resources so as to form a standard mode that is applicable to various demands, is still a tough problem to be solved (CHEN, 2010). Therefore, aiming at paving a way for efficiently allocating co-shared information resources for the special logistics enterprise—express company, firstly, some important matters relating to business

flow processing for express company are introduced. And then, a modified Co-shared Information Resource Fractal Unit (CIRFU) and corresponding model "Reconstructed Resource Optimization Allocation (RROA)" are presented. With above issues intensively analyzed, finally, a numerical simulation is given to show that the function of such model meet the demand of information resource allocation for express company.

2 Introduction to Business Flow Processing for Express Company

Investigation and study on current typical express companies show that the general characters of these enterprises are of.

- imperative to co-share business information
- business flow unitary and fixed, rarely changed
- time-saved, cost-cut

In order to analyze the demand on information resource for express company successfully, above all, the complete business flow processing should be studied and presented. In accordance with a large amount of investigative materials from various express companies, and by use of such analysis method for business flow as UML, an overall transaction flow diagram is shown in Figure 1 as below.
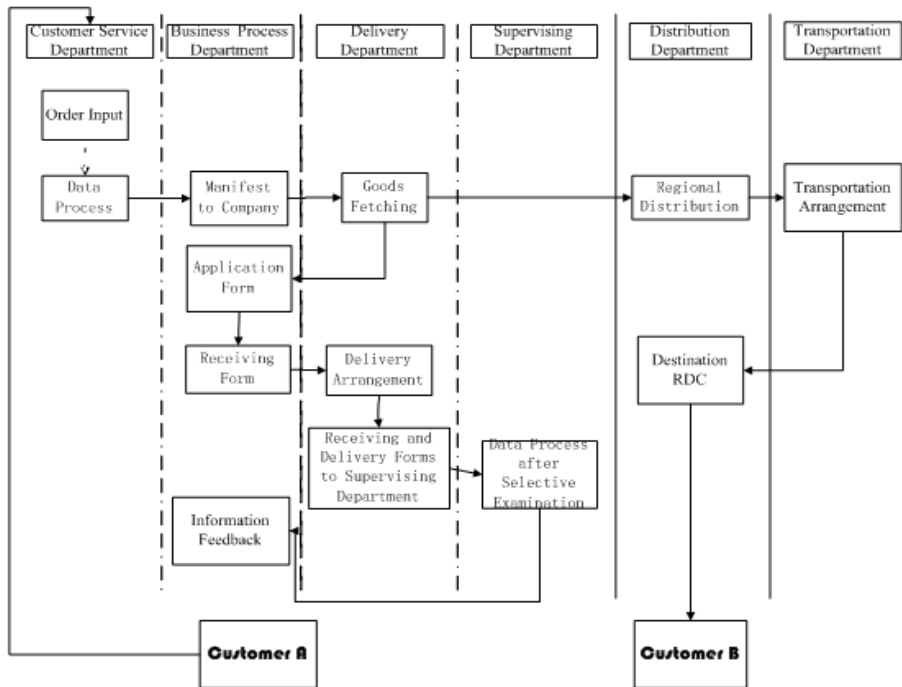

Fig. 1. Overall transaction flow diagram (TFD) of express company

From above TFD, it is apparent that no matter what step the express business is, whether information co-sharing is successfully or not to a large extent depends on the information resource rational allocation among customers, various departments of express company. For example, Customer A is able to know its business process not only by inquiring Customer Service Department but also consulting other Department such as Delivery, Distribution and Transportation Department. And Customer B is vice versa.

3   Study on Model of Modified Co-shared Information Resource Fractal Unit (CIRFU) and Improved Re-constructed Resource Optimization Allocation (RROA) for Express Company

Studies from home and broad have shown that the modes of information processing are self similar or self quasi-similar, which means that such theory as fractal, could be used to analyze these phenomena (CHEN, 2010). As the express company is characteristic of distributed information resources and time-saved, such mode should be re-constructed so as to meet the specific needs. In accordance with the modes of Co-shared Information Resource Fractal Unit (CIRFU) and Re-constructed Resource Optimization Allocation (RROA), in view the special demand of express company, CIRFU is modified to represent the information resource group unit that is able to fulfill a complete express business process, which function is self similar despite its various real construction.

As a core component for information processing and co-sharing, the modified CIRFU aims at connecting the customers, departments of express company with relevant information co-shared groups via Internet (IOT). The function of CIRFU mainly includes:

- Processing information with Cloud Group DB Center and Web DB
- Acting as a co-shared information resource provider to allocate relevant information to customers and partner departments

Despite the various forms of information presentation from distributed Database, the function of CIRFU always appears self similar. Therefore, by building a complete modified CIRTU, the demand of information co-sharing for current express company will be meet.

In compliance with the distributed environments for express business processing, when the function of CIRFU tends be self similar, the generalized entropy $H_\omega(\varepsilon)$ is inclined to a fixed value. As a matter of fact, this value is equal to the maximum value of entropy—upper limit $H(x)$, and $f(x) = B \exp\{-\lambda_1 g_1(x) - \lambda_2 g_2(x) - \cdots - \lambda_n g_n(x)\}$ (CHEN, 2010).

In view of the modified CIRFU being formed by such general characters as distributed information resources, co-sharing business information oriented, business flow unitary and fixed, and business process time-saved, the improved model of RROA is analyzed as follows.

In view of the modified CIRFU being formed by distributed information resources, co-sharing business information oriented,   business flow unitary and fixed, and business process time-saved, the improved model of RROA is analyzed as follows.

Let $\{X(t), t \geq 0\}$ be a non negative integer stochastic process. In accordance with such information resources characteristic of distributed, co-shared and time-saved, the whole information processing can be described as.

- $\{X(0), = 0\}$
- $\{X(t), t \geq 0\}$ is independent increment
- Probability $P\{X(t+h) - X(t) = 1\} = \lambda(t)h + o(h)$
- $P\{X(t+h) - X(t) \geq 2\} = o(h)$

Assume $p_n(s,t) = P\{X(s+t) - X(s) = n\}$,

$$\tilde{u}(t) = \int_0^t \lambda(s)\mathrm{d}s \qquad (3\text{-}1)$$

$$p_n(s, t+h) = P\{X(s+t+h) - X(s) = n\}, \quad h > 0$$

$$= \sum_{i=0}^n P\{X(s+t) - X(s) = i, X(s+t+h) - X(s+t) = n-i\}$$

$$= \sum_{i=0}^n p_i(s,t) p_{n-i}(s+t, h)$$

$$= p_n(s,t)[1 - h\lambda(s+t)] + p_{n-1}(s,t)\lambda(s+t)h + o(h)$$

Then, $\dfrac{p_n(s, t+h) - p_n(s,t)}{h} = -\lambda(s+t)p_n(s,t) + \lambda(s+t)p_{n-1}(s,t) + o(1)$

And when $h \to 0+0$, in view of t, $p_n(s,t)$ is partially derived as,

$$\frac{\partial}{\partial t} p_n(s,t) = -\lambda(s+t) p_n(s,t) + \lambda(s+t) p_{n-1}(s,t)$$

Consider the probability goal function of $p_n(s,t)$ based on plural number plane,

$$\tilde{M}(s,t,z) = \sum_{i=1}^{\infty} p_n(s,t) Z^n, \qquad |Z| \leq 1$$

When, $n \leq 0$, $p_n(s,t) = 0$

So, $\tilde{M}'_t(s,t,z) = -\lambda(s+t)\tilde{M}(s,t,z) + \lambda(s+t)Z\tilde{M}(s,t,z), \qquad |Z| \leq 1$

$\tilde{M}(s,t,z) = C(s,z)\exp[(\tilde{u}(s+t) - \tilde{u}(s)(Z-1)]$

$p_n(s,0) = P\{X(s+0) - X(s)\} = n\} = 0, \ n \geq 1$

So, $p_0(s,0) = 1$

Thus, $\tilde{M}(s,t,z) = 1$

Then, $C(s,z) = 1$

$\tilde{M}(s,t,z) = \exp[(\tilde{u}(s+t) - \tilde{u}(s)(Z-1)]$

$$= \sum_{n=0}^{\infty} \exp\{-[(\tilde{u}(s+t) - \tilde{u}(s)]\} \frac{[(\tilde{u}(s+t) - \tilde{u}(s)]^n z^n}{n!}$$

$$p_n(s,t) = P\{X(s+t) - X(s) = n\}$$
$$= \exp\{-[(\tilde{u}(s+t) - \tilde{u}(s)]\}\frac{[(\tilde{u}(s+t) - \tilde{u}(s)]^n}{n!}, \qquad n \geq 0 \tag{3-2}$$

When $X(t) = n$, equation (3-2) can be simplified as,

$$P\{X(t) = n\} = \frac{[-(\tilde{u}(t)]^n}{n!}\exp[-(\tilde{u}(t)] \qquad\qquad n \geq 0 \tag{3-3}$$

By virtue of equations $(3\text{-}1) \sim (3\text{-}3)$, the probability to fulfill co-shared tasks in express business process could be determined. And then, corresponding tasks mathematical expectation value is to be obtained by equation (3-4).

$$E[X(t)] = \tilde{u}(t) \qquad\qquad n \geq 0 \tag{3-4}$$

$E[X(t)]$ stands for the actual business tasks fulfilled by co-shared information resources.

Take equation (3-1) into consideration, which is of the similar form as the model of co-shared information resources allocation that is applied to dynamically organize configured information resource (CHEN, 2006).

Combing the model of co-shared information resources allocation (CHEN, 2006) and RROA (CHEN, 2010), by putting equations $(3\text{-}1) \sim (3\text{-}4)$ into practice, the mathematical model of improved Re-constructed Resource Optimization Allocation (RROA) for express company is described as equations (3-5), (3-6) as below.

$$\left[\tilde{\boldsymbol{B}}_s\right] = \begin{bmatrix} \tilde{u}_{11} & \cdots & \cdots & \tilde{u}_{1m} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{u}_{k1} & \cdots & \cdots & \tilde{u}_{km} \end{bmatrix}_{k \times m} \begin{pmatrix} 1 \leq i \leq k \\ 1 \leq j \leq m \end{pmatrix}$$

$$= \left[\tilde{\boldsymbol{B}}_s^{(1)}\right] + \cdots + \left[\tilde{\boldsymbol{B}}_s^{(i)}\right] + \cdots + \left[\tilde{\boldsymbol{B}}_s^{(k)}\right]$$

$$\tilde{\boldsymbol{d}}_s = \sum_{i=1}^{k}\tilde{\boldsymbol{d}}_{ij} \qquad \tilde{\boldsymbol{d}}_{ij} = [\tilde{\boldsymbol{B}}_S^{(i)}]\boldsymbol{e}^{(j)}$$

$$\sum_{s=1}^{t}\tilde{\boldsymbol{d}}_s = \eta\tilde{\boldsymbol{C}} \tag{3-5}$$

$$\sum_{s=1}^{t}\tilde{\boldsymbol{d}}_s^{(j)} = \eta\tilde{\boldsymbol{C}}^{(j)} \tag{3-6}$$

$$s.t. \sum_{i=1}^{t}\sum_{j=1}^{m}\left(\frac{\tilde{d}_{si}}{\tilde{d}_{si}^{(j)}}\right) \leq m$$

- m: task numbers that CIRFU should fulfill
- $\tilde{\boldsymbol{B}}_s$: dynamical co-shared information set for express company A
- $\tilde{\boldsymbol{d}}_s$: equivalent efficiency set of co-shared information for express A

- $\boldsymbol{e}$: unit vector relating to e CIRFU
- $\tilde{\lambda}$: Efficiency of CIRFU corresponding to specific task m
- $\tilde{\boldsymbol{c}}$: tasks to be fulfilled by express company A
- $\tilde{u}_m$: Equivalent efficiency of CIRFU

4 Case Study

By erecting the relevant modified Co-shared Information Resource Fractal Unit (CIRFU), and with the application of the mathematical model of improved Re-constructed Resource Optimization Allocation (RROA), the actual information resources co-sharing of express business process can be simulated and analyzed in Figure 2 and Table 1 respectively as below.
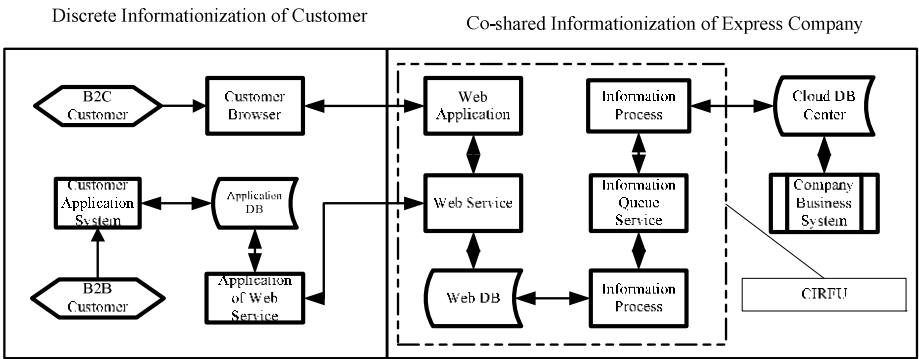

Fig. 2. Topology Structure of Co-shared Information Resource Fractal Unit for Express Company

Table 1. Comparison between Actual and Simulation by RROA

Task	Actual processing	RROA	Actual allocation of CIRFU by RROA	Error Analysis (%)
	Utilization Efficiency of Co-shared Information Resources (%)			
R_1	47.0	51.1	CIRFU co-shared in 4 tasks	8.72
R_2	29.4	30.2	CIRFU co-shared in 5 tasks	2.73
R_3	76.6	80.0	CIRFU co-shared in 4 tasks	4.44
R_4	87.3	92.1	CIRFU co-shared in 4 tasks	5.50
R_5	9.4	10.3	CIRFU co-shared in 5 tasks	9.58

In comparison with conventional method (Repoussis, 2007), above simulation results are satisfactory with the largest error value less than 10%.

5   Conclusion

Based on the systematical analysis of important issues relating to express business flow process, this paper proposes a modified Co-shared Information Resource Fractal Unit (CIRFU). More study on express business flow is given, an improved model as Re-constructed Resource Optimization Allocation (RROA) are presented. With the establishment of CIRFU, the improved RROA can be successfully applied to allocate distributed information resources efficiently and reasonably for express business process. Furthermore, the case study—numerical simulation shows that this model is able to organize and allocate co-shared information resources efficiently and reasonably.

References

1. Chen, N.: Study on Model of Co-shared Information Resource Allocation Based on Multi-fractal. In: Proceedings of the 2010 International Conference of Logistics Engineering and Management, vol. 387, pp. 3715–3721. ASCE, Chengdu (2010)
2. Chen, N.: Research on Model and Algorithm of Fractal Data Mining Based on IOT. In: Proceedings of the 2010 International Conference of Logistics Engineering and Management, vol. 387, pp. 3708–3714. ASCE, Chengdu (2010)
3. Chen, N.: Research on Model and Application of Resource Allocation in Multi-project Management Based on Stochastic Theory. J. Chinese Managemenet of Science 14, 75–80 (2006)
4. Repoussis: The open vehicle routing problem with time windows. Journal of the Operational Research Society 58, 355–367 (2007)

Optimal Replica Selection Algorithm in Data Grid

Bing Tang and Li Zhang

School of Computer Science and Engineering
Hunan University of Science and Technology, Xiangtan 411201, China
btang@hnust.edu.cn

Abstract. Data replication technique in grid reduces access latency and bandwidth consumption. When different sites hold replicas of the same data, selecting the best replica is a significant benefit. In this research, the topology of Virtual Token Ring (VTR) and the VTR-based data network are presented. Then, a replica price model and a replica selection strategy are proposed. Optimal data replica is defined as the replica with the smallest transfer cost. The Buyer and Seller algorithm based on VTR network and auction protocol are also described in detail. Performance analysis demonstrates that the proposed replica selection algorithm shows a significant performance improvement over traditional replica catalog and round-robin probing based algorithm.

Keywords: Replica Selection, Virtual Token Ring, Data Grid.

1 Introduction

In data grid, large scale geographically distributed users often require access to a large amount of data (terabytes or petabytes), and the data may be distributed on remote grid nodes. Managing this large amount of data in a centralized way is ineffective due to extensive access latency and load on the central server. One solution is to duplicate the require data to obtain several data replicas, and place them on different grid nodes.

Data replica management strategy is how to managing data replica creation, selection, location and consistency in dynamic, distributed and heterogeneous grid environment. Data replica management service is a significant benefit to data grid, for instance, it decreases data access latency, decreases network bandwidth consuming, avoids network congestion, balances grid node load, and improves data availability. In data grid environments, a replica catalog is used to register files using a logical filename. The replica catalog provides (one to many) mapping from logical file names (LFN) to physical file names (PFN) that include the storage location. The replica location service is either centralized or distributed among sites. When many sites hold the replica, in order to satisfy user's data access request, replica management service is responsible for selecting the best replica for user. An effective data replica selection strategy is important to the performance of the whole grid system.

In this research, a new data replica network and data replica selection algorithm is presented. The rest of the paper is organized as follows. Section 2 surveys the related work of data replica management and replica selection. Section 3 demonstrates VTR data network and the topology. In Section 4, replica selection strategy is introduced,

and selection algorithm as well as replica price model are presented. Performance analysis is given in Section 5. Finally, Section 6 concludes the whole paper.

2 Related Work

In 1980s', the token ring protocol was designed for data communication in local area network [1] [2]. These years, token ring network has been widely used in wireless communication field, and improved token ring protocols are also used in many engineering fields [3]. In this paper, a virtual token ring based method is presented to implement replica management and selection.

Data replica management in Grid has been an important research issue since the birth of Grid. In the early of 1990s', Globus project studied the replica management in Grid, and introduced a RMS (Replica Management Service) and Replica Catalog, and also a data transfer module called as GridFTP, and released a series of APIs for replica management [4]. The famous EU Data Grid also designed a RLS (Replica Location Service) and a LRC (Local Replica Catalog) server [5].

A data replica selection strategy is related to different engineering and application background. Different application requires different replica selection standard, and the standard may be response time, replica reliability, or access cost. Currently, the existed replica selection models include static model, round-robin probing selection model, regressive prediction model, probabilistic model, and economy based model, *etc*. In a real application, the number of replicas in a data grid is huge, and the replica always dynamically changes. Hence, it is difficult to determine the optimal replica, and it is usually a relative optimal replica.

The key in implementing replica selection is how to predict replica response time. There are two methods to predict replica response time. One is performance model based prediction, and the other is access history information based prediction.

(1) Performance model based prediction

The implement of performance model based prediction include building up a performance model, obtaining physical parameters required by performance model. The weakness of this method is that it relies on the information of an amount of physical equipments. Chang *et al*. presented a dynamic hierarchical replication strategy combined with scheduling policy to improve the data access efficiencies in a cluster grid, which considers network performance parameter [6].

(2) Access history information based prediction

This method predicts replica response time through the history study of data transfer time between requesting node and replica node. There are two keys lies on the implement of access history information based prediction, and they are gathering historical performance, and the predicting. There exists several traditional prediction approaches. For example, Vazhkudai *et al*. presented a regression model based on network traffic load and data transfer history using GridFTP middleware [7]. Rahman *et al*. proposed a replica selection strategy using the K-Nearest Neighbor rule which

also considered previous file transfer logs [8]. All these approaches collect historical records of interaction between requesting node and replica node, and predict the end-to-end performance between nodes.

3   VTR Data Network

In this paper, the token ring used in optimal replica selection algorithm is not a real token ring in computer networks, while it is a virtual ring consisted of several nodes which hold the copy of one file. In the virtual token ring, node handles token sending and token receiving, which is similar to [3].

1) Token sending and token receiving obey a harmonious rule. All the nodes in the ring have equal accessing right, and there is no conflict during token sending and token receiving.

2) There is network latency in virtual token ring, which leads to response latency to replica request from user. If the best replica node is selected, a direct connection between the best replica node and requesting node will be build.
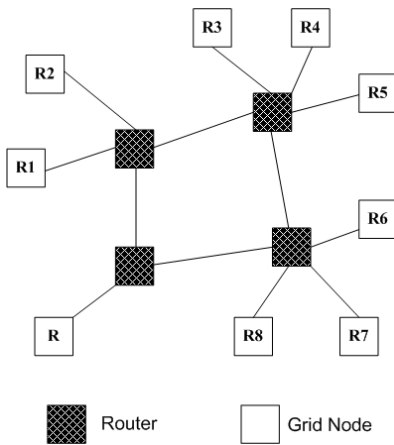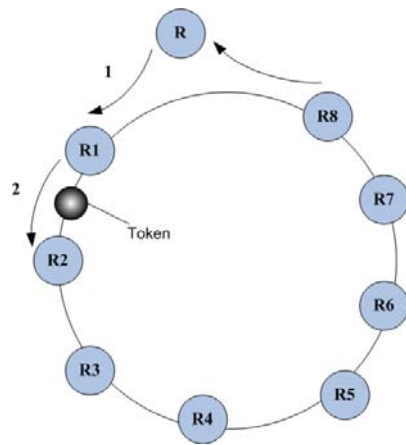

Fig. 1. Physical topology of data grid   Fig. 2. Logical topology of VTR

3.1   Virtual Token Ring

Here, we define *requesting node* as the node/site which request a data file *F*, and we also define *replica node* as the node/site which holds the replica of file *F*.

(1) Physical Topology

From the physical perspective, the traditional architecture of grid is shown in Fig. 1, and it is also called as cluster grid. A cluster represents an organization unit which is a group of sites that are geographically close. In Fig. 1, we may consider that there are four big sites, and four routers. There are 8 nodes, R1, R2, R3, R4, R5, R6, R7, and R8, which host the replica, and R is the requesting node.

(2) Logical Topology

From the logical perspective, all the replica nodes form a ring, and each node just stands for one replica. The requesting node is also recognized as one node, so there are totally N+1 nodes in the ring. Each node has a unique previous node and a unique successive node (or known as next hop node). As you see in Fig. 2, in this circle, the next hop node of R is R1, the next hop node of R1 is R2, and so on, and finally, the next hop node of R8 is R. Token moves in this ring in the way of ask and answer.

3.2   Replica Catalog

In the VTR data network showed by Fig. 2, each node is aware of its next hop node. Replication Location Service requires a server to hold the mapping between LFN and PFN, and all the replica node are registered in the Replica Catalog Server. At the same time, when a new node which holds replica joining, the Replica Catalog Server will assign a next hop node to it. The Replica Catalog Server is responsible for the new replica publishing and replica leaving, which means node joining and node leaving in the VTR network. When a new data is registered in gird, we define several data attributes for meta-data. Attributes keys include i) *replica number*, ii) *fault-tolerant flag*, iii) *data lifetime*, iv) *replica routing-table*. Routing-table indicates the previous and successive node relationship, and it is used to build the token ring network topology.

4   VTR-Based Replica Selection Algorithm

The optimal replica selection algorithm is based on VTR and auction protocol. The Buyer denotes the replica requesting site. The Seller denotes the site which holds the replica, and Seller will bid a proposal of a price, which is packed in the token, and passed to the next Seller. All the Sellers will give their own price proposal. The lower price means a lower transfer cost from Seller to Buyer. Selecting the lowest bidding Seller is just realized selecting the best replica.

The auction protocol in this paper is compatible with the token passing method. The token is a mark which contains some segments, just like a TCP packet with a variable length, but each segment of token has their meanings. The bidding proposal of price is only one segment, and other segments include the id, the command type, the source node, the next hop destination, the size, the MD5 checksum, *etc*.

Here, we also define a replica price model to estimate price proposed by different Sellers. When a Seller bid a proposal of a price, network performance and other factors borrowed from commodity business should be taken into consideration.

4.1   Algorithm Description

The core of replica selection algorithm is just data replica request algorithm, or we say token updating and passing algorithm inessential. The algorithm of Buyer and Seller based on VTR and auction protocol are described as the following **Algorithm 1** and **Algorithm 2**.

Algorithm 1. *Buyer Algorithm Based on VTR and Auction Protocol*

Require: Let the physical file name of required data to be *phy_name*
Require: Let the logical file name of required data to be *log_name*
1: {Buyer initialization and send out replica request to Replica Catalog}
2: **if** <*phy_name, log_name*>mapping *not* existed in Replica Catalog **then**
3:    report to user and exit
4: **else**
5:    get the first node in data replica router table
6:    generate *token*
7: **end if**
8: {Token Ring start}
9: set *Timer*
10: send out *token*
11: **repeat**
12:    wait for
13:    **if** timeout event is triggered **then**
14:      send out *token* again
15:    **end if**
16: **until** replica event is triggered
17: obtain the best replica node
18: build a direct connect with the best Seller

Algorithm 2. *Seller Algorithm Based on VTR and Auction Protocol*

Require: Let the successive node to be N_{sus}
Require: Let the previous node included in token to be N_{pre}
Require: Let the price included in token to be P_{token}
Require: Let the new bidding price to be P_{new}
1: **repeat**
2:    wait for
3:    send periodically heart beat signal to Replica Catalog
4:    **if** timeout event is triggered **then**
5:      send out *token* again
6:    **end if**
7: **until** *token* is received
8: {parse token}
9: **if** N_{pre} is *not* true **then**
10:    give up the *token* and wait for
11: **else**
12:    get the P_{token}
13:    compute P_{new}
14:    **if** $P_{new} < P_{token}$ **then**
15:      update *token* with P_{new}
16:    **end if**
17:    get the N_{sus} and update *token* with N_{sus}
18:    set *Timer*
19:    send out *token*
20: **end if**

4.2 Replica Price Model

A set of factors and their weightiness are considered in this paper. A replica price model to compute and estimate the proposed price by Seller is given as follow.

$$P = \lambda_1 \left(\frac{M}{N_s} + D \right) + \lambda_2 \frac{ae^L}{R} + \lambda_3 \frac{b}{CQ} \quad \lambda_1 + \lambda_2 + \lambda_3 = 1 \tag{1}$$

where that, P indicates the replica transfer cost from Seller to Buyer. According to the auction protocol and Seller algorithm, a smaller P means a smaller price and a smaller transfer cost. The variables in Equation (**1**) and their meanings are shown in Table 1.

As you see in Equation (**1**), a larger D means a smaller network delay and a lower price. The larger the value of R is, the more stable the network is, and the lower the price is, while R is a predicted value. A busier Seller may propose a higher price, and the exponential function is introduced to show the important role that the Seller's load plays. C indicates the reputation of Seller, and a higher value means a more trustful Seller. Q means service quality level. Thereby the larger the value of Q is, the lower the price is. λ_1, λ_2 and λ_3 are three weightiness coefficients, which can be initialized with different values according to different grid applications.

Table 1. Variables' definition and their meanings

Variable	Meaning	Value
M	stands for the file size of data replica	by Megabytes
Ns	stands for network bandwidth	by Mbps
D	stands for network latency, including waiting time and other warm-up time	by seconds
R	stands for network reliability, end-to-end network stabilization evaluation	ten levels {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
L	stands for Seller's load (CPU workload, memory load, data storage service load)	ten levels {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
C	denotes Seller's credit or reputation	five levels {1, 2, 3, 4, 5}
Q	denotes quality(service quality, network transfer quality)	three levels {1, 2, 3}

5 Performance Analysis

Proposed data replica selection algorithm is compared with a popular round-robin probing based algorithm. The comparison mainly focuses on the delay performance (the time spend for selection best replica, or known as replica response time).

In round-robin (RR) model, the network topology is a star network, as you see in Fig. 3. R1, R2, R3, R4, and Rn hold replica, and R (R0) stands for requesting node. In the mode of ask and answer, each Seller proposes a price to Buyer. Finally, after all Sellers have been probingly accessed, the Buyer selects the lowest price from all proposals, which is just the best replica.
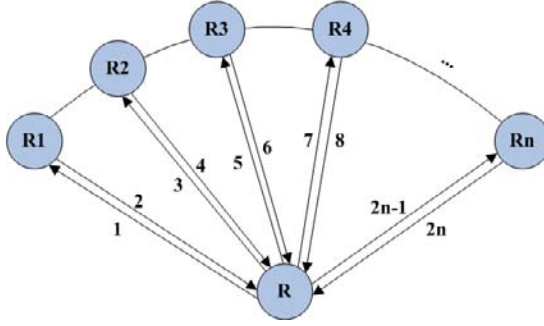
Fig. 3. Round-robin probing based replica selection strategy

In order to compare *algorithm* I (round-robin probing based selection algorithm) with *algorithm* II (VTR based selection algorithm), we make some assumptions as follows.

(1) The number of replicas is denoted as *n*;

(2) The time for computing price (including the time for predicting network status from NWS) is denoted as P_i.

(3) The Network bandwidth matrix $Ns_{(n+1),(n+1)}$ is a symmetrical matrix, which is generated from NWS. $Ns_{i,j}$ denotes the end-to-end network bandwidth between node R_i and node R_j. So we are aware of that,

a) $Ns_{i,j} = Ns_{j,i}$;

b) when $i = j$, $Ns_{i,j} = \infty$;

c) when $i \neq j$, $Ns_{i,j} \in \{10, 45, 100, 155, 622, 1000, 2500, 10000\}$, $i, j = 0,1,2,\ldots, n$.

(4) The length of network data packets are denoted as follow, in *algorithm* I, we suppose L_{ask} indicates inquiring packet, and $L_{response}$ indicates ACK packet, thereby we suppose that $L_{ask}=L_{response}$; in *algorithm* II, token packet is denoted by L_{token}, generally speaking, we have $L_{token} > L_{ask} > L_{response}$.

(5) Network latency is denoted as D_i.

(6) Data packet transfer time is denoted as

$$T_{ij} = \frac{L}{Ns_{i,j}}$$

where that L stands for L_{ask}, $L_{response}$ or L_{token}, and $i, j = 0,1,2,\ldots, n$.

(7) Delay time for two algorithms are demonstrated as follows,

algorithm I: $Delay1 = \sum_{i=1}^{n} (\frac{L_{ask} + L_{response}}{Ns_{0,i}} + P_i + D_i) = \sum_{i=1}^{n} (2T_{0,i} + P_i + D_i)$ (2)

$$T_{0,i} = \frac{L_{ask}}{Ns_{0,i}} = \frac{L_{response}}{Ns_{0,i}}$$

algorithm II: $Delay2 = T_{0,1} + \sum_{i=1}^{n} (P_i + \frac{L_{token}}{Ns_{i,i+1}} + D_i) = T_{0,1} + \sum_{i=1}^{n} (P_i + T_{i,i+1} + D_i)$ (3)

$$T_{i,i+1} = \frac{L_{token}}{Ns_{i,i+1}}$$

Comparing Equation **(2)** and **(3)**, we know that *Delay*1 > *Delay*2. As the increase of *n*, it becomes *Delay*1 >> *Delay*2, which indicates that *algorithm* II is better than *algorithm* I. As the increase of *n*, the advantage becomes more conspicuous, and as the increase of data packet length, the advantage also becomes more remarkable. So, the proposed VTR based method out performs round-robin probing based method in terms of delay.

6   Conclusion

After surveyed existed data replica management and selection methods, this paper proposed an improved VTR-based replica selection algorithm. This paper analyzed all kinds of characteristics of grid node, such as CPU, memory, work load and reputation, and also network conditions, such as latency, bandwidth and reliability, and presented a reasonable transfer cost estimate model. This model could evaluate the cost (known as transfer cost, or response time) between Buyer and the Seller. In this model, we can set several right coefficients to denote emphasis on different factors.

It gives the performance analysis results of comparing the proposed optimal replica selection algorithm with traditional round-robin based replica selection algorithm. The delay time of these two algorithms is introduced, and comparison results show that the proposed algorithm provides a high effective replica lookup and selection service, which out performs traditional replica selection algorithm.

References

1. IEEE standard for local area network: token-passing bus access method and physical layer specification, ANSI/IEEE Std 802.4-1985 (1985)
2. IEEE standards for local area networks: token ring access method and physical layer specifications, IEEE Std 802.5-1989 (1989)
3. Zhou, Z.D., Tang, B., Xu, C.: Design of Distributed Industrial Monitoring System Based on Virtual Token Ring. In: The 2nd IEEE Conf. on Industrial Electronics and Applications, Harbin, China, pp. 598–603 (2007)
4. Foster, I., Kesselman, C.: Globus: A Metacomputing Infrastructure Toolkit. The Int'l J. Supercomputer Applications and High Performance Computing 11(2), 115–128 (1997)
5. Hoschek, W., Jaén-Martínez, F.J., Samar, A., et al.: Data Management in an International Data Grid Project. In: The First IEEE/ACM Int'l Workshop on Grid Computing, Bangalore, India, pp. 17–20 (2000)
6. Chang, R.-S., Chang, J.-S., Lin, S.-Y.: Job Scheduling and Data Replication on Data Grids. Future Generation Comp. Syst. 23, 846–860 (2007)
7. Vazhkudai, S., Tuecke, S., Foster, I.: Replica Selection in the Globus Data Grid. In: The First IEEE Int'l Symp. on Cluster Computing and the Grid (2001)
8. Rahman, R.M., Alhajj, R., Barker, K.: Replica Selection Strategies in Data Grid. J. Parallel Distrib. Comput. 68, 1561–1574 (2008)

On the Operational Semantics
of a Higher Order Safe Ambients Calculus[*]

Zining Cao[1,2]

[1] Department of Computer Science and Technology
Nanjing University of Aero. & Astro., Nanjing 210016, P.R. China
[2] Provincial Key Laboratory for Computer Information Processing Technology
Soochow University, Suzhou 215006, P.R. China
caozn@nuaa.edu.cn

Abstract. In this paper, we propose a higher order safe ambients calculus. In this setting, we propose an extended labelled transition system and an extended labelled bisimulation for this calculus. We also give the reduction barbed congruence and prove the equivalence of extended labelled bisimulation and reduction barbed congruence for this calculus.

1   Introduction

Mobile Ambients was proposed and studied intensively in [3]. The calculus of Mobile Ambients (MA) is proposed both as a core programming language for the Web and as a model for reasoning about properties of mobile processes, including security. In contrast with previous formalisms for mobile processes such as the π-calculus, whose computational model is based on the notion of communication, the MA computational model is based on the notion of movement. An ambient, which may be thought of as a named location, is the unit of movement. Processes within the same ambient may exchange messages; ambients may be nested, so to form a hierarchical structure. The three primitives for movement allow: an ambient to enter another ambient; an ambient to exit another ambient; a process to dissolve an ambient boundary thus obtaining access to its content. Elegant type systems for MA have been given; they control the type of values exchanged within an ambient and the mobility of ambients. A few variants of MA were proposed in literatures [1,4]. In the Safe Ambients calculus (SA) [4], for example, CCS-style co-actions are introduced into the calculus to control potential interferences from other ambients. Although there are lots of variants of MA. But as far as we know, there are seldom works about MA with higher order communication. The only example is [2].

In this paper, we propose a higher order extension of Safe Ambients with passwords (SAP) [5], named MHSAP, and study its semantics. The aim of this

---

paper is to give a new operational semantics theory of MHSAP which is based on an extended labelled transition system. In general, labelled transition systems for ambients calculi are difficult to give. This paper gives an extended labelled transition system for MHSAP. In this system, an extended labelled transition is in the form of: $P \xrightarrow{\Gamma, \alpha} Q$. Intuitively, this means that process P can perform action α in environment Γ, then continues as Q. Based on this extended labelled transition system, we present an extended labelled bisimulation for MHSAP, whose definition is simpler than the bisimulation for SAP in [6] . Furthermore, we prove that this extended labelled bismulation coincides with reduction barbed congruence. This paper is organized as follows: Section 2 gives a brief view of syntax and operational semantics of higher order ambients calculus. Then we also give the reduction barbed congruence. In Section 3, we give an extended labelled transition system for this higher order ambients calculus and an extended labelled transition system based bisimulations, called extended labelled bisimulation, for MHSAP. In Section 4, we prove the coincidence of reduction barbed congruence and extended labelled bisimulation for this higher order ambients calculus. The paper is concluded in Section 5.

2   Monadic Higher Order Safe Ambients Calculus

In this section, we present a monadic higher order safe ambients calculus (named as MHSAP), which is an extension of safe ambients by adding capability of higher order communication. Mobile capabilities (in, out, open and their co-capabilities) make ambient calculi in born with the higher order property. But these mobile capabilities are linear, i.e., only one copy of a process can move, whereas higher order communication ((X) and $\langle P \rangle$) are non-linear higher order operators since more than one copy of a process can be communicated. Therefore MHSAP extends SAP with non-linear higher order communication capabilities.

2.1   Syntax and Labelled Transition System

The formal definition of process is given as follows:

$P ::= 0 \mid X \mid (X).P \mid \langle P_1 \rangle.P_2 \mid in\langle n, h \rangle.P \mid out\langle n, h \rangle.P \mid open\langle n, h \rangle.P \mid \overline{in}\langle n, h \rangle.P \mid \overline{out}\langle n, h \rangle.P \mid \overline{open}\langle n, h \rangle.P \mid P_1 | P_2 \mid (\nu n)P \mid n[P] \mid recX.P$, where $n \in$ set N of names, $X \in$ set Var of process variables.

Structural congruence is a congruence relation including the following rules:

$P|Q \equiv Q|P$; $(P|Q)|R \equiv P|(Q|R)$; $P|0 \equiv P$; $(\nu n)0 \equiv 0$; $(\nu m)(\nu n)P \equiv (\nu n)(\nu m)P$; $(\nu n)(P|Q) \equiv P|(\nu n)Q$ if $n \notin fn(P)$; $(\nu n)(m[P]) \equiv m[(\nu n)P]$ if $n \neq m$.

Informally, 0 denotes inaction. X is a process variable. $c.P$ can perform action c, where c is in the form of $in\langle n, h \rangle$, $out\langle n, h \rangle$, $open\langle n, h \rangle$, $\overline{in}\langle n, h \rangle$, $\overline{out}\langle n, h \rangle$, $\overline{open}\langle n, h \rangle$, (X), $\langle Q \rangle$, then continues as P. $P_1|P_2$ is a parallel composition of two processes P_1 and P_2. In each process of the form $(\nu n)P$ the occurrence of n is bound within the scope of P. $n[P]$ denotes process P in an ambients n. $recX.P$ is a recursive definition of process. An occurrence of n in P is said to be free iff

it does not lie within the scope of a bound occurrence of n. The set of names occurring free in P is denoted $fn(P)$. An occurrence of a name in P is said to be bound if it is not free, we write the set of bound names as $bn(P)$. $n(P)$ denotes the set of names of P, i.e., $n(P) = fn(P) \cup bn(P)$. We use $n(P, Q)$ to denote $n(P) \cup n(Q)$. A process is closed if it has no free variable; it is open if it may have free variables. Processes P and Q are α-convertible, $P \equiv_\alpha Q$, if Q can be obtained from P by a finite number of changes of bound names and bound variables. The class of the processes is denoted as Pr. The class of the closed processes is denoted as Pr^c.

The formal definition of indexed context is given below:

$C ::= [] \mid 0 \mid X \mid (X).C \mid \langle P \rangle.C \mid \langle C \rangle.P \mid in\langle n, h \rangle.C \mid out\langle n, h \rangle.C \mid open\langle n, h \rangle.C$
$\mid \overline{in}\langle n, h \rangle.C \mid \overline{out}\langle n, h \rangle.C \mid \overline{open}\langle n, h \rangle.C \mid C|P \mid P|C \mid (\nu n)C \mid n[C] \mid recX.C$

The operational semantics of processes is given in Table 1. We have omitted the symmetric of the parallelism and interaction.

Table 1.

$$STRUC : \frac{P \longrightarrow P'}{Q \longrightarrow Q'} P \equiv Q, P' \equiv Q'$$

$$COM : (X).P|\langle Q \rangle.R \longrightarrow P\{Q/X\}|R$$

$$IN : n[in\langle m, h \rangle.P_1|P_2]|m[\overline{in}\langle m, h \rangle.Q_1|Q_2] \longrightarrow m[n[P_1|P_2]|Q_1|Q_2]$$

$$OUT : m[n[out\langle m, h \rangle.P_1|P_2]|P_3]|\overline{out}\langle m, h \rangle.Q \longrightarrow n[P_1|P_2]|m[P_3]|Q$$

$$OPEN : open\langle n, h \rangle.P|n[\overline{open}\langle n, h \rangle.Q_1|Q_2] \longrightarrow P|Q_1|Q_2$$

$$PAR : \frac{P \longrightarrow P'}{P|Q \longrightarrow P'|Q} \qquad RES : \frac{P \longrightarrow P'}{(\nu n)P \longrightarrow (\nu n)P'}$$

$$AMB : \frac{P \longrightarrow P'}{n[P] \longrightarrow n[P']} \qquad REC : \frac{P\{recX.P/X\} \longrightarrow P'}{recX.P \longrightarrow P'}$$

2.2 Reduction Barbed Congruence

Now we can give the concept of reduction barbed congruence for higher order ambients processes. Reduction barbed congruence is a behavioural equivalence defined as the largest equivalence that is preserved by all the constructs of the language, is preserved by the reduction semantics of the language, and preserves barbs, which are simple observables of terms.

Now we review the concept of reduction barbed congruence for SAP. In the remainder of this paper, we abbreviate $P\{R/U\}$ as $P\langle R \rangle$. In the following, we use $P \Longrightarrow P'$ to abbreviate $P \longrightarrow ... \longrightarrow P'$.

Definition 1. For each name n, the observability predicate $\Downarrow_n$ is defined by
$P \Downarrow_n$ if $\exists P'$, $P \Longrightarrow P' \equiv (\nu \widetilde{k})(n[\overline{open}\langle n, h \rangle.P_1|P_2]|P_3)$, where $n, h \notin \{\widetilde{k}\}$.

Definition 2. A symmetric relation $R \subseteq Pr^c \times Pr^c$ is a weak reduction barbed congruence if P R Q implies:
(1) $C[P]$ R $C[Q]$ for any $C[]$;
(2) $P \Longrightarrow P'$ implies there exists Q' such that $Q \Longrightarrow Q'$ and P' R Q';
(3) $P \Downarrow_n$ implies $Q \Downarrow_n$.
We write $P \approx_{Ba} Q$ if P and Q are weakly reduction barbed congruent.

3   A New Operational Semantics Theory for MHSAP

The definition of reduction barbed equivalence is simple and intuitive. In practise, however, it is difficult to use: the quantification on all contexts is a heavy proof obligation. Simpler proof techniques are based on labelled bisimilarities, which are co-inductive relations that characterise the behaviour of processes using a labelled transition system (abbreviated LTS). An LTS consists of a collection of relations of the form $P \xrightarrow{\alpha} Q$. The judgement above means that the process P can realise the action α, and becomes Q. The reduction semantics of a process is easily encoded in an LTS because a reduction step can be seen as an interaction with an empty context: this is traditionally called a τ-action.

Although the idea of labelled bisimilarity is very general and does not rely on the specific syntax of the calculus, the definition of an appropriate LTS and associated weak bisimilarity for SAP turned out to be harder than expected (See [6]). In [6], a labelled transition system for SAP was presented. To give this labelled transition system, authors define the concepts about pre-actions, actions, labels, extended processes, concretions, and outcomes. The labelled transition system is formulated as transitions of the form $E \xrightarrow{\lambda} O$ where λ denotes a label and E and O range over extended processes and outcomes, respectively.

In this section, we give an extended labelled transition system for MHSAP and an extended labelled bisimulation for MHSAP. In this extended labelled transition system for MHSAP, a label is extended by a pair of context and action. The extended labelled transition system is formulated as transitions of the form: $P \xrightarrow{\Gamma, \alpha} Q$, where α denotes an action, Γ denotes a context, and P and O range over processes. Intuitively, this transition denotes that in the environment Γ, process P can perform action α, then continues as Q.

3.1   An Extended Labelled Transition System

To present the extended labelled transition system, we give the formal definition of processes, actions and environments in the following.

Processes: $P, Q ::= 0 \mid X \mid (X).P \mid \langle P_1 \rangle.P_2 \mid in\langle n, h \rangle.P \mid out\langle n, h \rangle.P \mid open\langle n, h \rangle.P \mid \overline{in}\langle n, h \rangle.P \mid \overline{out}\langle n, h \rangle.P \mid \overline{open}\langle n, h \rangle.P \mid P_1|P_2 \mid (\nu n)P \mid n[P] \mid recX.P$

Actions: $\alpha ::= \tau \mid in\langle n, h \rangle \mid \overline{in}\langle n, h \rangle \mid out\langle n, h \rangle \mid \overline{out}\langle n, h \rangle \mid open\langle n, h \rangle \mid \overline{open}\langle n, h \rangle \mid Am - in\langle m, h \rangle \mid n[\overline{in}\langle n, h \rangle] \mid AM - out\langle m, h \rangle \mid m[AM - out\langle m, h \rangle] \mid n[\overline{open}\langle n, h \rangle] \mid \langle P \rangle \mid (P)$

Environments: $\Gamma ::= [*] \mid 0 \mid X \mid (X).\Gamma \mid \langle \Gamma_1 \rangle.\Gamma_2 \mid in\langle n, h \rangle.\Gamma \mid out\langle n, h \rangle.\Gamma \mid open\langle n, h \rangle.\Gamma \mid \overline{in}\langle n, h \rangle.\Gamma \mid \overline{out}\langle n, h \rangle.\Gamma \mid \overline{open}\langle n, h \rangle.\Gamma \mid \Gamma_1|\Gamma_2 \mid (\nu n)\Gamma \mid n[\Gamma] \mid recX.\Gamma$

The operational semantics of processes is given in Table 2. The transitions in this system are of the form $P \xrightarrow{\Gamma, \alpha} Q$, which means that process P can perform action α in environment Γ, then continues as Q. For example, transition $in\langle n, h \rangle.P \xrightarrow{m[[*]|D]|n[\overline{in}\langle n,h \rangle.E|F], \ in\langle n,h \rangle} n[m[P|D]|E|F]$ means that if process $in\langle n, h \rangle.P$ is in the environment $m[[*]|D]|n[\overline{in}\langle n, h \rangle.E|F]$ (i.e., replacing $[*]$ in $m[[*]|D]|n[\overline{in}\langle n, h \rangle.E|F]$ by $in\langle n, h \rangle.P$), it can performs action $in\langle n, h \rangle$ and then continues as $n[m[P|D]|E|F]$. We have omitted the symmetric of the parallelism and interaction.

Table 2.

$$ALP : \frac{P \xrightarrow{\Gamma,\,\alpha} P'}{Q \xrightarrow{\Gamma,\,\alpha} Q'} \ where \ P \equiv Q, P' \equiv Q'$$

$$RES : \frac{P \xrightarrow{\Gamma,\,\alpha} P'}{(\nu n)P \xrightarrow{\Gamma,\,\alpha} (\nu n)P'} \ where \ n \notin fn(\alpha)$$

$$PAR : \frac{P \xrightarrow{\emptyset,\,\tau} P'}{P|Q \xrightarrow{\emptyset,\,\tau} P'|Q} \qquad LOC : \frac{P \xrightarrow{\emptyset,\,\tau} P'}{n[P] \xrightarrow{\emptyset,\,\tau} n[P']}$$

$$REC : \frac{P\{recX.P/X\} \xrightarrow{\Gamma,\,\alpha} P'}{recX.P \xrightarrow{\Gamma,\,\alpha} P'}$$

$$INP : (X).P \xrightarrow{[*]|\langle Q\rangle.E,\ (Q)} P\{Q/X\}|E$$

$$OUTP : \langle Q\rangle.P \xrightarrow{[*]|(X).E,\ \langle Q\rangle} P|E\{Q/X\}$$

$$IN : in\langle n,h\rangle.P \xrightarrow{m[[*]|D]|n[\overline{in}\langle n,h\rangle.E|F],\ in\langle n,h\rangle} n[m[P|D]|E|F]$$

$$CO-IN : \overline{in}\langle n,h\rangle.P \xrightarrow{m[in\langle n,h\rangle.D|E]|n[[*]|F],\ \overline{in}\langle n,h\rangle} n[P|m[D|E]|F]$$

$$OUT : out\langle n,h\rangle.P \xrightarrow{n[m[[*]|D]|E]|\overline{out}\langle n,h\rangle.F,\ out\langle n,h\rangle} m[P|D]|n[E]|F$$

$$CO-OUT : \overline{out}\langle n,h\rangle.P \xrightarrow{n[m[out\langle n,h\rangle.D|E]|F]|[*],\ \overline{out}\langle n,h\rangle} P|m[D|E]|n[F]$$

$$OPEN : open\langle n,h\rangle.P \xrightarrow{[*]|n[\overline{open}\langle n,h\rangle.D|E],\ open\langle n,h\rangle} P|D|E$$

$$CO-OPEN : \overline{open}\langle n,h\rangle.P \xrightarrow{open\langle n,h\rangle.D|n[[*]|E],\ \overline{open}\langle n,h\rangle} P|D|E$$

$$PAR-IN : \frac{P \xrightarrow{m[[*]|D|E]|n[\overline{in}\langle n,h\rangle.F|G],\ in\langle n,h\rangle} P'}{P|D \xrightarrow{m[[*]|E]|n[\overline{in}\langle n,h\rangle.F|G],\ in\langle n,h\rangle} P'}$$

$$PAR-CO-IN : \frac{P \xrightarrow{m[in\langle n,h\rangle.E|F]|n[[*]|D|G],\ \overline{in}\langle n,h\rangle} P'}{P|D \xrightarrow{m[in\langle n,h\rangle.E|F]|n[[*]|G],\ \overline{in}\langle n,h\rangle} P'}$$

$$PAR-OUT : \frac{P \xrightarrow{n[m[[*]|D|E]|F]|\overline{out}\langle n,h\rangle.G,\ out\langle n,h\rangle} P'}{P|D \xrightarrow{n[m[[*]|E]|F]|\overline{out}\langle n,h\rangle.G,\ out\langle n,h\rangle} P'}$$

$$PAR-CO-OUT : \frac{P \xrightarrow{n[m[out\langle n,h\rangle.E|F]|G]|[*]|D,\ \overline{out}\langle n,h\rangle} P'}{P|D \xrightarrow{n[m[out\langle n,h\rangle.E|F]|G]|[*],\ \overline{out}\langle n,h\rangle} P'}$$

$$PAR-OPEN : \frac{P \xrightarrow{[*]|D|n[\overline{open}\langle n,h\rangle.E|F],\ open\langle n,h\rangle} P'}{P|D \xrightarrow{[*]|n[\overline{open}\langle n,h\rangle.E|F],\ open\langle n,h\rangle} P'}$$

$$PAR-CO-OPEN : \frac{P \xrightarrow{open\langle n,h\rangle.E|n[[*]|D|F],\ \overline{open}\langle n,h\rangle} P'}{P|D \xrightarrow{open\langle n,h\rangle.E|n[[*]|F],\ \overline{open}\langle n,h\rangle} P'}$$

$$AM-IN : \frac{P \xrightarrow{m[[*]]|n[\overline{in}\langle n,h\rangle.D|E],\ in\langle n,h\rangle} P'}{m[P] \xrightarrow{[*]|n[\overline{in}\langle n,h\rangle.D|E],\ AM-in\langle n,h\rangle} P'}$$

$$AM-CO-IN: \cfrac{P \xrightarrow{m[in\langle n,h\rangle.D|E]|n[[*]],\ \overline{in}\langle n,h\rangle} P'}{n[P] \xrightarrow{m[in\langle n,h\rangle.D|E]|[*],\ n[\overline{in}\langle n,h\rangle]} P'}$$

$$AM-OUT: \cfrac{P \xrightarrow{n[m[[*]]|D]|\overline{out}\langle n,h\rangle.E,\ out\langle n,h\rangle} P'}{m[P] \xrightarrow{n[[*]|D]|\overline{out}\langle n,h\rangle.E,\ AM-out\langle n,h\rangle} P'}$$

$$AM-AM-OUT: \cfrac{P \xrightarrow{n[[*]]|\overline{out}\langle n,h\rangle.D,\ AM-out\langle n,h\rangle} P'}{n[P] \xrightarrow{[*]|\overline{out}\langle n,h\rangle.D,\ n[AM-out\langle n,h\rangle]} P'}$$

$$AM-CO-OPEN: \cfrac{P \xrightarrow{open\langle n,h\rangle.D|n[[*]],\ \overline{open}\langle n,h\rangle} P'}{n[P] \xrightarrow{open\langle n,h\rangle.D|[*],\ n[\overline{open}\langle n,h\rangle]} P'}$$

$$RES-OPEN: \cfrac{P \xrightarrow{\Gamma,\ \langle Q\rangle} P'}{(\nu\widetilde{p})P \xrightarrow{\Gamma,\ (\nu\widetilde{p})\langle Q\rangle} (\nu\widetilde{p})P'} \quad where\ fn(Q)\cap\{\widetilde{p}\}=\emptyset$$

$$COM-TAU: \cfrac{C \xrightarrow{[*]|(X).E,\ (\nu\widetilde{p})\langle P\rangle} G,\quad D \xrightarrow{[*]|\langle Q\rangle.F,\ (P)} G}{C|D \xrightarrow{\emptyset,\ \tau} G}$$
$$where\ \langle Q\rangle.F\equiv C,(X).E\equiv D,\ fn(F)\cap\{\widetilde{p}\}=\emptyset$$

$$IN-TAU: \cfrac{\begin{array}{c}C \xrightarrow{[*]|n[\overline{in}\langle n,h\rangle.E|F],\ AM-in\langle n,h\rangle} n[E|F|m[G|H]],\\ D \xrightarrow{m[in\langle n,h\rangle.G|H]|[*],\ n[\overline{in}\langle n,h\rangle]} n[E|F|m[G|H]]\end{array}}{C|D \xrightarrow{\emptyset,\ \tau} n[E|F|m[G|H]]}$$
$$where\ m[in\langle n,h\rangle.G|H]\equiv C,\ n[\overline{in}\langle n,h\rangle.E|F]\equiv D$$

$$OUT-TAU: \cfrac{\begin{array}{c}C \xrightarrow{\overline{out}\langle n,h\rangle.E|[*],\ n[AM-out\langle n,h\rangle]} E|m[F|G]|n[H],\\ D \xrightarrow{[*]|n[m[out\langle n,h\rangle.F|G]|H],\ \overline{out}\langle n,h\rangle} m[F|G]|n[H]|E\end{array}}{C|D \xrightarrow{\emptyset,\ \tau} E|m[F|G]|n[H]}$$
$$where\ n[m[out\langle n,h\rangle.F|G]|H]\equiv C,\ \overline{out}\langle n,h\rangle.E\equiv D$$

$$OPEN-TAU: \cfrac{\begin{array}{c}C \xrightarrow{[*]|n[\overline{open}\langle n,h\rangle.E|F],\ open\langle n,h\rangle} E|F|G,\\ D \xrightarrow{open\langle n,h\rangle.G|[*],\ n[\overline{open}\langle n,h\rangle]} E|F|G\end{array}}{C|D \xrightarrow{\emptyset,\ \tau} E|F|G}$$
$$where\ open\langle n,h\rangle.G\equiv C,\ n[\overline{open}\langle n,h\rangle.E|F]\equiv D$$

3.2   An Extended Labelled Bisimulation

Based on the extended labelled transition system, we can give an extended labelled bisimulation. This bisimulation is defined in the standard manner and is in a simpler form than the bisimulation in [6].

In the following, we use $P \xRightarrow{\varepsilon} P'$ to abbreviate $P \xrightarrow{\emptyset,\ \tau} ... \xrightarrow{\emptyset,\ \tau} P'$ and use $P \xRightarrow{\Phi,\ \alpha} P'$ to abbreviate $P \xRightarrow{\varepsilon}\xrightarrow{\Phi,\ \alpha}\xRightarrow{\varepsilon} P'$.

Definition 3. A symmetric relation $R \subseteq Pr^c \times Pr^c$ is a weak extended labelled bisimulation if $P\ R\ Q$ implies:

(1) whenever $P \stackrel{\varepsilon}{\Longrightarrow} P'$, there exists Q' such that $Q \stackrel{\varepsilon}{\Longrightarrow} Q'$ and $P'\ R\ Q'$;

(2) whenever $P \stackrel{\Phi,\ \alpha}{\Longrightarrow} P'$, where α is not in the form of $(\nu\widetilde{p})\langle E \rangle$, there exists Q' such that $Q \stackrel{\Phi,\ \alpha}{\Longrightarrow} Q'$ and $P'\ R\ Q'$;

(3) whenever $P \stackrel{\Phi,\ (\nu\widetilde{p})\langle E \rangle}{\Longrightarrow} P'$, there exists Q' such that $Q \stackrel{\Phi,\ (\nu\widetilde{q})\langle F \rangle}{\Longrightarrow} Q'$ and $P'\ R\ Q'$.

We write $P \approx_S Q$ if P and Q are weakly extended labelled bisimilar.

Definition 4. For $P, Q \in Pr$, we write $P \approx_S^o Q$ if $P\{\widetilde{E}/\widetilde{X}\} \approx_S Q\{\widetilde{E}/\widetilde{X}\}$ for any $\widetilde{E}$, where $\widetilde{X} = fv(P) \cup fv(Q)$.

4 Equivalence between Reduction Barbed Congruence and Extended Labelled Bisimulation

In this section, we will give that extended labelled bisimulation coincides with reduction barbed congruence. This result shows that extended labelled bisimulation completely characterises reduction barbed congruence in MHSAP.

4.1 The Characterisation

We firstly give the congruence of $\approx_S^o$.

Proposition 1. For all $P, Q, S, P \approx_S^o Q$ implies:
1. $\alpha.P \approx_S^o \alpha.Q$;
2. $P|S \approx_S^o Q|S$;
3. $(\nu n)P \approx_S^o (\nu n)Q$;
4. $n[P] \approx_S^o n[Q]$;
5. $(X).P \approx_S^o (X).Q$;
6. $\langle R \rangle.P \approx_S^o \langle R \rangle.Q$;
7. $\langle P \rangle.R \approx_S^o \langle Q \rangle.R$;
8. $recX.P \approx_S^o recX.Q$.

To give the equivalence between $\approx_{Ba}$ and $\approx_S$, we need the following lemma.

Lemma 1. $P \approx_{Ba} Q$ implies:

1. whenever $P \stackrel{\Phi,\ \alpha}{\Longrightarrow} P'$, where α is not in the form of $(\nu\widetilde{p})\langle E \rangle$, there exists Q' such that $Q \stackrel{\Phi,\ \alpha}{\Longrightarrow} Q'$ and $P' \approx_{Ba} Q'$;

2. whenever $P \stackrel{\Phi,\ (\nu\widetilde{p})\langle E \rangle}{\Longrightarrow} P'$, there exists Q' such that $Q \stackrel{\Phi,\ (\nu\widetilde{q})\langle F \rangle}{\Longrightarrow} Q'$ and $P' \approx_{Ba} Q'$.

Now we can give the equivalence between $\approx_S$ and $\approx_{Ba}$.

Proposition 2. For any processes P and Q, $P \approx_S Q \Leftrightarrow P \approx_{Ba} Q$.

Proof : ($\Rightarrow$) It is trivial by the congruence of $\approx_S^o$.

($\Leftarrow$) It is trivial by Lemma 1.

5 Conclusions

This paper studied the semantics of monadic higher order safe ambients calculus. We proposed an extended labelled transition system for MHSAP and an

extended labelled bisimulation for this calculus. We proved that extended labelled bisimulation coincides with reduction barbed congruence.

There are seldom works about MA with higher order communication. In [2], authors proposed an extension of the ambient calculus in which processes can be passed as values. A filter model for this calculus was presented. This model was proved to be fully abstract with respect to the notion of contextual equivalence where the observables are ambients at top level.

In [6], a labelled transition system and a labelled bisimulation for SAP are studied. But their labelled transition system is far from standard and needs some auxiliary concepts such as pre-actions and outcomes. Their labelled bisimulation is also not defined in the standard way and complicated.

In this paper, we proposed an alternative theory of labelled transition system based semantics for monadic higher order safe ambients calculus (MHSAP). Firstly, our extended labelled transition system is a clear extension of standard labelled transition system. The idea is simple: whenever a process $C[P]$, i.e., by a subprocess P inserted into an environment $\Gamma = C[*]$, may perform action α, then evolves to a process Q, the associated labelled transition system has a transition $P \xrightarrow{\Gamma,\,\alpha} Q$, i.e., the process P evolves into Q with a label (Γ, α). Secondly, the definition of the extended labelled bisimulation is similar to the standard definition of bisimulation and is very simple. Intuitively, P is bisimilar to Q if whenever P evolves into P' with a label (Γ, α), Q evolves into Q' with the same label Γ, α, and reversely holds. In this paper, we only study the weak bisimulation. But the definitions and the results can be easy to extended to the case of strong bisimulation. We believe that the approach in this paper can also be extended to other process calculi.

References

1. Bugliesi, M., Castagna, G., Crafa, S.: Boxed ambients. In: Kobayashi, N., Babu, C. S. (eds.) TACS 2001. LNCS, vol. 2215. Springer, Heidelberg (2001)
2. Coppo, M., Dezani-Ciangcaglini, M.: A fully abstract model for higher-order ambients. In: Cortesi, A. (ed.) VMCAI 2002. LNCS, vol. 2294, pp. 255–271. Springer, Heidelberg (2002)
3. Cardelli, L., Gordon, A.: Mobile ambients. Theoretical Computer Science 240(1), 177–213 (2000); An extended abstract appeared in Proc. of FoSSaCS 1998
4. Levi, F., Sangiorgi, D.: Controlling interference in ambients. In: Proc. 27th Symposium on Principles of Programming Languages. ACM Press, New York (2000)
5. Levi, F., Sangiorgi, D.: Mobile safe ambients. ACM Transactions on Programming Languages and Systems 25(1), 1–69 (2003)
6. Merro, M., Hennessy, M.: A Bisimulation-based Semantic Theory of Safe Ambients. ACM Transactions on Programming Languages and Systems 28(2), 290–330 (2006)
7. Merro, M., Zappa Nardelli, F.: Bisimulation proof methods for mobile ambients. In: Baeten, J.C.M., et al. (eds.) ICALP 2003. LNCS, vol. 2719. Springer, Heidelberg (2003)

NPGPU: Network Processing on Graphics Processing Units

Yangdong Deng[1], Xiaomemg Jiao[1], Shuai Mu[1], Kang Kang[1], and Yuhao Zhu[2]

[1] Tsinghua University, Institute of Microelectronics
100084, Beijing, China
[2] University of Texas at Austin, Electrical and Computer Engineering Department
TX 78701, Austin, USA
`dengyd@tsinghua.edu.cn, {jiaoxm000,kk06.thu}@gmail.com,`
`mus04@mails.tsinghua.edu.cn,`
`yuhao.zhu@mail.utexas.edu`

Abstract. The Internet is still expanding despite its already unprecedented complexity. To meet the ever-increasing bandwidth requirements under fast appearing new services and applications, today's Internet routers and other key network devices are challenged by two conflicting requirements, high performance and good programmability. In this work, we propose a series of data-parallel algorithms that can be efficiently implemented on modern graphics processing units (GPUs). Experimental results proved that the GPU could serve as an excellent packet processing platform by significantly outperforming CPU on typical router applications. On such a basis, we proposed a hybrid microarchitecture by integrating both CPU and GPU. Besides dramatically enhancing packet throughput, the integrated microarchitecture could also optimize quality-of-service metrics, which is also of key importance for network applications. Our work suggests that an integrated CPU/GPU architecture provides a promising solution for implementing future network processing hardware.

Keywords: GPU, router, table lookup, packet classification, meta-programming, deep packet inspection, Bloom filter, DFA, Software Router, QoS.

1 Introduction

The Internet is one of the most fundamental inventions in the long-standing struggle of the human being to better use and share information. The Internet has become the backbone of human society by connecting the world together. It has profoundly changed the way we live. A key tendency of the Internet is that its traffic has always been rising in an exponential manner since the invention of the Internet. The constant increasing of the traffic is the joint result of two basic momenta. First, more and more people are getting linked to the Internet. Even today there is still a large room for the expansion of broadband access in developing countries. In fact, now China already has the largest number of Internet users, but they are only 25% of China population. The second momentum is the blossoming of on-line video, P2P file-sharing and gaming

applications. As a result, Internet traffic will have to grow at an accelerated rate in the future [1]. The overall traffic measured in Exabytes (i.e., 10^{18} bytes) for the next a few years is illustrated in Fig. 1.
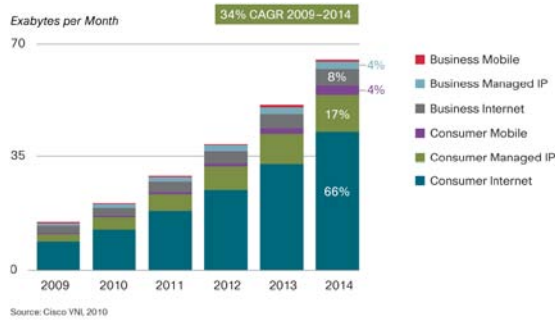

Fig. 1. Global Internet traffic

Besides the overwhelming traffic, another important trend of Internet development is the fast emerging of new protocols [2] due to the deep-going and diversification of network applications and services. On the other hand, the foundation of current networks is based on two technologies, Ethernet and TCP/IP, which were both developed in 1970s [3]. Although it is impressive that the two protocols are still alive today, they have to be frequently updated and patched to meet the ever-changing requirements of today's network applications. As a result, the network processing platforms must be highly programmable to guarantee extendibility and customizability.

Future network devices, especially the "backbone" devices like core routers and wireless controller have to meet the above two fundamental requirements, high throughput and superior flexibility (i.e., programmability). In this work, we focus on an important class of network devices, Internet routers, as a first step toward designing next generation network processing microarchitectures. The responsibility of a router is to provide the physical and logic connections among multiple computer networks by forwarding packets in a timely manner. The IP layer packet processing involves such operations as checking IP header, packet classification, routing table lookup, decrementing TTL value, and packet fragmentation. The packet latency is determined by the following data-plane operations: Checking IP Header (CheckIPHeader) → Packet Classification (Classifier) → Routing Table Lookup (RTL) → Decrementing TTL (DecTTL) → IP Fragmentation (Fragmentation) [4]. In addition, to meet the ever-demanding requirements for intrusion detection, deep packet inspection (DPI) [5] is increasingly becoming a regular task deployed in IP routers. String match (StrMatch) and regular expression match (RegMatch) are two major operations of DPI.

Today's IP routers need to deliver a processing capacity of up to 90Tbs (tera bits per second), and also maintain programmability so as to adapt to new protocols and services. To simultaneously achieve these two goals, most modern routers would be built with dedicated packet processing engines, network processor units (NPUs).

However, NPUs are hard to program due to the lack of mature programming models as well as software development tools [6]. In addition, many NPUs still integrate application specific circuit modules on the same chip to expedite time consuming tasks. Such modules would not be re-configured after tape-out [7].

Recently graphic processing units (GPUs) are quickly rising as a high performance computing platform with a throughput up to 1.5TFLOPS [8]. GPUs also have a stable mass market and thus strong supports for software development (e.g., [9]). Accordingly, it is appealing to leverage the mature GPU microarchitecture for network routing processing. A few recent works already demonstrated the significant potential of GPUs to accelerate packet processing applications ([10]-[12]). In this paper, we outline the overall design of our GPU based router implementation. Our recent work on extending GPU microarchitecture for better routing processing is also covered. To the best of the authors' knowledge, this work is the first one to develop an integrated CPU and GPU microarchitecture for packet processing applications.

2   GPU Architecture and Programming Model

GPUs were originally dedicated graphics acceleration engines, but later turned out to be a high performance general-purpose computing platform after the redesigning of microarchitecture [8] and introduction of new programming models [9]. A typical GPU is organized as an array of multiprocessors or shader cores, with each shader core installing multiple streaming processors (SPs) as well as a small amount of software controlled shared memory. According to current general purpose computing on GPU (GPGPU) models, a GPU program consists of a large number of threads orchestrated into thread blocks. During execution, every thread block would be assigned to a unique shader core, where it would be decomposed into 32-thread groups, or so-called warps, which is the basic unit of job scheduling on GPUs. The execution of a warp follows a single-instruction, multiple data (SIMD) fashion. In other words, threads in a warp always follow the same instruction schedule but handle different data set. The SIMD execution implies that the performance would degrade when a program incurs different execution paths inside a warp of threads.

GPUs with the general purpose computing capability are usually installed on graphics card together with its memory (i.e., global memory in CUDA terminology). The global memory offers a very high memory bandwidth at the cost of a long latency. A GPGPU program always starts on CPU needs to transport data from CPU main memory to GPU global memory before GPU begins execution. The data transferring is through a standard PCIe bus with a peak data rate of 8GB/s [13].

3   GPU Accelerated Routing Processing

As illustrated in Fig. 2, a PC based software router architecture was developed in this work. An NVIDIA GTX280 GPU serves as a packet processing engine. The north-bridge, i.e., memory controller, has two 16-lane PCIe interfaces, with one connected to the graphics card and the other to network-interface-cards (NICs). Each NIC card needs 4 lanes, and thus up to 4 NICs can be plugged in. The main memory serves as buffers for incoming packets.
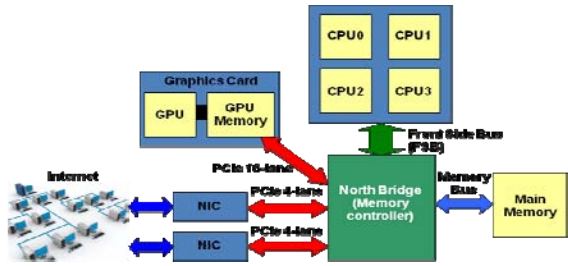
Fig. 2. System diagram of the proposed GPU based software router

We implemented all data-plane routing operations and two major DPI operations on the GPU based software router. Table 1 summarizes the characteristics of these operations, the reference implementation on CPU and the corresponding testing datasets. Among these routing processing operations, CheckIPHeader, DecTTL, and Fragmentation are much less compute-demanding and can be straightforwardly implemented on GPUs. In the following part of this section, we introduce the algorithms for implementing the remaining operations on GPU.

Table 1. Characteristics of routing operations

Packet processing operations	CPU reference	Dataset
Checking IP header (CheckIPHeader)	Taken from RouterBench [14]	WIDE traces [15]
Packet Classification (Classifier)	Linear search	ClassBench [16]
Routing table lookup (RTL)	Radix tree algorithm [14]	RIS [17] & FUNET [18]
Decrementing TTL (DecTTL)	Taken from RouterBench [14]	WIDE traces [15]
IP fragmentation (Fragmentation)	Taken from RouterBench [14]	WIDE traces [15]
String match (StrMatch)	Bloom filter [19]	SNORT [5]
Regular expression match(RegMatch)	AC algorithm [20]	SNORT [5]

3.1 Packet Classification

Packet classification often serves as the first step of routing operations. When a packet comes, a router will check if the packet head matches certain rules in a pre-defined set of rules. Given a match, a corresponding action will be taken on the packet. In this work, we used synthesized rule-sets created by ClassBench [16]. After comparing different packet classification algorithms [21], we used the simplest approach, linear search, because it is the only algorithm that could scale to large rule set with over 2000 rules.

However, the GPU implementation of the linear search algorithm turns out to be very inefficient due to excessive number of the memory read operations to access rules stored in GPU global memory. To attack these two problems, we adopted a metaprogramming technique. Metaprogramming refers to the practice of generating source or executable code dynamically from a more abstracted program, i.e., a metaprogram). Taking this approach, every rule is translated into a fragment of C code that checks if a packet matches this rule. Then a rule-set corresponds to a collection of C code segments combined together. Running the code segment is equivalent to verifying a packet against the very rule set. This technique makes it

possible for a rule-set to be compiled as an integral part of program code, which can be efficiently broadcast to all cores on a GPU through the instruction issuing mechanism. Experiments showed that the GPU implementation could deliver a speed-up of over 30X. The speed-up of GPU implementations over their CPU equivalents is illustrated in Fig. 3.
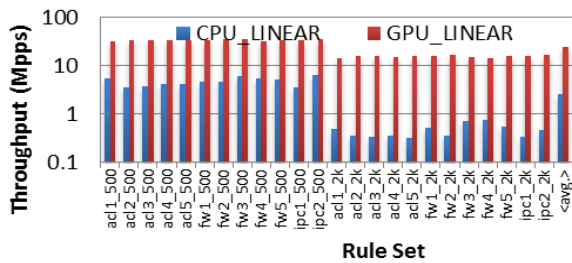

Fig. 3. Classification throughput using linear search on both CPU and GPU

3.2 Routing Table Lookup

Routing table lookup is the central operation of all routers. The mapping of IP destination to egress port) is recorded in a routing table. Upon receiving a packet, a router looks up the table to select a port to which the packet should be forwarded. We adopted a radix tree based longest prefix match algorithm, which is part of RouterBench [14] and is already deployed in Berkeley Unix, for GPU implementation. In the original radix tree, pointers are used to manage tree nodes and edges. Such pointer chasing operations are extremely difficult on GPUs. In our implementation, we proposed a modified data structure called portable routing table (PRT), which uses displacement instead of pointers for tree operations. The parallelization scheme is to straightforwardly deploy one thread for each packet. The GPU implementation was tested on real packet traces collected by RIS [17] and FUNET [18]. Table 2 compares the performance of CPU and GPU implementations. Overall, GPU could outperform CPU by over 6X.

Table 2. Routing table lookup performance of CPU and GPU

Packettrace	#entries of route table	#packets	CPUtime (ms)	GPUtime (ms)	Speed-up
FUNET	41709	99840	22670	3459	6.6
RIS 1	243667	121465	24875	3827	6.5
RIS 2	573810	144908	25637	4135	6.2

3.3 String Match

String match is a key step in any network intrusion detection systems. It checks if a packet body contains any illegal text strings. Most string matching algorithms depend on pointers manipulations for efficient operation, but such algorithms are not amenable to GPUs because of the unpredictable memory access patterns. In this work, we used a Bloom filter based algorithm for GPU implementations [19]. The idea is to

store the Hash values of the illegal keywords with multiple Hash functions during preprocessing. Given a packet, the same set of Hash values are also computed for every string in the packet body. If all the Hash values match the pre-computed value, the string is illegal. The CPU and GPU performance comparison on varying numbers of rule set (i.e., a group of forbidden keywords) is illustrated in Fig. 4. The 3 bars of GPU implementations correspond to GPU computation plus CPU-GPU data transfer time, pure GPU execution, and GPU computation plus streaming CPU-GPU data transfer time. On average, the GPU execution is 19X faster than its CPU equivalent.
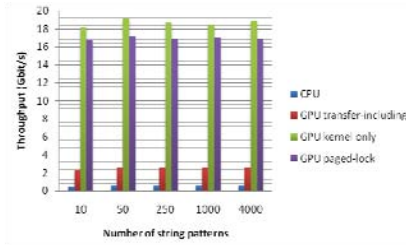
Fig. 4. String matching throughput   Fig. 5. Regular expression match throughput
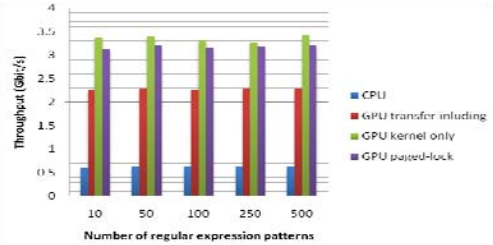
3.4   Regular Expression Match

Regular expression match is another key operation of network intrusion detection. The objective is to check if a packet contains text patterns that can be represented as regular expressions. We used the classical Aho-Corisick (AC) algorithm [20] for this purpose. The AC algorithm uses Deterministic Finite Automata (DFA) [22] to recognize patterns of regular expressions. A DFA can be stored as a table with each row corresponding to a state and each column recording the next state given an input character. The state transition is challenging for GPU because the computation density is too low. After careful optimization, however, the GPU implementation can be 15X faster and even outperform an FPGA implementation [23]. The comparison between CPU and GPU implementations is shown in Fig. 5.

4   An Integrated CPU/GPU Packet Processing Microarchitecture

In the previous section, the potential of GPU for packet processing has been justified. However, two main problems still need to be resolved toward practical GPU based packet process engines. First of all, the communication mechanism between CPU and GPU seriously degrades system throughput. In fact, the packets arriving at the router are first copied to CPU main memory and then to GPU global memory through a PCIe bus. The extra memory copy introduces performance and power overhead. Second, current GPUs follow a batched execution model. In fact CPU needs to buffer enough packets before launching GPU to process them. Such a mechanism could worsen the latency for those earlier-arrived packets and thus violate the quality-of-service (QoS) requirements.
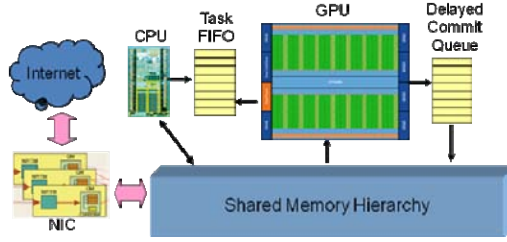
Fig. 6. Hermes microarchitecture

To address the above two problems, we developed a hybrid microarchitecture, Hermes, by integrating CPU and GPU cores on a single chip. The CPU and GPU access a common memory structure including both caches and DRAMs. A simple first-in, first out (FIFO) memory, designated as the task FIFO, is inserted between CPU and GPU. Upon the arrival of network packets, CPU would create a new entry in the task FIFO. The GPU would regularly monitor the FIFO and starts execution when either of the following two conditions is met: 1) the number of packets is big enough for execution with maximum efficiency; and 2) the waiting time of the first packet exceeds a pre-defined latency threshold. Another FIFO memory is inserted after GPU to reorder the packets for handling network protocols with ordering requirements.

The basic pattern of parallel execution is to process every packet with a different thread. The programming model of Hermes is built on top of NVIDIA CUDA with minimum modifications. We abandon the concepts of thread blocks and instead directly scheduling warps.
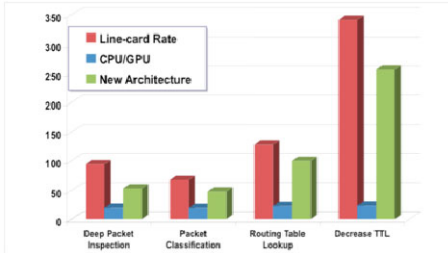

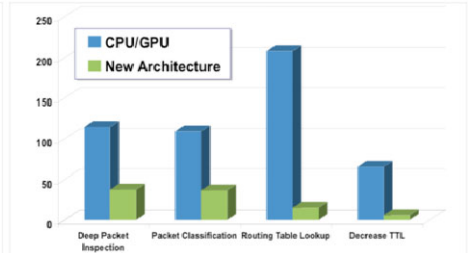**Fig. 7.** Processing throughput comparison   **Fig. 8.** Latency comparison

To evaluate Hermes, we implemented a complete CUDA-enabled software router, which covers all the tasks as declared in Section 4. Since CheckIPHeader, DecTTL, and Fragmentation have almost identical behaviors, we use DecTTL as a representative to explain the results. Fig. 7. compares the throughputs of our proposed architecture (with 16 shader cores) and the discrete CPU/GPU architecture discussed in the previous section. The "line card rate" bars are the input traffic, which is always higher than the processing throughput. Clearly, the Hermes architecture could improve the performance by another factor of 5-6X. Fig. 8. evaluate the latency of the two architectures. On average, the processing latency on Hermes is 82% lower.

5   Conclusion

This work is the first step toward developing next generation massively parallel packet processing platforms. We evaluated the potential of GPU for routing processing. On such a basis, a new hybrid GPU and CPU architecture is proposed to further improve the performance. Our work opens new path to build packet processing engines that could simultaneously meet the requirements of throughput and programmability.

References

1. Cisco, Hyperconnectivity and the Approaching Zettabyte Era,
   http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/Hyperconnectivity_WP_e-book.pdf
2. Shin, M., Kim, Y.: New Challenges on Future Network and Standardization. Advanced Communication Technology 1, 754–759 (2008)
3. Varghese, G.: Network Algorithmics: An Interdisciplinary Approach to Designing Fast Networked Devices. Morgan Kaufmann, San Francisco (2005)
4. Chao, H.J., Liu, B.: High Performance Switches and Routers. Wiley Interscience, Hoboken (2007)
5. The Snort Project: Snort users manual 2.8.0,
   http://www.snort.org/docs/snort/manual/2.8.0/snortmanual.pdf
6. Kulkarni, C., Gries, M., Sauer, C., Keutzer, K.: Programming Challenges in Network Processor Deployment. In: International Conference on Compilers, Architecture and Synthesis for Embedded Systems, pp. 178–187 (2003)
7. De Carli, et al.: PLUG: Flexible Lookup Modules for Rapid Deployment of New Protocols in High-speed Routers. In: SIGCOMM, Barcelona, Spain (2009)
8. Blythe, D.: Rise of the Graphics Processor. Proceedings of IEEE 96, 761–778 (2008)
9. NVIDIA: CUDA Programming Guide 2.3 (2009)
10. Mu, S., et al.: IP Routing Processing with Graphic Processors. In: Design Automation and Test in Europe, Dresden, Germany (2010)
11. Han, S., Jang, K., Park, K.S., Moon, S.: PacketShader: a GPU-Accelerated Software Router. In: SIGCOMM, New Delhi, India (2010)
12. Kang, K., Deng, Y.: Scalable Packet Classification via GPU Metaprogramming. In: Design Automation and Test in Europe, Grenoble, France (2010)
13. PCI-SIG: PCIe® Base 3.0 Specification,
   http://www.pcisig.com/specifications/pciexpress/base3/
14. Luo, Y., Bhuyan, L., Chen, X.: Shared Memory Multiprocessor Architectures for Softwre IP Routers. IEEE Transaction On Parallel and Distributed Systems 14, 1240–1249 (2003)
15. MAWI Working Group: Traffic Archive, http://mawi.wide.ad.jp/mawi/
16. ClassBench, ClassBench: A Packet Classification Benchmark,
    http://www.arl.wustl.edu/classbench/index.htm
17. Routing Information Service (RIS),
    http://www.ripe.net/projects/ris/rawdata.html
18. http://www.ripe.net/projects/ris/rawdata.html
19. Bloom, B.: Space/Time Trade-offs in Hash Coding with Allowable Errors. Communication of the ACM 13, 422–426 (1970)

20. Aho, A.V., Corasick, M.J.: Efficient String Matching: an aid to bibliographic search. Communications of the ACM 18, 333–340 (1975)
21. Taylor, D.E.: Survey and Taxonomy of Packet Classification Techniques. ACM Computing Surveys 37, 238–275 (2005)
22. Hopcroft, J.E., Motwani, R., Ullman, J.D.: Introduction to Automata Therory, Languages, and Computation. Addison-Wesley, Reading (2000)
23. Sugawara, Y., Inaba, M., Hiraki, K.: Over 10Gbps String Matching Mechanism for Multi-stream Packet Scanning Systems. In: Becker, J., Platzner, M., Vernalde, S. (eds.) FPL 2004. LNCS, vol. 3203, pp. 484–493. Springer, Heidelberg (2004)

A Hybrid Routing Mechanism
for ZigBee Wireless Sensor Networks

Pengliu Tan[1] and Mingshan Ju[2]

[1] School of Software, Nanchang Hangkong University, Nanchang, China
pengliu.tan@gmail.com
[2] College of Information and Technology, Nanchang Hangkong University, Nanchang, China
ju_128@yahoo.cn

Abstract. Cyber-Physical Systems (CPS) is one of the latest research fields. Wireless Sensor Network (WSN) is an important research content of CPS. "Real-time" is the most critical feature and performance demand of CPS. In this paper, a hybrid routing mechanism, including improved Cluster-Tree routing protocol and IAODVjr routing protocol, is proposed for ZigBee WSN. The hybrid mechanism can reduce the end-to-end transmission delay and improve the predictability of the overall network in WSN, so as to be suitable for the real-time application's requirements in CPS.

Keywords: WSN, Cluster-Tree, IAODVjr.

1 Introduction

Wireless sensor network (WSN) [1, 2] becomes an important topic for researchers in recent year. A WSN consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, and to cooperatively pass their data through the network to a main location. Under the main goal to provide low-power, cost-effective, flexible, reliable, and scalable wireless products, ZigBee Alliance [3] has been developing and standardizing the ZigBee network. ZigBee is based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). The low cost of ZigBee Network allows the technology to be widely deployed in different wireless applications and the low power-usage allows for extending network life time with smaller batteries. ZigBee is one of the predominant standards commonly used in WSN communications. ZigBee specification [4] defined the top layer of IEEE 802.15.4 from network layer to application layer. ZigBee network defines three kinds of devices personal area network (PAN) coordinator, router, and end device.

Routing strategy in ZigBee uses a combination of two kinds of routing protocol as default. One is Tree Routing (TR) protocol and another is Ad Hoc On-demand Distance Vector (AODV [5]) protocol. The addressing scheme for the nodes in this network uses distributed addressing scheme which follows the tree topology construction. In the applications, the frequently-used protocols are Cluster-Tree routing (The cluster-tree model is proposed in Section 5.2.1.2 in Reference [6]) and $AODV_{jr}$[7]. In TR basis, the Cluster-Tree routing considers the idea of cluster and is

suitable for the occasions with non-moving nodes. Cluster-tree routing can decrease the energy consumption of the master cluster heads and balance the energy consumption of the whole network on the ground that the energy consumption is relative to square distance in free space or four-square distance in multi-path fading space. However, AODV routing protocol provides a method of routing in mobile ad hoc networks. $AODV_{jr}$ is a trimmed down AODV specification which removes all but the essential elements of AODV. Moreover, both of them are not meet the real-time requirements of WSN in CPS and must be further improved. In [8], the authors presented an enhancement of the TR protocol called Improved Tree Routing (ImpTR) protocol. The new ImpTR protocol determined the shortest path to the sink node depending on the neighbor table instead of following the tree topology. The packets were forwarded to the neighbor node if the path to the destination through neighbor node is shorter than the path through personal area network (PAN) coordinator. Results showed that the proposed ImpTR algorithm provided shorter average end-to-end delay, increased throughput and decreased the energy consumption from the network when compared to the original TR routing protocol. In this paper, we propose a hybrid routing protocol for ZigBee WSN. The hybrid protocol consists of improved Cluster-Tree routing protocol and improved $AODV_{jr}$ ($IAODV_{jr}$) routing protocol. The improved Cluster-Tree routing protocol, which is similar to ImpTR, introduces neighbor table into the original Cluster-Tree protocol. $IAODV_{jr}$ routing protocol is the extension to $AODV_{jr}$. The hybrid protocol can decrease the average end-to-end delay, reduce the energy consumption of the master cluster heads, balance the energy consumption of the overall network, and enhance predictability to meet the real-time requirements of applications based on CPS.

This paper is organized as follows. Section 2 explains the improved Cluster-Tree routing protocol. $IAODV_{jr}$ routing protocol is presented in Section 3. Section 4 describes the proposed hybrid routing mechanism. Simulation results are shown in section 5. We conclude our paper in Section 6.

2   Improved Cluster-Tree Routing Protocol

Improved Cluster-Tree routing protocol mainly makes improvements on the routing addressing process. It contains three parts: cluster formation, network address allocation and routing addressing.

2.1   Cluster Formation

When node starts, it selects a back off time T randomly. During this time, if it receives the *hello message* from a cluster head, it will join the corresponding cluster of the cluster head and become its slave node. If not, it will become the cluster head node and broadcast hello message at the end of T. In the process, the node does not forward the *hello message* to ensure that there is only one hop in communicating. Cluster head maintains a cluster member information table, which contains cluster member ID, remaining energy, and depth information. When node receives *hello messages* from multiple cluster heads, it needs to make the comparison and select more reasonable cluster to join. This depends on the depth information of cluster head. The cluster

head with larger depth is chosen to join its cluster, so as to reduce the burdens of upper cluster heads. But if they have the same depth, the cluster head with more remaining energy will be selected. To reduce traffic in the process, cluster head does nothing when receiving *hello message*.

In this way, node messages are transmitted to cluster head in one hop, and arrive at the sink node through upper cluster heads finally. Given the energy factor, the node with more remaining energy will become new cluster head within a cluster later.

2.2   Network Address Allocation

Cluster-Tree routing is based on network address allocation in ZigBee network. There are three types of nodes: coordinator, routing node, terminal node. Each node has its own network address space. The coordinator and routing node are responsible for store and forward routing, and they adopt IAODV$_{jr}$. Terminal node is weak, with small memory and low power, and is suitable to be leaf and use Cluster-Tree algorithm. When a new node is permitted to join, a parent child relation will be formed, and the node will be assigned to a unique network address by its parent node.

In the network, *Depth* denotes the required minimum hops of a node when it sends data to sink node via father-child link. When the network is established, both the network address and *Depth* of sink node are initialized to zero. During the address allocation, the parameters are set as follows: *Cm* is the maximum number of children per parent. *Rm* is the maximum number of router children a parent can have. *Lm* is the maximum depth of the network. *Cskip(d)* is the address block size for each of its router child. On the same network, different nodes often have the same *Rm*, *Cm* and *Lm*. Ref. [8] described the detailed network address allocation.

2.3   Routing Addressing

In this paper, neighbor table of node is introduced into the routing addressing process. The neighbor table of node can be obtained when it join the network. The contents of the neighbor table can be adjusted. According to user demand, you can set some basic information about neighbor nodes, such as extended address, network address, node type, relationship between a neighbor node and the current node, link quality indication (LQI), and so on. When a node receives any frame from its neighbor node, the information in its neighbor table will be updated. When a node *p* receives a data packet, if *p* is the destination node then accepts the packet, otherwise forward the packet. Assuming the address of destination node is *Ad*, we will judge whether it is a descendant node of node *p* according to the following inequality:

$$Ap < Ad < Ap + Cskip(d-1) \tag{1}$$

(a) It is true, if the destination node is a leaf node, the address *An* of next hop is *Ad*, else

$$An = Ap + 1 + [(Ad - (Ap+1))/Cskip(d)] * Cskip(d) \tag{2}$$

And then forward data packets to appropriate child node.

(b) Otherwise, we search the next hop address in the neighbor table of node *p*. If destination node is in the table, forward data packets to destination node directly; if

not, then search the neighbor table of destination node. If there is the same node in neighbor tables of source node and destination node, there is only two hops from source node to the destination node, and next hop node is their common neighbor node. Otherwise, we make judgment of the best path to destination node, then forward data packets following the path.

It is assumed that the set of the addresses of all nodes in neighbor table is N [$A1$, $A2$, $A3$… An], Ad is the address of destination node, Ai is an element of the set, and $D=|Ad-Ai|$. The process of selecting nodes in neighbor table is as follows:

First, we find the smallest $D1$, $D2$ and $D3$ ($D1<D2<D3$). Then we identify their addresses of the corresponding neighbor node A^1, A^2 and A^3. Thus, we ascertain the three nodes in neighbor table. In this way, we can find the nearest neighbor node of destination node as much as possible and reduce routing hops. Next time, we should select the node except ones selected last time in order to avoid the duplication and to reduce unnecessary calculations and storage consumption. The number of nodes in neighbor table can be determined according to the actual requirement, and three is taken here.

During searching the best path, first we find the common parent node with maximum depth of each neighbor node and destination node, and compute the hops according to the depth of common parent node, and then select the neighbor node with minimum hops as the next hop. But if there are several paths with the same hops, we compare the LQI of every node in neighbor table and select the path with the largest LQI. In this way, it will not only avoid the phenomenon of retransmission, but also can ensure the transmission quality.

3   Improved AODV$_{jr}$ (IAODV$_{jr}$)

The improvements of AODV$_{jr}$ are mainly at the aspects of RREQ and RREP packet format. In TCP protocol, because TCP can provide duplex communication, it is unnecessary that the two sides of communication send the ACK each other, and we can attach it to the replied data packet. In this way, it can not only reduce communication frequency and delay, but also improve the communication efficiency and the real time performance. Similarly, we add the ACK or data to the regular packets. That is to say, the data and command can be attached to the RREQ packet from source node. In turn, destination node can also pack the ACK or data into the RREP packet.

Improved RREQ packet format (dashed part is additional) is as follow:

Byte:1	1	1	2	1	1	n
Command frame identity	Command options	RREQ_ID	Destination address	Path cost	path_delay	Data or command
Network load						

Improved RREP packet format (dotted part is additional) is as follow:

Byte:1	1	1	2	2	1	1	n
Command frame identity	Command options	RREP_ID	Address of sender	Address of reply	Path cost	path_delay	ACK or data
Network load							

The format of command options with one byte (dotted part is modified) is as follow:

Bit:0-6	7
Length of additional data	Route repair

The seven bits in command options are used to record the length of additional data, and if the value of length is equal to zero, it means the packet is a regular route packet and has not any additional data.

From source to destination, end-to-end delay is made up of transmission delay and processing delay. The former is related to the distance and is ignored here. We only take into account the node processing delay. Obviously, different node has different processing delay for the same packet. If we record the processing delay of every node in routing path, this is favor of optimizing route. Processing and forwarding delay of a packet going through a node can be obtained through statistics. The modified RREP packet and RREQ package have a field *path_delay*, which is used to record the total end-to-end delay from source to destination node. The value of *path_delay* is initialized to zero, and increases when the packet goes through each forwarding node, and finally, it records the total delay of the entire path. Thus, we can choose the path with the minimum *path_dealy*, this will reduce the end-to-end delay and improve the real-time performance.

Routing algorithm of IAODV$_{jr}$ is as follows:

First, source node which wants to send data will search the routing in its route table. If it exists and is valid, then the data will be immediately sent according to the routing.

Secondly, if the routing does not exist or has been marked as invalid, the source node will create a PREQ packet and broadcast it by flooding. When middle node receives the PREQ packet, it will judge whether the packet has been processed by itself according to RREQ_ID in RREQ. If it is, it is simply discarded. Otherwise, it will create or update the reverse path, which can be used when the destination node sends RREP to the source node, to the source node, and then search the route table.

Next, when destination node receives RREQ, it will generate a RREP and send it to the source node through the reverse path. When middle node and source node receive RREP, they will update their route tables. Moreover, source node will start sending data to destination node.

4   The Hybrid Routing Mechanism

According to the different characteristics (data types and different needs), we can select different methods by setting the value of *DiscoverRoute* in the head of data frame. The three policies are as follows:

1. *Suppression route discovery*: It uses the existed route table. If there is no address of destination node in the route table, set nwkUsingTreeRouting as true, and use Improved Cluster-Tree routing algorithm.
2. *Enable route discovery*: It uses the existed route table. If there is no address of destination node in the route table, it will use IAODV$_{jr}$ to initial route discovery. If the node has not routing ability, it will use Improved Cluster-Tree routing.
3. *Force route discover*: It uses IAODV$_{jr}$ forcedly.

Therefore, for continuous data, we will use *enable route discovery*, in others words, we use IAODV$_{jr}$ to select the best path. For the discrete or control data, we use *suppression route discovery*, because Improved Cluster-Tree routing need not set up route table, and can transmit data quickly. When the information in route table needs to be updated, we can use *force route discovery* to reestablish the routing.

5   Simulation

We simulate the two improved protocols using OPNET. We adopt the mesh topology and use 50 nodes. The 50 nodes are randomly deployed in one area with size 1km^2. Other parameters are set as default. The results are shown as Fig. 1 and Fig. 2.

From the results, we can see that the improved protocols can efficiently decrease the average end-to-end delay compared to Cluster-tree and AODV respectively.
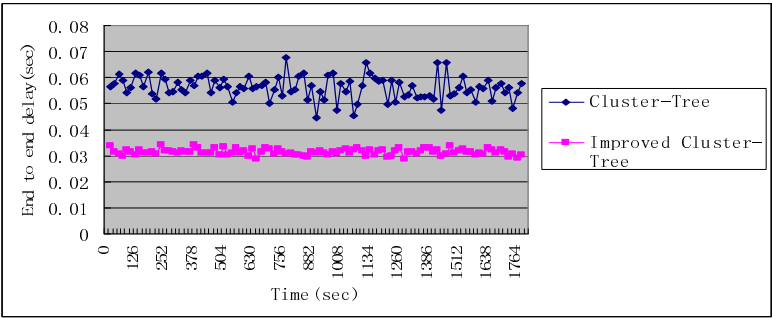
Fig. 1. End to end delay comparison chart
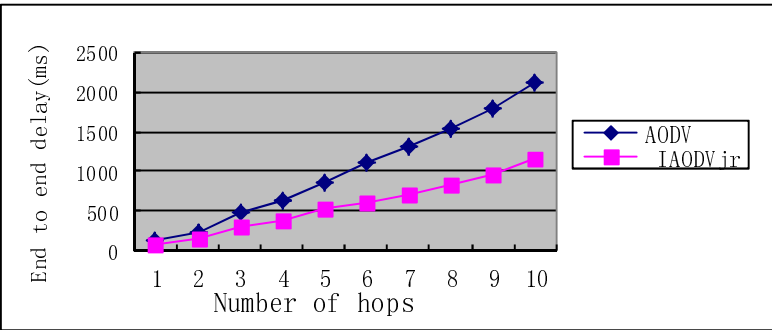
Fig. 2. Average of end to end delay

6   Conclusion

In this paper, a hybrid routing mechanism, including improved Cluster-Tree routing protocol and IAODV$_{jr}$ routing protocol, is proposed for WSN. The improved Cluster-

Tree routing protocol, which is similar to ImpTR, introduces neighbor table into the original Cluster-Tree protocol. IAODV$_{jr}$ is the extension to AODV$_{jr}$. In addition, we make simulations for improved protocol separately. The hybrid protocol can decrease average end-to-end delay, reduce the energy consumption of the master cluster heads and balance the energy consumption of the whole network, and enhance predictability to meet the real-time requirements of applications in CPS. In the future work, we will realize the hybrid routing mechanism in actual project.

References

1. Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless Sensor Networks: A Survey. Journal of Computer Networks 38(4), 393–422 (2002)
2. Kay, R., Mattern, F.: The Design Space of Wireless Sensor Networks. Journal of IEEE Wireless Communications 11(6), 54–61 (2004)
3. ZigBee Information, http://www.ZigBee.org
4. ZigBee Alliance: Zigbee Specification v1.0 (2005)
5. Perkins, C.E., Royer, E.M.: Ad hoc On-Demand Distance Vector Routing. In: 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100. IEEE Press, New York (1999)
6. IEEE-TG15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE standard for Information Technology (2003)
7. Chakeres, I.D., Klein-Bernd, L.: AODVjr, AODV simplified. Mobile Computing and Journal of Communication Review 6(3), 100–101 (2002)
8. Al-Harbawi, M., Rasid, M.F.A., Noordin, N.K.: Improved Tree Routing (ImpTR) Protocol for ZigBee Network. International Journal of Computer Science and Network Security (IJCSNS) 9(10), 146–152 (2009)

Research on the Establishment of Distributed Storage Virtual Geographic Environment Based on Lustre File System

Liqun Yue, Jiangpeng Tian, Xiong You, and Qing Xia

Institute of Surveying and Mapping, Information Engineering University,
Zhengzhou 450052, China
ylqylq_2005@126.com

Abstract. Nowadays the geographic spatial data in surveying and mapping field are increased explosively. Meanwhile, the users need more and more security and stability in data storage, traditional way of data storage cannot fulfill the requirement of users. By summing up the structure and the trait of Lustre file system, we use Luster file system to store massive geographic data, the main framework of Distributed Storage Virtual Geographic Environment System is given, we establish meta data server, data storage server, and Linux client, explain the process of obtaining spatial information in storage system. Finally, an experiment is finished to prove the high-effect and high-stability of distributed storage virtual geographic environment by using Lustre.

Keywords: Lustre File System, Distributed Storage, Virtual Geographic Environment, Meta data, Linux Client.

1   Introduction

With the development of computer technology and as well as surveying and mapping technology, currently, many observation networks all over the world, such as geology, meteorology, geology, oceanography, environment and biology, obtain the information night and day. The visual areas have expanded so rapidly and the storage and management of terrain data has extended hugely since enormous information from every observation satellites all over the earth[1, 2]. It is necessary to design a rational data storage solution to address the distributed storage of massive data.

Relative to data stored in the stand-alone, currently, distributed file system is the first choice since its high stability, expansibility and cost performance. Therefore, this paper focuses on building Distributed Storage Virtual Geographic Environment based on Lustre[3], in order to solve the sharing and using of massive distributed geospatial data.

2   Analysis of Lustre File System Performance

Lustre is an object-based network storage file system developed by Cluster File Systems. It is said that top 30 computers in the world, 10 computers with Lustre, including IBM's Blue Color gene (BlueGene) [4].

2.1   Structure of Lustre File System

Nodes in the system are divided into three types according to function: Client, OST (Object Storage Targets) and MDS (Meta-Data Service) (Figure 1). The management of all parallel file is assumed by the MDS node [5].
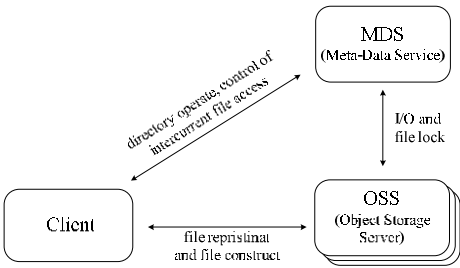

Fig. 1. Structure of Lustre File System

2.2   Features of Lustre File System

Lustre file system has the following features: simple configuration, easy management and high security.

Simple configuration

Data transmission on three parts of file system is according to the same naming convention based on the global name space. Global name space is that every file and directory in the file system has a unified, unique name. In all application servers, the user can use the same name to access the files or directories without caring about the locations of actual storage and metadata server providing services [6,7].

Easy management

Lustre file system on a single machine can become a metadata server, storage server and one or a few of the client part, that is, the metadata server is also used as a client.
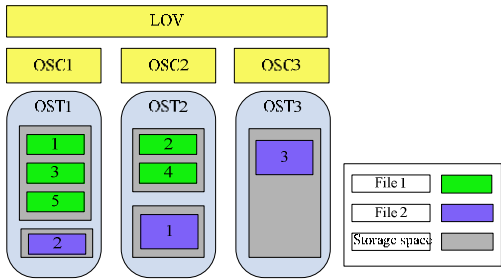

Fig. 2. File Storage Mode of Lustre File System

High security

Lustre file system can be applied in two ways to solve the problem: Firstly, the data is stored by dividing into files and the metadata server does not store data. when

the storage server is stolen in the form of stand-alone, the above data is not accessed since it is not independent (Figure 2), thus making the stored data cannot be obtained; Secondly, Lustre file system backup features are easy to store and data between servers can back up each other.

In addition, Lustre has adapting function for OST which is not available. For example, when an OST is broken and the data cannot be accessed, it will only generate an error, a new file creation operation will automatically avoid failure OST [8,9].

3   To Construct the Distributed Storage Virtual Geographic Environment System Based on Lustre

3.1   Architecture of Distributed Storage Virtual Geographic Environment System

Through the distributed file system to store spatial data, the first is that metadata server is used for the Linux client to provide the index files and data blocks; storage server is mainly used to store the terrain and texture data, Linux client is mainly to solve the bottleneck that file system must be Linux operating system, responsible for the area's cache of data blocks frequently used, require a larger buffer for machine at best; Windows client is a display terminal for visual system. System structure shown in Figure 3.
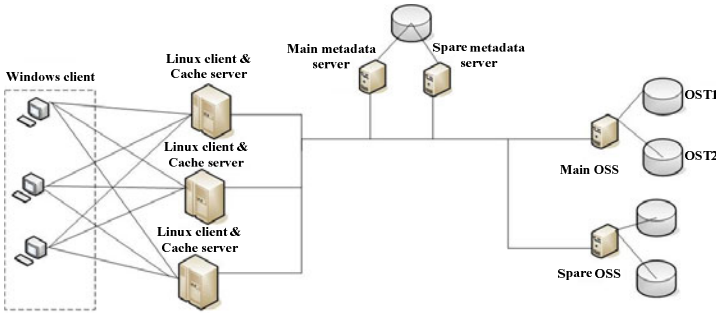

Fig. 3. Architecture of Distributed Storage Virtual Geographic System

3.2   Construction of Single-Mode Metadata Server

Metadata server play a role for liaison and translation in the entire distributed storage system, metadata server and storage server are mainly responsible for the interaction between geospatial information file block and some other system information. Metadata server is responsible for completion of the construction of the file system namespace and directory/file search, as shown in Figure 4, which consists of nine modules, each module is a single thread mode.

Metadata server's main tasks include the following three aspects. Firstly, construction and management of global file distribution view. Secondly, the block/sector-related meta-data management (about 90% of the load) has to be responsible to the OSD, Metadata server is responsible only for management of

metadata associated with file (directory) (almost 10% of the load), that is to say file (directory) is mapped to the object. Thirdly, make security policy of the data storage and sharing and make it come true.
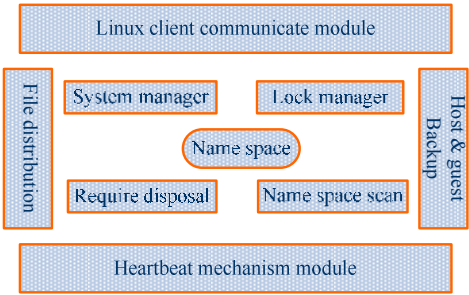

Fig. 4. Structure of Metadata Server

3.3 The Building of Cluster-Based Data Storage Server

The advantages of cluster are found in most data storage server for building Lustre file system, so the cluster-based data storage server can play the best data storage performance. Cluster-based data storage server is responsible for geospatial data storage, to achieve the interaction between Linux client and the physical storage media. In the system, data storage is based on the object storage, storage server using this method to store all the spatial data in the physical storage device, and complete management of each object. Data storage server is responsible for the management of actual spatial information file, including create, update, delete, read and other operations; it is also responsible for reporting properties of spatial information to the metadata server, such as name, time, location, size, format, modified time etc.; it is also receives query request from the metadata server. Data storage server is generally prefer to the non-Windows operating systems such as Linux, Unix, etc., because there are more robust, less breakdown for Linux operating system, and it is in line with the requirements of data storage [10,11].

The performance and robustness of the data storage server has a great impact on the whole system. The normal running of the system needs data storage server with relatively high performance, good fault tolerance and high availability, in order to achieve these goals, the software architecture of data storage server is designed, as shown in Figure 5.

3.4 To Build Linux-Based Multi-Cache Client Server

File system client, running on Linux operating system, is the interface between visualization system and storage system, which is an important component of the file system designed specifically for the project. Together with metadata management subsystem and storage management subsystem, they constitute a distributed, parallel, read-only file system to support the terminal visual system running.
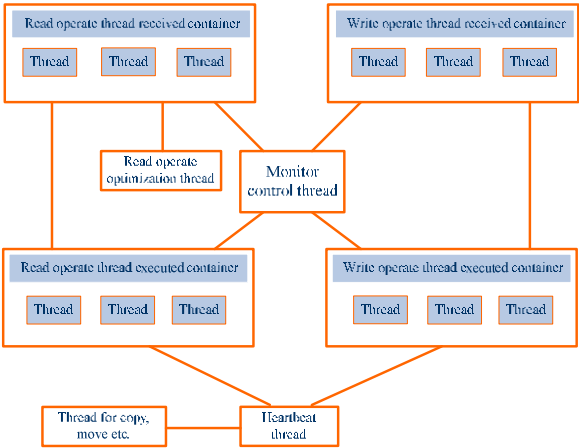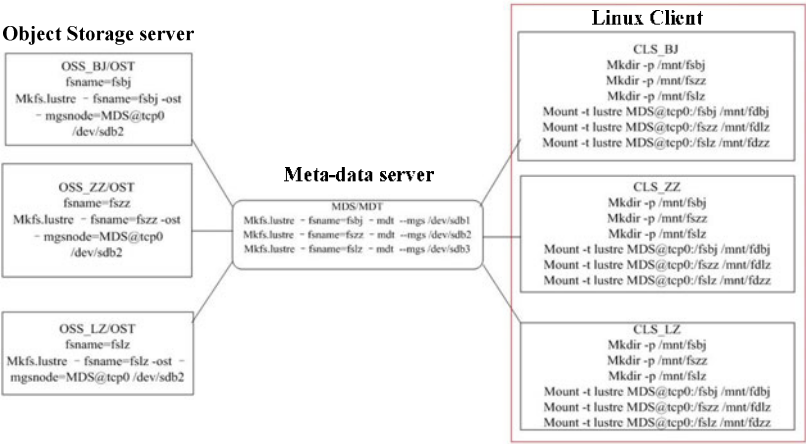
Fig. 5. Architecture of Storage Server

Fig. 6. Client Multi-cache Server

Lustre can basically meet the requirements of Distributed Storage Virtual Geographic Environment System for file system, the only shortcoming is that the Windows client cannot run Lustre file system directly. The solution in this paper is that to build Linux clients in different parts around the metadata server as a data block cache server, then the only thing remained to do is to achieve file transmission between Linux client and visualization terminal. In order to improve speed of data extraction, using multi-threading technology, visualization terminal can obtain the same piece of data from different Linux clients at the same time. The metadata server and the Linux clients sharing the same computer is theoretically feasible, but it will increase the pressure on the metadata. The metadata information is directly read in and resident in the cache, so the memory used is relatively large. Therefore, an

increase in different areas of the Linux client in the metadata servers not only has the advantage of reducing the load of metadata, but also the Linux client can be used as the block cache server for this specific area, the specific structure shown in Figure 6.

3.5   Spatial Information Access Processes in Storage System

File operations include create, delete, open, read, rename, and modify the contents of the relevant attributes. File read operations composed of the following six steps:

1, visualization system request to read file for kernel by calling the read file function, the distributed storage VGE system send this application requests to Linux client, the client locate the target Chunk block according to the starting position and length, if you want to read the contents of several Chunk blocks at the same time, the Linux client will make this request divided into several separate read requests.

2, Linux clients package the serial number index of the file descriptor and the Chunk block in the file into a standard communications message and send to metadata server.

3, Metadata server query the target Chunk block according to the file descriptor and index, the Chunk block may have multiple backup Chunk, metadata server sent all the backup information to the Linux client.

4, Linux client Chunk based on the received Chunk block information, according to its own routing table to find a data storage server with the more recent distance and less load, and send the data read requirement to this data storage server.

5, The data storage server use the received basic index information of Chunk block to find the destination file, then compare with application requirements whether the version number are the same, if different, return damaged information and read operation failed.

6, Linux client transmit the received data to the back-end visualization systems, visual systems cache Chunk block and use it.

4   Experiment and Test

The advantages to restore the data with Lustre file system include universality and stability. Hardware equipment and storage solutions, take ZhengZhou for example, there are 10 storage severs, 1 metadata sever, 1 Linux client and a number of Windows clients, it is better to backup the metadata server and Linux client separately, and 10 storage severs can be distributed by region or resolution.

To test the Lustre file system read and write performance, the following way is practiced: one OST and one MDS for Group 1; three OST and one MDS for Group 2; Group 3 is common stand-alone file transfer mode. The configuration of the three groups as follows:

Group 1: Gigabit Ethernet; two computers with 2.6G CPU frequency and 512M RAM; Lustre1.6.0 file system; Redhat9.0Linux operating system.

Group 2: Gigabit Ethernet; four computers with 2.6G CPU frequency and 512M RAM; Lustre1.6.0 file system; Redhat9.0Linux operating system.

Group 3: Gigabit Ethernet; one computer with 2.6G CPU frequency and 512M RAM; Redhat9.0Linux operating system.

Client: Gigabit Ethernet; one computer with 2.6G CPU frequency and 512M RAM; Redhat9.0Linux operating system. Test results are shown in Table 1 and Figure 7:

Table 1. Three Different Network Operating Statistics

	Data write 1M	Data read 1M	Data write 10M	Data read 10M	Data write 1000M	Data read 1000M
Group 1	0.124s	0.116s	9.012s	9.117s	80.787s	80.516s
Group 2	0.123s	0.119s	8.833s	8.819s	75.854s	77.395s
Group 3	0.121s	0.118s	9.512s	9.823s	85.865s	84.342s
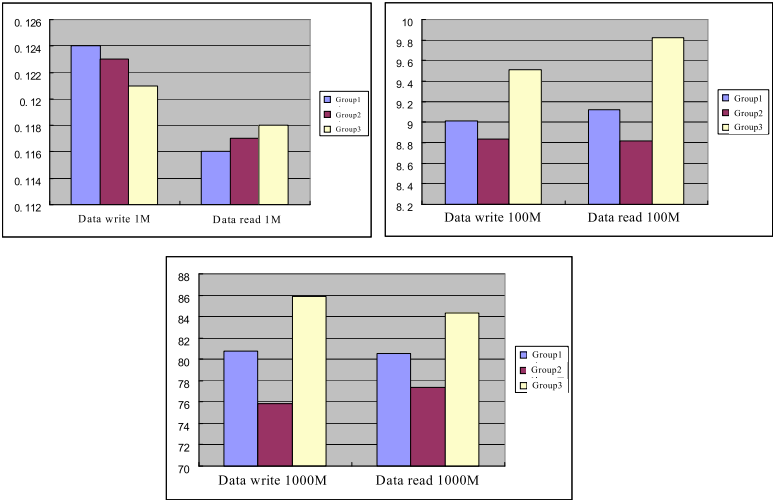
Fig. 7. Figures of Three Different Network Operating Statistics

As shown in the test result, when transferring smaller files, the results in three test environments made little difference and are likely to be affected by other factors, stand-alone storage is probably better than Lustre file system; on the other hand, Lustre demonstrates its superiority when the file is larger, and the more OST, the better the result of file operating.

5   Conclusion

This paper aims at the mass data storage of geographic information and studies the Lustre file system, then builds a Distributed Storage Virtual Geographic Environment based on Lustre and tests its availability and efficiency with experiment. Moreover, the paper also studies some problems to be solved, the current scope of the tests is also limited to small-scale local area network, and do not take full account of the network of factors, the client permissions to access the data is not set and the user may

inadvertently damage the data when accessing it. In addition, the Lustre file system shows a poor support on the Windows operating system, so in the relevant application there are also certain storage limitations. Therefore, in future research work, we will take the stability and scalability of the file system itself as well as how the users of Windows operating system access the Lustre file system data as research focuses.

References

1. Jun, G., Yunjun, X., Xiong, Y., Guang, S.: The Application of Virtual Reality Simulation in the Battlefield Environment. PLA Publishing House, Beijing (1999)
2. Ying, D.: A Research on Key Technologies for Global Multi-resolution Virtual Terrain Environment. Institute of Surveying and Mapping, PLA Information Engineering University, Ph.D (2005)
3. Lin, H., Batty, M.: Virtual Geographic Environments. Science Press, Beijing (2009)
4. Guo, Y.: Object-based network storage. Electronic Industry Press, Bingjing (2007)
5. Zhou, J., Yu, S.: Principles and Techniques of Network Storage. Tsinghua University Press, Beijing (2005)
6. Zhao, W.: Network Storage Technologies. Tsinghua University Press, Beijing (2005)
7. Jia, L.: Network Storage and Military Applicate. National Defence Industry Press, Beijing (2006)
8. Zhou, S.-P., Wang, N.: Lustre File System Management and Use. High Performed Computer Technology (2007)
9. Lustre 1.8 Operations Manual.1-7
10. Zhang, X.: Key Technology of Distributed File System (2009)
11. Zheng, X., Wang, H.: High Availability Design of Massive Data File System (2006)

Asymmetric Multiparty-Controlled Teleportation of Arbitrary n-qudit States Using Different Quantum Channels[*]

Run-Hua Shi[1,2] and Hong Zhong[1,2]

[1] Key Laboratory of Intelligent Computing & Signal Processing of Ministry of Education, Anhui University, Hefei, 230039, China
[2] School of Computer Science and Technology, Anhui University, Hefei, 230039, China
hfsrh@sina.com, zhongh@mail.ustc.edu.cn

Abstract. We present two schemes for asymmetric multiparty-controlled teleportation of an arbitrary n-qudit state using different quantum channels between the sender Alice and the controllers, where the first scheme utilizes the generalized Bell states in d-dimensional Hilbert space as the quantum channels and the second scheme takes the generalized multi-particle GHZ maximally entangled states as quantum resources. In addition, Alice shares n generalized Bell states with the receiver Bob in two schemes. In order to avoid performing three-particle or multi-particle joint measurements and consuming more qudits of the multi-particle maximally entangled states, Alice introduces the generalized CNOT gate operations and then obtains higher communication efficiency than the previous schemes based on entanglement swapping.

Keywords: Quantum information, Quantum teleportation, Quantum state sharing.

1   Introduction

In 1993, Bennett et al. [1] first presented a quantum teleportation scheme, where an arbitrary unknown state of a qubit could be teleported from a sender to a distant receiver with the aid of an Einstein-Podolsky-Rosen (EPR) pair. After their original works, the quantum teleportation has attracted widespread attention due to its important applications in quantum communication and quantum computation, and there are a lot of studies focused on the quantum teleportation in both the theoretical [2-20] and experimental [21-23] aspects.

The quantum controlled teleportation scheme was first presented by A. Karlsson and M. Bourennane [2], in which an unknown quantum state was perfectly teleported from the sender Alice to the receiver Bob with the help of one or many controllers [24-27]. Later, Hillery, Bužek and Berthiaume first presented an original quantum secret sharing (QSS) scheme [28]. QSS concentrates mainly on two kinds of research, one only deals with the QSS of classical information and another with the QSS of

---

quantum information, in which the secret is an arbitrary unknown quantum state. Until 2004, the latter case was first clearly termed by Lance *et al*. [29] as the quantum state sharing (QSTS). Subsequently, there were lots of QSTS protocols proposed in Refs. [30-40]. In essence, QSTS is equivalent to the controlled teleportation.

Recently, Z.J. Zhang, et al. [41] proposed some ways for perfect teleportation of arbitrary *n*-qudit states using different quantum channels (*n* GBS or 2*n*-qudit GES). In this paper, we extend their schemes and present two ways for asymmetric multiparty-controlled teleportation in a generalized *d*-dimensional Hilbert space. For a *d*-dimensional Hilbert space, its basis has *d* eigenvectors along *z*-direction Z_d, can be written as [20]

$$|0\rangle, |1\rangle, |2\rangle, ..., |d-1\rangle . \tag{1}$$

The *d* eigenvectors of another unbiased measuring basis X_d can be described as

$$|\tilde{u}\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} e^{2\pi i l u / d} |l\rangle . \tag{2}$$

A set of maximally *d*-dimensional Bell states can be described as follows

$$\left|\phi^{uv}\right\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} e^{2\pi i l u / d} |l\rangle \otimes |l \oplus v\rangle . \tag{3}$$

Arbitrary state of two qudits in *d*-dimensional Hilbert space can be expressed as

$$\left|\psi\right\rangle_{xy} = \sum_{k,l=0}^{d-1} \alpha_{kl} |kl\rangle_{xy} , \tag{4}$$

where $\sum_{k,l=0}^{d-1} |\alpha_{kl}|^2 = 1$. The generalized Controlled- Not (CNOT) gate operation in the *d*-dimensional Hilbert space can be defined as

$$C_{xy} \left|\psi\right\rangle_{xy} = \sum_{k,l=0}^{d-1} \alpha_{kl} |k(l \oplus k)\rangle_{xy} , \tag{5}$$

where x is the control particle and y the target particle, and $l \oplus k = (l+k) \bmod d$.

2   Asymmetric Multiparty-Controlled Teleportation of Arbitrary *n*-qudit States Using Generalized Two-qudit Bell States

For simplicity, we first consider three-party controlled quantum teleportation scheme of an arbitrary single-qudit state. Suppose that there are three parties, say, Alice, Bob and Charlie, where Alice is the sender, Bob the receiver and Charlie the controller. The basic idea of this teleportation scheme is shown in Figure 1.

An arbitrary single-qudit state can be written as

$$\left|\psi\right\rangle_x = \sum_{l=0}^{d-1} \alpha_l |l\rangle_x , \tag{6}$$

where x is the particle in the state $|\psi\rangle_x$, and all α_l s are complex numbers that satisfy the normalization condition $\sum_{l=0}^{d-1}|\alpha_l|^2=1$. In order to teleport the unknown single-qudit state $|\psi\rangle_x$, Alice first shares two generalized Bell states ($\left|\phi^{00}\right\rangle_{12}$ and $\left|\phi^{00}\right\rangle_{34}$) with Bob and Charlie, where the two particles 2, 4 are sent to Bob, Charlie, respectively, and the two particles 1, 3 are retained with Alice. Here, the state of the whole system of five particles can be written as

$$|\psi\rangle_{x1234}=|\psi\rangle_x\otimes\left|\phi^{00}\right\rangle_{12}\otimes\left|\phi^{00}\right\rangle_{34}=\sum_{l=0}^{d-1}\alpha_l|l\rangle_x\otimes\frac{1}{\sqrt{d}}\sum_{l'=0}^{d-1}\left|l'l'\right\rangle_{12}\otimes\frac{1}{\sqrt{d}}\sum_{l''=0}^{d-1}\left|l''l''\right\rangle_{34}$$

$$=\frac{1}{d}\sum_{l,l',l''=0}^{d-1}\alpha_l\left|ll'l'l''l''\right\rangle_{x1234}\ .$$
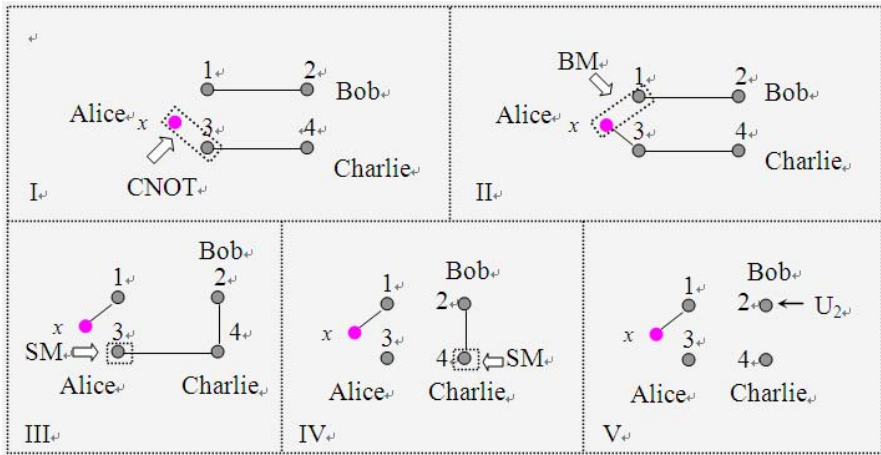
(7)

Fig. 1. The basic idea of our three-party controlled quantum teleportation scheme of an arbitrary single-qudit state

After setting up the quantum channels, Alice introduces a generalized CNOT gate operation. That is, she sends the two particles x and 3 through the generalized CNOT gate, where x is the control particle and 3 the target particle. After applying the generalized CNOT gate operation, the state of the whole system of five particles can be written as

$$C_{x3}|\psi\rangle_{x1234}=\frac{1}{d}\sum_{l,l',l''=0}^{d-1}\alpha_l\left|ll'l'(l\oplus l'')l''\right\rangle_{x1234}\ .$$

(8)

Subsequently, Alice performs a generalized Bell-basis measurement on the two-particle pair (x, 1) first and then a single-particle measurement on the particle 3 with the basis X_d. Without loss of generality, we suppose that the outcomes obtained by

Alice are $\left|\phi^{00}\right\rangle_{x1}$, $\left|\tilde{0}\right\rangle_{3}$, so the state of the retained two particles 2 and 4 can be written as (without being normalized)

$$|\psi\rangle_{24} =_3 \left\langle\tilde{0}\right|\otimes {}_{x1}\left\langle\phi^{00}\right|(C_{x3}|\psi\rangle_{x1234}) = \frac{1}{d^2}(\sum_{l=0}^{d-1}(\alpha_l|l0\rangle+\alpha_l|l1\rangle+...+\alpha_l|l(d-1)\rangle)_{24}. \qquad (9)$$

If Charlie agrees to help Bob obtain the original state, Charlie should perform a single particle measurement on his particle 4 with the basis Z_d and inform Bob of his measurement result. Finally, Bob can recover the unknown single-qudit state $|\psi\rangle_x$ by applying a local unitary operation on his particle 2 according to the measurement results of Alice and Charlie. For example, if Charlie performs a single particle measurement on his particle 4 with the basis Z_d, Bob needs not do anything on his particle 2 and then obtains the unknown single-qudit state $|\psi\rangle_x$ by Eq. (9). That is, the original state is faithfully teleported from Alice to Bob with the permission of Charlie.

It is straightforward to generalize this three-party controlled quantum teleportation scheme of an arbitrary single-qudit state to the case for Alice teleporting an arbitrary n-qudit state $|\psi\rangle_{x_1x_2...x_n}$ to Bob with m controllers: Charlie$_1$, Charlie$_2$, …, Charlie$_m$. Similarly, Alice first shares n generalized Bell states ($\left|\phi^{00}\right\rangle_{12}$, $\left|\phi^{00}\right\rangle_{34}$,…, $\left|\phi^{00}\right\rangle_{(2n-1)(2n)}$) with Bob, where n particles 2, 4,…, (2n) are sent to Bob and the retained n particles 1, 3,…, (2n -1) kept with her. Then Alice shares m generalized Bell states ($\left|\phi^{00}\right\rangle_{1'2'}$, $\left|\phi^{00}\right\rangle_{3'4'}$,…, $\left|\phi^{00}\right\rangle_{(2m-1)'(2m)'}$) with Charlie$_1$, Charlie$_2$, …, Charlie$_m$, respectively, where the particle $(2i)'$ is sent to Charlie$_i$. After setting up the quantum channels, Alice sends these two-particle pairs (x_n, 1'), (x_n, 3'),…, (x_n, $(2m-1)'$) through the generalized CNOT gates, respectively, where the first particle in these two-particle pairs is the control particle and the second particle the corresponding target particle. Subsequently, Alice first performs n generalized Bell-basis measurements on the two-particle pairs (x_1, 2), (x_2, 4),…, (x_n ,2n), respectively, and then m single-particle measurements on these particles 1', 3',…, $(2m-1)'$ with the basis X_d, respectively. After Alice performing these measurements, the quantum information of the unknown n-qudit state $|\psi\rangle_{x_1x_2...x_n}$ will be transferred into the subsystem composed of the retained $n+m$ particles, which are held in hands by Bob and all controllers, such that they can cooperate to extract the quantum information. If all controllers agree to help Bob obtain the original state, each of these controllers should perform a single particle measurement on their particles with the basis Z_d, respectively, and inform Bob of their measurement results via the classical channels. Finally, Bob can recover the unknown n-qudit state $|\psi\rangle_{x_1x_2...x_n}$ by applying a local unitary operation on his n particles according to the measurement results of Alice and all controllers.

3   Asymmetric Multiparty-Controlled Teleportation of Arbitrary *n*-qudit States Using Generalized Multi-Qudit GHZ States

For simplicity, we first consider this perfect teleportation of an arbitrary 2-qudit state with two controllers. Suppose that Alice is the sender, Bob the recover and Charlie₁ and Charlie₂ the controllers, as illustrated in Figure 2.
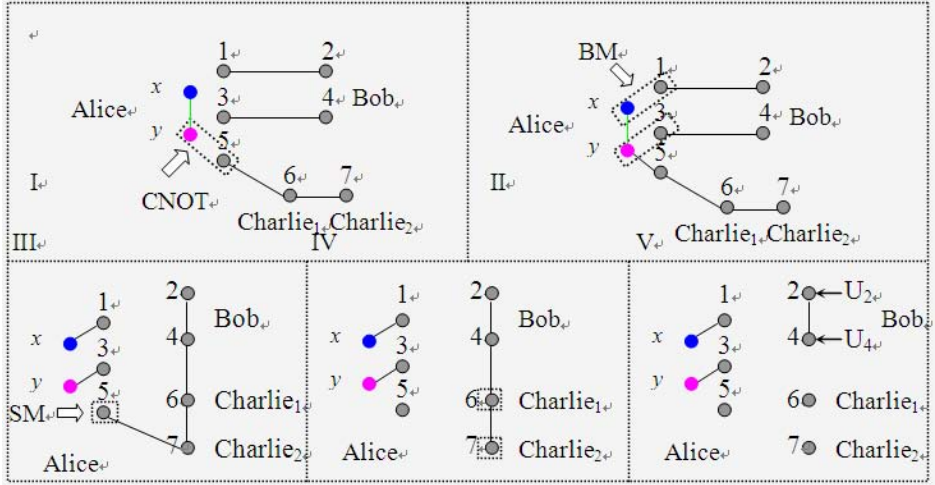

Fig. 2. The basic idea of our controlled teleportation of an arbitrary two-qudit state with two controllers

In order to teleport an arbitrary two-qudit state $|\psi\rangle_{xy}$ (sees Eq. (4)) from Alice to Bob with the permissions of two controllers Charlie₁ and Charlie₂, Alice first prepares two generalized Bell states ($|\phi^{00}\rangle_{12}$, $|\phi^{00}\rangle_{34}$), where the two particles 3 and 4 are sent to Bob, and the two particles 1 and 2 kept with her. In addition, Alice shares a generalized GHZ state ($|\phi^{000}\rangle_{567}$) with Charlie₁ and Charlie₂, where the two particles 6, 7 are sent to Charlie₁, Charlie₂, respectively, and the particle 5 kept with her. After setting up the quantum channels, Alice sends two particles y and 5 through a generalized CONT gate, where y is the control particle and 5 the target particle. After applying the generalized CNOT gate operation, the state of the whole system of nine particles can be written as

$$C_{y5}|\psi\rangle_{xy1234567} = \frac{1}{d\sqrt{d}} \sum_{\substack{k,l,i \\ j,v=0}}^{d-1} \alpha_{kl} |kliijj(v \oplus l)vv\rangle_{xy1234567} \, . \tag{10}$$

Subsequently, Alice performs two generalized Bell-basis measurements on two-particle pairs (x, 1), (y, 3), respectively, first and then a single-particle measurement

on the particle 5 with the basis X_d. Without loss of generalization, we suppose that the outcomes obtained by Alice are $\left|\phi^{00}\right\rangle_{x1}$, $\left|\phi^{00}\right\rangle_{y3}$ and $\left|\tilde{0}\right\rangle_3$, so the state of the retained four particles 2, 4, 6 and 7 can be written as (without being normalized)

$$\left|\psi\right\rangle_{2467} = {}_3\left\langle\tilde{0}\right| \otimes {}_{x1}\left\langle\phi^{00}\right| \otimes {}_{y3}\left\langle\phi^{00}\right| (C_{y5}\left|\psi\right\rangle_{x1234567}) = \frac{1}{d^3}\sum_{k,l,v=0}^{d-1}\alpha_{kl}\left|klvv\right\rangle_{2467}. \tag{11}$$

If two controllers agree to help Bob obtain the original state, each of two controllers should perform a single particle measurement on their particles with the basis X_d, respectively, and inform Bob of their measurement results. Finally, Bob can recover the unknown two-qudit state $\left|\psi\right\rangle_{xy}$ by applying a local unitary operation on his two particles 2 and 4 according to the measurement results of Alice and all controllers.

Similarly, it can generalize this five-party scheme to the case for Alice teleporting an arbitrary n-qudit state to Bob with m controllers, in which n generalized Bell states are utilized as the quantum channel between Alice and Bob, and a generalized $(m+1)$-qudit GHZ state as the quantum channel between Alice and all controllers. Due to limited space, here we do not make further reference to this.

4   Discussion and Summary

In this paper, we have presented two asymmetric multiparty-controlled teleportation schemes of arbitrary n-qudit states using different quantum channels, where the sender Alice utilizes the generalized two-qudit Bell states as the quantum channels between Alice and the controllers in the first scheme and the generalized multi-qudit GHZ states in the second scheme. Especially, the quantum channels in the present schemes are asymmetric, that is, the quantum channels between Alice and Bob are different from those between Alice and the controllers. It is obvious that the asymmetric scheme consumes less qudits as the quantum channels than the symmetric schemes [31-40].

In order to avoid performing three-particle or multi-particle joint measurements as Refs. [20,32] and consuming more qudits of the multi-qudit maximally entangled states as Refs. [31,36], in our schemes the sender Alice introduces and applies the generalized CNOT gate operations. Compared with the previous schemes based on entanglement swapping, our schemes consume fewer quantum and classical resources and thus obtain higher communication efficiencies, and lessen the difficulty of the quantum measurements, as the generalized CNOT gate operations are applied.

The security of our schemes mainly depends on the process for setting up the quantum channels. In order to set up the secure quantum channels with all participants, Alice can use the decoy-photon technique. However, the proportion of the decoy photons is small and can be negligible in theory. That is, almost all the quantum resources (except for the instances chosen for eavesdropping check) can be used to carry the quantum information if the participants act in concert, thus the intrinsic efficiency for qudits approaches 100% in our schemes.

References

[1] Bennett, C.H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A., Wotters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett. 70(13), 1895–1899 (1993)

[2] Karlsson, A., Bourennane, M.: Quantum teleportation using three-particle entanglement. Phys. Rev. A 58(6), 4394–4400 (1999)

[3] Ikram, M., Zhu, S.Y., Zubairy, M.S.: Quantum teleportation of an entangled state. Phys. Rev. A 62(2), 22307-1–22307-9 (2000)

[4] Li, W.L., Li, C.F., Guo, G.C.: Probabilistic teleportation and entanglement matching. Phys. Rev. A 61(3), 34301-1–34301-3 (2000)

[5] Gorbachev, V.N., Trubilko, A.I.: Quantum teleportation of EPR pair by three-particle entanglement. J. Exp. Theor. Phys. 91(5), 894–898 (2000)

[6] Lu, H., Guo, G.C.: Teleportation of a two-particle entangled state via entanglement swapping. Phys. Lett. A 276(6), 209–212 (2000)

[7] Lee, J., Kim, M.S.: Entanglement Teleportation via Werner States. Phys. Rev. Lett. 84(18), 4236–4239 (2000)

[8] Shi, B.S., Jiang, Y.K., Guo, G.C.: Probabilistic teleportation of two-particle entangled state. Phys. Lett. A 268(4), 161–164 (2000)

[9] Zho, J.D., Hou, G.: Teleportation scheme of S-level quantum pure states by two-level Einstein-Podolsky-Rosen states. Phys. Rev. A 64(1), 12301-1–12301-4 (2001)

[10] Yan, F.L., Wang, D.: Probabilistic and controlled teleportation of unknown quantum states. Phys. Lett. A 316(5), 297–303 (2003)

[11] Fujii, M.: Continuous-variable quantum teleportation with a conventional laser. Phys. Rev. A 68(5), 50302-1–50302-4 (2003)

[12] An, N.B.: Teleportation of coherent-state superpositions within a network. Phys. Rev. A 68(2), 22321-1–22321-6 (2003)

[13] Bowen, W.P., Treps, N., Buchler, B.C., Schnabel, R., Ralph, T.C., Bachor, H.A., Syml, T., Lam, P.K.: Experimental investigation of continuous-variable quantum teleportation. Phys. Rev. A 67(3), 32302-1–32302-4 (2003)

[14] Gao, T., Yan, F.L., Wang, Z.X.: Quantum secure direct communication by Einstein-Podolsky-Rosen pairs and entanglement swapping. Quant. Inform. Comp. 4(6), 186–195 (2004)

[15] Yang, C.P., Chu, S.I., Han, S.: Efficient many-party controlled teleportation of multiqubit quantum information via entanglement. Phys. Rev. A 70(2), 22329-1–22329-8 (2004)

[16] Gordon, G., Rigolin, G.: Generalized teleportation protocol. Phys. Rev. A 73(4), 42309-1–42309-4 (2006)

[17] Gao, T., Yan, F.L., Li, Y.C.: Optimal controlled teleportation via several kinds of three-qubit states. Sci China Ser G-Phys Mech Astron 51(10), 1529–1556 (2008)

[18] Zhan, Y.B., Zhang, Q.Y., Wang, Y.W., Cheng, M.P.: Schemes for Teleportation of an Unknown Single-Qubit Quantum State by Using an Arbitrary High-Dimensional Entangled State. Chin. Phys. Lett. 27(1), 10307 (2010)

[19] Wang, T.J., Zhou, H.Y., Deng, F.G.: Quantum state sharing of an arbitrary m-qudit state with two-qubit entanglements and generalized Bell-state measurements. Physica A 387(18), 4716–4722 (2008)

[20] Dong, J., Teng, J.F., Wang, S.Y.: Controlled Teleportation of Multi-qudit Quantum Information by Entanglement Swapping. Commun. Theor. Phys. 51(5), 823–827 (2009)

[21] Bouwmeester, D., Pan, J.W., Matle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental Quantum Teleportation. Nature 390(6660), 575–579 (1997)

[22] Boschi, D., Branca, S., Martini, F.D., Hardy, L., Popescu, S.: Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. Phys. Rev. Lett. 80(6), 1121–1125 (1998)

[23] Furusawa, A., Sorensen, J.L., Braunstein, S.L., Fuchs, C.A., Kimble, H.J., Polzik, E.S.: Unconditional Quantum Teleportation. Science 282(5389), 706–709 (1998)

[24] Zhang, Z.J.: Controlled teleportation of an arbitrary n-qubit information using quantum secret sharing of classical message. Phys. Lett. A 352(1-2), 55–58 (2006)

[25] Zhan, X.G., Li, H.M., Zeng, H.S.: Teleportation of Multi-qudit Entangled States. Chin. Phys. Lett. 23(11), 2900–2902 (2006)

[26] Li, X.H., Deng, F.G., Zhou, H.Y.: Controlled teleportation of an arbitrary multi-qudit state in a general form with d-dimensional Greenberger-Horne-Zeilinger states. Chin. Phys. Lett. 24(5), 1151–1153 (2007)

[27] Zhang, Z.J., Li, Y., Man, Z.X.: Improved Wojcik's eavesdropping attack on ping-pong protocol without eavesdropping-induced channel loss. Phys. Lett. A 341(5-6), 55–59 (2005)

[28] Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59(3), 1829–1834 (1999)

[29] Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Tripartite Quantum State Sharing. Phys. Rev. Lett. 92(17), 177903-1–177903-4 (2004)

[30] Li, Y.M., Zhang, K.S., Peng, K.C.: Multiparty secret sharing of quantum information based on entanglement swapping. Phys. Lett. A 324(5-6), 420–424 (2004)

[31] Deng, F.G., Li, C.Y., Li, Y.S., Zhou, H.Y., Wang, Y.: Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys. Rev. A 72(2), 22338-1–22338-8 (2005)

[32] Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs. Phys. Rev. A 72(4), 44301-1–44301-4 (2005)

[33] Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements. Eur. Phys. J. D 39(3), 459–464 (2006)

[34] Wang, Z.Y., Liu, Y.M., Wang, D., Zhang, Z.J.: Generalized quantum state sharing of arbitrary unknown two-qubit state. Opt. Commun. 276(2), 322–326 (2007)

[35] Yuan, H., Liu, Y.M., Han, L.F., Zhang, Z.J.: Tripartite Arbitrary Two-Qutrit Quantum State Sharing. Commun. Theor. Phys. 49(5), 1191–1194 (2008)

[36] Li, X.H., Zhou, P., Li, C.Y., Zhou, H.Y., Deng, F.G.: Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J. Phys. B: At. Mol. Opt. Phys. 39(8), 1975–1983 (2006)

[37] Man, Z.X., Xia, Y.J., An, N.B.: Quantum state sharing of an arbitrary multiqubit sate using nonmaximally entangled GHZ states. Eur. Phys. J. D 42(2), 333–340 (2007)

[38] Wang, T.J., Zhou, H.Y., Deng, F.G.: Quantum state sharing of an arbitrary m-qudit state with two-qubit entanglements and generalized Bell-state measurements. Physica A 387(18), 4716–4722 (2008)

[39] Xiu, X.M., Dong, L., Gao, Y.J., Chi, F.: A Theoretical Scheme for Multiparty Multi-particle State Sharing. Commun. Theor. Phys. 49(5), 1203–1206 (2008)

[40] Sheng, Y.B., Deng, F.G., Zhou, H.Y.: Efficient and economic five-party quantum state sharing of an arbitrary m-qubit state. Eur. Phys. J. D 48(2), 279–284 (2008)

[41] Zhang, Z.J., Liu, Y.M., Wang, D.: Perfect teleportation of arbitrary n-qudit states using different quantum channels. Phys. Lett. A 372(1), 28–32 (2007)

Parallel Computing of Multi-resolution Combined Fuzzy Networks

Yan Liang

China United Network Communications Group Company Limited
Postdoctoral Workstation, 100033 Beijing, China
Beijing Universial of Posts and Communications
`liangy6@chinaunicom.cn`

Abstract. This paper presents the parallel computing of a multi-resolution combined fuzzy network. To improve computing speed, a parallel structure is developed for the fuzzy network. This paper gives a fuzzy neural network classifier for an instance to implement the parallel computing. The fuzzy neural network classifier presented consists of 4 parallel classification logic units, each of which has the same structure and functions, so that the classification logic units can compute and operate classification simultaneously and obtain results at the same time. The fuzzy neural network classifier is realized using field programmable gate array (FPGA) and shows good independency and extensibility. Test results show that it can be cascaded to achieve high speed computing and classification.

Keywords: parallel computing, fuzzy neural network classifier, hyper-box, high speed computing.

1 Introduction

Fuzzy networks are of importance for patter recognition, signal detection, and control system [1]. Most of the proposed systems use the artificial neural network [2, 3] or fuzzy logic [4] for event classification. Artificial neural networks have attracted a great deal of attention because of their inherent pattern recognition capabilities and parallel computing and learning capability. Also, the key benefit of fuzzy logic is that it is propitious to solve classification problems because its knowledge representation is explicit in utilizing simple "IF-THEN" relations [5]. Therefore, by combining both merits together, neural-fuzzy systems [6] with appropriate neural-fuzzy learning algorithms [7] are widely used in recent classification applications, such as facial expression recognition [8], system monitoring [9], etc. In classification field, Simpson proposed a fuzzy min-max neural network (FMMNN) [10] which uses hyper-box as the basis of fuzzy sets. This model has a disadvantage that the training result has a close relationship with the pattern input order. To overcome this shortcoming and achieve high-speed classification, Chen Xi put forward a new kind of classifier named multi-resolution combined fuzzy min-max classifier [11].

    This paper presents a hardware design with a parallel structure of the classification part of multi-resolution combined fuzzy network classifier for the first time. The

training algorithm is implemented by software and the classification process is realized by hardware. In this paper, the model and algorithm of the fuzzy network classifier are introduced in section two. The parallel structure design is proposed in section three. And section four presents the hardware realization. This design is verified using field programmable gate array (FPGA).

2   Model and Algorithm

A three-layer fuzzy network is shown as Fig. 1 [11, 12]. Data are read through input nodes, and computed by second layer, the hyper-box nodes. A variable number of hyper-boxes are used to represent a class to allow the formation of arbitrary decision boundaries. So the hyper-box can be taken as a node of the neural network, and also be regarded as a fuzzy rule. Weights which connect input nodes to hyper-box nodes contain information of maximum and minimum of hyper-boxes. After calculation and comparison at the second layer, result is output by the third layer, the output nodes. What connect hyper-box nodes to class nodes are binary value, which show the sorts of hyper-boxes.
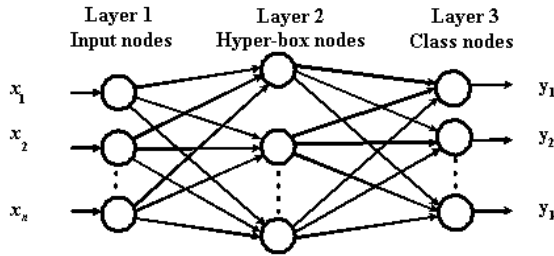
Fig. 1. Three-layer fuzzy neural network

The hyper-box is defined as a multi-dimension rectangle. It is represented by the minimum and the maximum of the multi-dimension rectangle. The hyper-box membership function plays a crucial role in the fuzzy min-max classification algorithms. To overcome the disadvantage of the fuzzy min-max model, that the training result is influenced by pattern input order [13], the fuzzy hyper-box reliability [14] is introduced into the improved new multi-resolution combined fuzzy network classifier model. Each hyper-box is determined by 4 variables,

$$B = \{ X , V , W , P \} . \tag{1}$$

where B_j represents the jth hyper-box, V_j and W_j represent the max value and the min value of the hyper-box, X_h is the sort of the hyper-box and P_j is the hyper-box reliability. The hyper-box reliability P_j is defined as below,

P_j = number of correct classified patterns in B_j / number of all patterns in B_j . $\qquad$ (2)

During the learning process, if the sort of a new input pattern is the same as a hyper-box already exists, and the position of the new input pattern is in the hyper-box or the hyper-box can comprise the position of the input pattern through expanding

without exceeding the permitting scope of the hyper-box, the hyper-box needs not reduce though it is overlapped with other hyper-box. The only thing needed to do is to adjust the hyper-box reliability. If the position of the input pattern is not in the proper area that the hyper-box can comprise through expanding or there is no hyper-box whose sort is the same as the input pattern, a new hyper-box is set up.

During the classification process, reliability parameters of the hyper-boxes that comprise the input pattern are compared. The sort of the new input pattern is the same as the sort of that hyper-box with the maximal reliability. If no existed hyper-box comprises the input pattern, a deny signal is given and the sort of the input pattern is uncertain.

As the hyper-box reliability is introduced, when all of the training patterns are used to train the classifier, they need to be read again to get the hyper-box reliability. In order to simplify the training process, a hypothesis is introduced that the density of the area generated by the hyper-box expansion is equal to that of the hyper-box when it does not expand. Then the result of the expanding is just to add a pattern which is the same sort as the hyper-box. The number of the patterns which are different from the hyper-box can be gotten by multiplying the density of the patterns inside the hyper-box and the volume of the hyper-box after it expending. This can be illustrated as follows,

$$p = n_p / v_p . \tag{3}$$

$$P_j = [N_b + 1] / [N_b + 1 + (V_2 - V_1) * p] . \tag{4}$$

where p represents the density of the patterns inside the hyper-box, n_p represents the number of all patterns in the hyper-box and v_p is the volume of the hyper-box, P_j represents the reliability of the jth hyper-box, N_b is the number of the p patterns before hyper-box expanding, V_1 and V_2 represent the volumes of the hyper-box before and after expanding, respectively, and can be gotten from the max and min value of the hyper-box.

3   The Parallel Structure Design of Fuzzy Network Classifier

In consideration of the independency in controlling and the extensibility in classification, the structure of the multi-resolution combined fuzzy network classifier is mainly divided into two modules in hardware design. One is the controller module, and the other is the classification sub-module. The controller module dominates the data input and output, and generates a classifying signal to the classification module. But it does not care about the classification details. The classification sub-module classifies the input patterns stored into memory and keeps results in fixed memory without participating in the data input and output.

The communication signal (busy signal) of the classifier is designed as follow. When the input data are stored in the memory, the controller inspects the "busy" signal of the classification sub-module. If the signal is high, it means that the classification sub-module is not working then, the controller gives a "reset" signal and then gives a "begin" signal to inform the classification sub-module to start classifying. If the busy signal is low, the controller just waits until it inspects the "busy" signal again. Different parts of the classifier are illustrated below.

3.1   Controller

A normal system is often controlled by a universal MCU or a finite state machine[15]. In this design, as the controller is not very complicated, a Moore finite state machine is used to control the model. In order to predigest the instruction system the same instruction is used to read the data that denote the hyper-box information and the input data that need to be classified. The different kind of information is stored in different part of the memory.

The controller has three main functions: 1), storing the input data (including the data about the hyper-box information and the data of the pattern that need to be classified) into the memory; 2), sending the "begin" signal to inform the classification sub-module to start classifying; 3), storing the classification results into the memory and outputing the result. The communication of the controller with other modules is shown in Fig. 2.
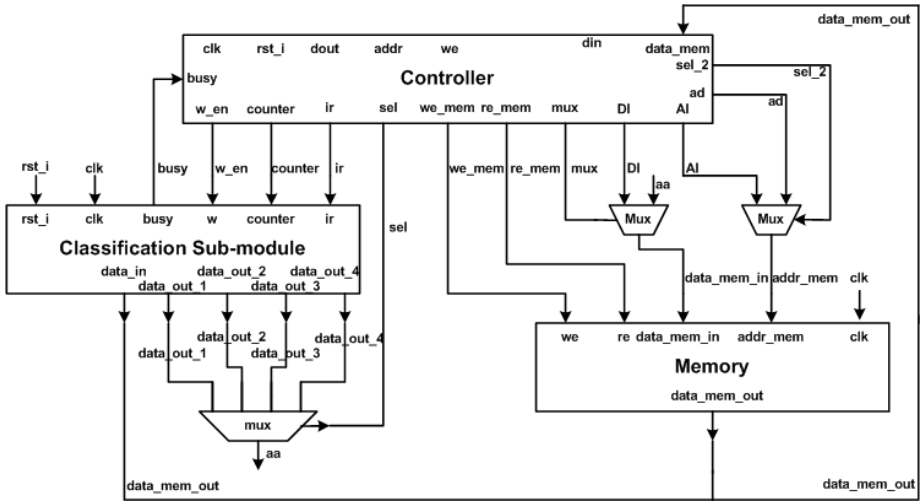
Fig. 2. The frame of the whole classifier

3.2   Distribution of the Data in Memory

The memory (RAM) can read or write a 16 bits data in a single clock period. Different part of the memory stores different data. The memory includes four parts. The distribution of different data is shown in Fig. 3. The hyper-box part is used to store the information of the hyper-box through training. The sequence of the data in a hyper-box is the maximal value, the minimal value, the reliability and the sort, respectively. The later hyper-box is stored next to the former. After one hyper-box is read, the next one can be read without computing the address of it. The address pointer can get it through adding 1 to itself. The "input_data" part is used to store the data of the input pattern that need to be classified. Different input data are also stored in a continuous space. The "reliability" part is used to store the reliability of hyper-box. The "class" part is

used to store the classification results (the sort of an input data should be). The number of memory units in the "class" part is the same as that of the classification logic units. Each memory unit stores a result of an input pattern.
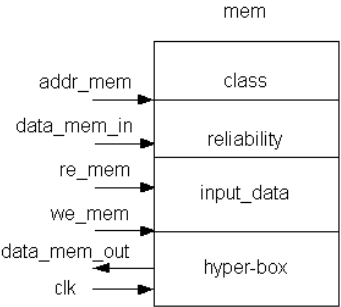

Fig. 3. Distribution of the date in memory

3.3   Structure of the Classification Logic Unit

The classification sub-module is made up of many classification logic units which have the same structure and functions. Each classification unit is a module which can classify data independently. The structure of classification logic unit is shown as Fig. 4.
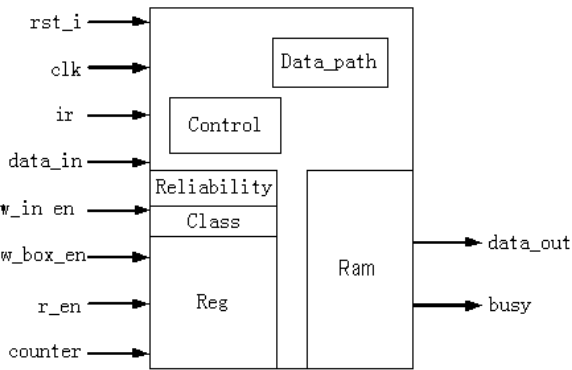
Fig. 4. The frame of the classification logic unit

The classification logic unit includes two groups of registers. One named "Reg" is used to store the input pattern. The other one named "Ram" is used to store the information of a hyper-box. When the classification logic unit receives the "begin" signal, the input patterns have been stored into the "Reg". The classification unit reads the information in the first hyper-box starts computing in the "Ram". When the reliability of the input pattern of the hyper-box is gotten, the reliability is stored into

the register "reliability" and the sort of the hyper-box is stored into the register "class". Then the next hyper-box is read in and the classification logic unit repeats the computing. The new reliability is gotten. If the new reliability is larger than the previous one, the new reliability and the sort of the new hyper-box are stored into the register "reliability" and the register "class" separately to replace the old ones. If the new reliability is smaller than the previous one, nothing will be done. Then the next hyper-box is read in and the same operation will be done. When all the hyper-boxes are read in, the computing is over. At this time the data in the register "class" is the sort of the input pattern. The classification process is shown in Fig. 5.
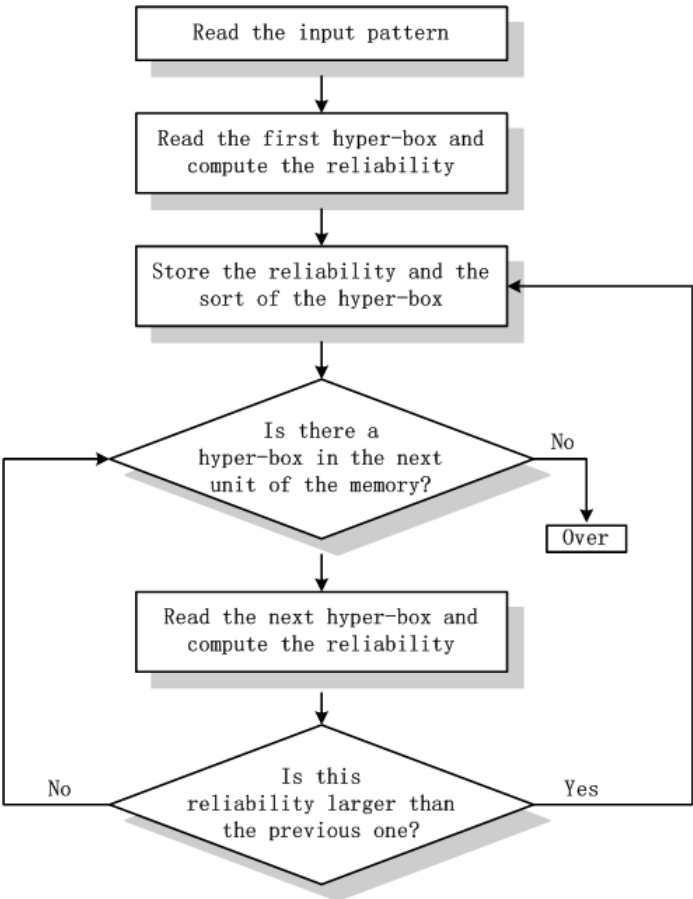
Fig. 5. The classification process

3.4   The Frame of Classification Sub-module

The classification sub-module is made of a few classification logic units which have the same structure. Fig. 6 shows a sub-module with four classification units.
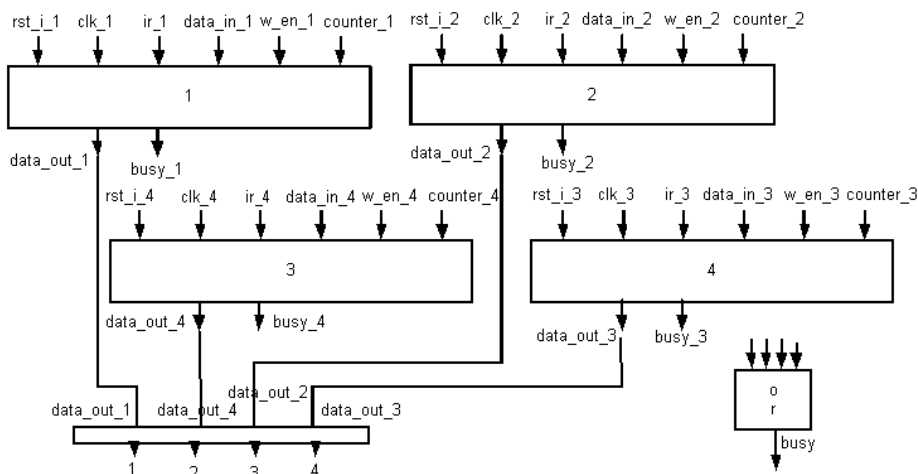
Fig. 6. The classification sub-module of the classifier

Here is the classification process of the multi-resolution combined fuzzy network classifier. Firstly, the data are distributed by the controller. Four input patterns are stored in four different registers which are in different classification logic units. Then, the controller sends the begin signal and is waiting for the response of the classification logic units. The classification logic units begin to classify data simultaneously and the four results can be got at the same time almostly. After the results are got, the controller stores them in the memory and the classification process is over. Here the "busy" signal is determined by all of the classification logic units. Whenever all the "busy" signals of the classification logic units are high, the "busy" signal of the whole classification sub-module is high.

4 Hardware Realization of the Multi-resolution Combined Fuzzy Network Classifier

A printed circuit board (PCB) shown in Fig. 7 has been designed using FPGA of Xilinx to verify the function of the multi-resolution combined fuzzy network classifier.

The input test data for verifying is divided randomly into learning sets and classification sets. The learning sets are used to train the classifier firstly, and the classification sets are used to test the classification after training. The standard data sets[16] such as four dimension IRIS data and six dimension BUPA data are taken as examples, of which 50% of four-dimensional IRIS data are selected randomly as training patterns and the other 50% are used for classification, or 75% of BUPA data for training and the rest for classification. The result of learning and classification is shown in Table 1.
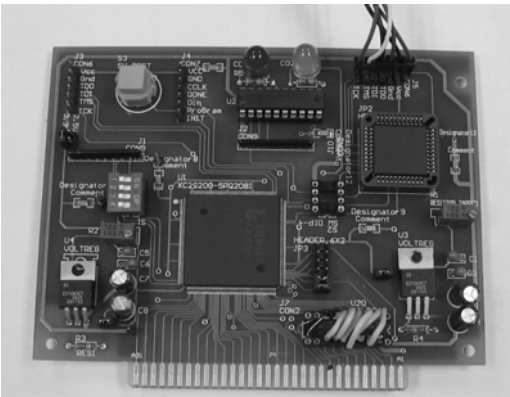
Fig. 7. The designed PCB for verifying

Table 1. The classification result realized using FPGA

Data sets	The right classification patterns in training/all training patterns	The right classification patterns in test/all test patterns
IRIS	75/75	73/75
BUPA	*254/259*	56/58

The experiment shows the astringency that the test result of the multi-resolution combined fuzzy network classifier agrees well with the simulation result. It shows good independency and extensibility.

5   Conclusion

This paper proposes an original hardware realization method of the multi-resolution combined fuzzy network. The current chip is designed with 4 classification logic units. In fact, more classification logic units can be integrated into one chip. Meanwhile, with this architecture, the chips can be cascaded as well to achieve a high speed classifier.

References

1. Bian, Z.Q., Zhang, X.G.: Patterns Recognition. Tsinghua University Publisher, Beijing (2000)
2. Ghosh, A.K., Lubkeman, D.L.: The classification of power system disturbance waveforms using a neural network approach. IEEE Transaction on Power Delivery 10, 109–115 (1995)
3. Santoso, S., Powers, E.J., Grady, W.M.: Power quality disturbance waveform recognition using wavelet-based neural classifier. I. Theoretical foundation, IEEE Transaction on Power Delivery 15, 222–228 (2000)

4. Dash, P.K., Mishra, S., Salama, M.A., Liew, A.C.: Classification of power system disturbances using a fuzzy expert system and a Fourier linear combiner. IEEE Transaction on Power Delivery 15, 472–477 (2000)

5. Youssef, A.M., Abdel-Galil, T.K., El-Saadany, E.F., Salama, M.M.A.: Disturbance classification utilizing dynamic time warping classifier. IEEE Transaction on Power Delivery 19, 272–278 (2004)

6. Urbano, J., Terashima, K., Kitagawa, H.: Skill-assist control of an omni-directional wheelchair by neuro-fuzzy systems using attendants force input. Journal of Innovative Computing, Information and Control 2, 1219–1248 (2006)

7. Shi, Y., Messenger, P., Mizumoto, M.: Fuzzy inference modeling based on fuzzy singleton-type reasoning. Journal of Innovative Computing, Information and Control 3, 13–20 (2007)

8. Bhavsar, A., Patel, H.M.: Facial expression recognition using neural classifier and fuzzy mapping. In: IEEE Indian 2005 Conference, pp. 134–383 (2005)

9. Wang, W., Ismail, F., Golnaraghi, F.: A neuro-fuzzy approach to gear system monitoring. IEEE Transaction on Fuzzy Systems 12, 710–723 (2004)

10. Simpson, P.K.: Fuzzy Min-Max Neural Networks-Part 1: Classification. IEEE Transaction on Neural Networks 3, 776–786 (1992)

11. Chen, X., Jin, D.M., Li, Z.J.: A New Kind of Fuzzy Neural Network Classifier. Electronics Transaction 30, 830–835 (2002)

12. Gabrys, B., Bargiela, A.: General Fuzzy Min-Max Neural Works for Clustering and Classification. IEEE Neural Networks 11, 769–783 (2000)

13. Meneganti, M., et al.: Fuzzy Neural Networks for Classification and Detection of Anomalies. IEEE Neural Networks 9, 848–861 (1998)

14. Chen, X., Jin, D.M., Li, Z.J.: Recursive Training for Multi-Resolution Fuzzy Min- Max Neural Network Classifier. In: The 6th International Conference on Solid-State and Integrated-Circuit Technology (ICSICT-2001), vol. 1, pp. 131–134 (2001)

15. Hennessy, J.L., Patterson, D.A.: Computer Organization & Design-The Hardware/software Interface. Morgan Kaufmann Publishers, San Francisco (1998)

16. Blake, C., Keogh, E.: UCI repository of machine learning databases, http://www.ics.uci.edu/~mlearn/MLRepository.html

An Implementation on Extracting H.264/AVC Compressed Data from Flash Video

Xinchen Zhang, Xiaoming Zhong, and Yanzi Huang

College of Physical Science and Technology,
Central China Normal University, Wuhan,
430079 Hubei, P.R. China
zhangxc@phy.ccnu.edu.cn

Abstract. In order to process, compare and contrast the video quality or analyze the video comment, we need to get the pure video data from the FLV file. This paper wants to describe our software implementation and research in the field of video data extracting from FLV file to H.264/AVC pure video. The structure and data bit syntax are introduced in the first part of the paper. Then an efficient soft-program design and instruction are presented especially including AVC compressed video data. Through these experiments, the software of extracting the FLV video data as AVC standard is implemented by C++ program, and the software is used in web video quality assessment system. Experimental results presented that the software can extract the video data correctly and efficiently. In the end of the paper, it makes the conclusion.

Keywords: H.264, AVC, FLV, Flash Video, Structure Analysis.

1 Introduction

Nowadays web videos are becoming more and more. Web videos have replace the traditional streaming media server-client application model. Customers only through the browser can quickly and easily watch the web video. The main models of streaming media services on the current network are flash video based on web browser and stream media business on P2P download technology.

There are hundreds of video file formats used all over the world, Audio Video Interleave File (avi), Flash Video File (flv), MPEG Video File (mpeg), MPEG-4 Video File (mp4), Apple QuickTime Movie (mov), and Windows Media Video File (wmv) to name a few [1]. The format defines how the video and audio are compressed, and how the two streams are packed in a single file. A format's quality-to-filesize performance is important. Its support across device too, especially given the recent rise of mobile devices (iphone, Android) with video capabilities. Because of its simple file structure, the flash video becomes the most improtant format in web video, Its relatively small size compared to other video file formats, and its popularity in video-hosting websites [2].

In this paper, we first introduce the structure and data syntax of the FLV file and video tag. In section 3, an implement design by program is presented. Then, we discuss the experiments results of extracting the AVC video. Finally, it concludes the work of the paper.

2   File Data Structure Analysis on Flash Video (FLV)

The document named "Video File Format Specification (Version 10)" [3] and [4], which published by Adobe, provides technical format information for the video file formats supported by Adobe Flash Player software—FLV and F4V.

An FLV file encodes synchronized audio and video streams. The audio and video data within FLV files are encoded in the same way as audio and video within SWF files. Starting with SWF files published for Flash Player 6, Flash Player can exchange audio, video, and data over RTMP connections with the Adobe Flash Media Server.

2.1   FLV File Structure

In the FLV video file format, each tag type is in an FLV file constitutes a single stream. There can be no more than one audio and one video stream, synchronized together, in an FLV file. An FLV file cannot define multiple independent streams of a single type.
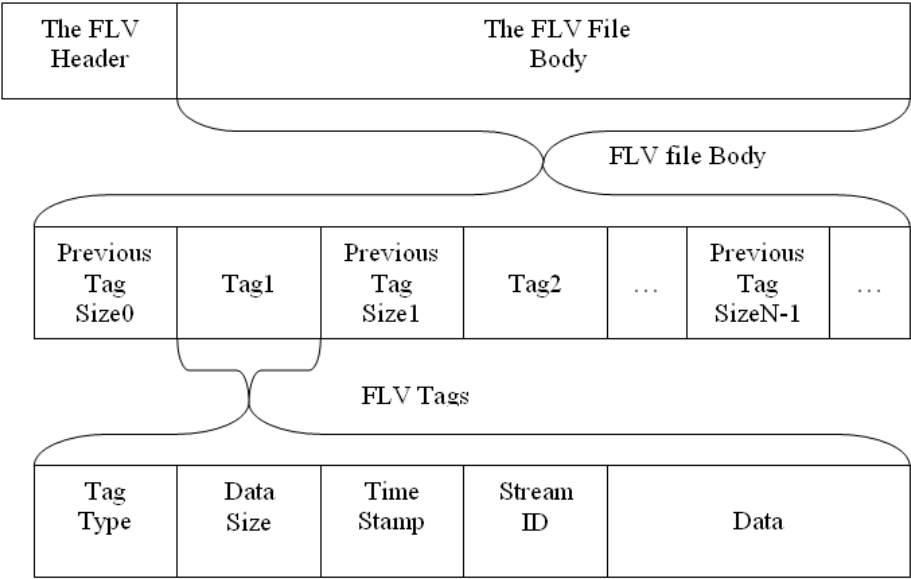
Fig. 1. The structure of the FLV file shows FLV file body and FLV tags data

The FLV file starts with the FLV File headers then metadata tag, which named as the FLV file body (data that describe the FLV), then interleaved audio, video and script or other reserved tags (actual data). The structure of the FLV file is shown in Fig.1.

From the file structure, we could concern that the FLV files usually have smaller file sizes compared to all the other formats. Using hexadecimal editor software "UltraEdit-32", which is a binary and hexadecimal file editing utility for Windows, it

was found out that the file format of FLV (Flash Video) is very simple. Fig.2 shows the starting part of a FLV file (Header) opened by the Hexadecimal Editor. The data addressed from 0x00 to 0x08 on the red line is the FLV Header data, which includes signature, version, typeflag, dataoffset. The data addressed from 0x09 to 0x0c on the blue line is the PreviousTagSize0, which means the previous tag length if it before the tagN. The data starting from 0x0d is tag1 of this FLV file, which length is defined by the DataSize parameter in the tag.

Fig. 2. The Starting Part of an FLV File opened by a Hexadecimal Editor

2.2   Video Tag

Video tags are similar to the VideoFrame tag in the SWF file format, and their payload data is identical. Video tag is indicated by the type of one FLV tag, if the tag type code is 0x09.

In each video tag, the bit data is let on the method as the syntax table describing, which is shown in Table 1.

Table 1. Video data syntax in the FLV video tag [4]

Field	Type	Comment
FrameType	UN[4]	1: keyframe (for AVC, a seekable frame)
		2: inter frame (for AVC, a nonseekable frame)
		3: disposable inter frame (H.263 only)
		4: generated keyframe (reserved for server use only)
		5: video info/command frame
CodecID	UB[4]	1: JPEG (currently unused)
		2: Sorenson H.263
		3: Screen video
		4-5: On2 VP6, or with alpha channel
		6: Screen video version 2
		7: AVC
VideoData	UI8 or Video frame payload	If CodecID == 2 {H263VIDEOPACKET}
		If CodecID == 3 {SCREENVIDEOPACKET}
		If CodecID == 4 {VP6FLVVIDEOPACKET}
		If CodecID == 5 {VP6FLVALPHAVIDEOPACKET}
		If CodecID == 6 {SCREENV2VIDEOPACKET}
		if CodecID == 7 {AVCVIDEOPACKET}

If the value of the codeID is 7, the video data is compressed by using H.264/AVC standard. H.264/AVC or MPEG-4 Par10 is a standard for video compression, and is

currently one of the most commonly used formats for recording [5]. Because H.264 has the best performance than existed standard, most video web site in China, such as "Tudou"[6], "Youku"[7], "Sina", select H.264/AVC using as video data packet.

The bit syntax of AVC video which is the payload in FLV file is shown in Table 2.

Table 2. AVCvideo packet data syntax [4]

Field	Type	Comment
AVCPacketType	UI8	0: AVC sequence header
		1: AVC NALU
		2: AVC end of sequence
CompositionTime	SI24	if AVCPacketType == 1{Composition time offset}
		Else {0}
Data	UI8[n]	if AVCPacketType == 0 {AVCDecoderConfigurationRecord}
		else if AVCPacketType == 1 {One or more NALUs (can be individual slices per FLV packets)}
		else if AVCPacketType == 2 {Empty}

In the Table.2, the composition times is described in ISO 14496-12, 8.15.3 section [8]. The offset in an FLV file is always in milliseconds.

The syntax of the composition times is as following presentation.

```
aligned(8) class CompositionOffsetBox
  extends FullBox('ctts', version = 0, 0) {
    unsigned int(32) entry_count;
    int i;

  for (i=0; i < entry_count; i++) {
      unsigned int(32) sample_count;
      unsigned int(32) sample_count;
      unsigned int(32) sample_offset;
      unsigned int(32) sample_offset;
  }

}
```

The description of AVCDecoderConfigurationRecord can be found at ISO 14496-15, 5.2.4 section [9]. This contains the same information that would be stored in an avcC box in an MP4/FLV file. The syntax is as following.

```
aligned(8) class AVCDecoderConfigurationRecord {
  unsigned int(8) configurationVersion = 1;
  unsigned int(8) AVCProfileIndication;
  unsigned int(8) profile_compatibility;
  unsigned int(8) AVCLevelIndication;
  bit(6) reserved = '111111'b;
  unsigned int(2) lengthSizeMinusOne;
  bit(3) reserved = '111'b;
  unsigned int(5) numOfSequenceParameterSets;
  for (i=0; i< numOfSequenceParameterSets; i++) {
    unsigned int(16) sequenceParameterSetLength ;
    bit(8*sequenceParameterSetLength)
```

```
  sequenceParameterSetNALUnit;
  }
  unsigned int(8) numOfPictureParameterSets;
  for (i=0; i< numOfPictureParameterSets; i++) {
    unsigned int(16) pictureParameterSetLength;
    bit(8*pictureParameterSetLength)
  pictureParameterSetNALUnit;
  }

}
```

3   Program Design and Implementation

Based on the results of the discussion on the FLV structure and data syntax, such as
the file header, file data tag, video and audio tags, a C++ program of pure AVC video
extracting has been developed and it has been integrated into the web video quality
assessment device on 3G TDS-CDMA system.
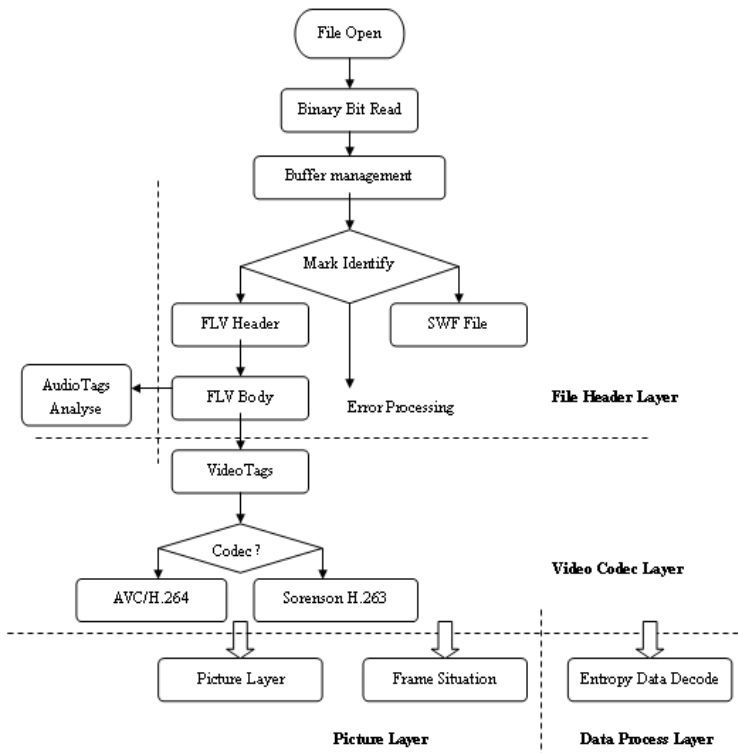
Fig. 3. Diagram of Data Processing in Extracting Stream Handler

The software includes four function layer parts. There are stream file analysis layer, video tag analysis layer, picture frame analysis layer and detail data analysis layer. The top layer achieves to decide which format stream file is used and to verify the FLV file Header is right or not. The second layer judges the video data's frame code type, get the length and offset of the frame and the data is by which compression standard. The third layer can get the parameters of the coded picture, such as spatial, temporal and bitrate information. The last layer accomplishes entropy decoding, syntax translating, MV, QP, DC parameters selecting.

In our design, the four component layers handle the different analysis functions. This software, which is implemented by C++ on Microsoft Visual Studio 2005, is the key component of the web video quality assessment system, with picture quality visual sense assessment and network transport performance component. The extracting and analysis soft program's block diagram is shown in Fig.3.
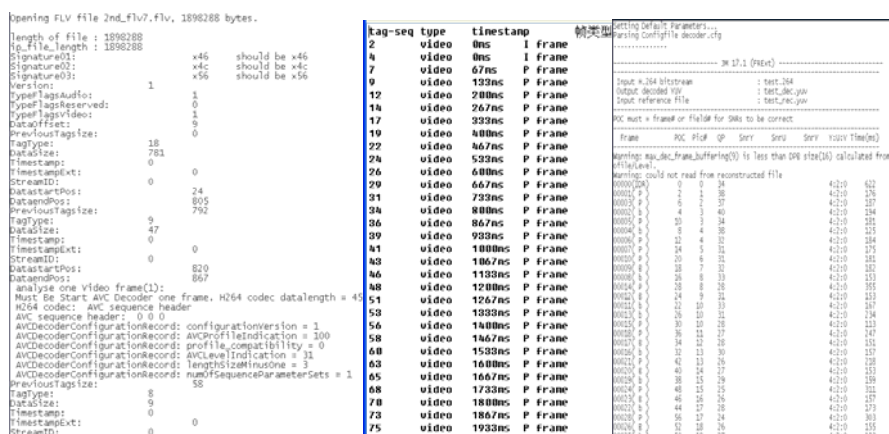

Fig. 4. The Running Results of Extracting Video Stream

4   Running Results

Fig.4 shows the program running results. The left picture gives us the output recording of the analysis process. The middle one records each frame picture should be playing at which time and frame type. The right picture shows the output information of H.264 decoder (JM17.1), which means the decoder, can decode the extracted pure video data.

In our experiments, the average extraction speed is 281 frames per second in CIF format (352*288 pixels).

5   Conclusion

The analysis of FLV file structure and the extraction of AVC video are discussed in this paper. It explores the details processing of the soft program implementation. The results indicate that the extraction method is efficient and correct and the soft can be

used for the system which needs to get the video data to process or analyze. Although it is for Flash web video application, it can be extended to use in other application with FLV file.

References

1. The File Extensions Resource, http://www.fileinfo.com/filetypes/video
2. Mozo, A.J., Obien, M.E., Rigor, C.J., et al.: Video Steganography using Flash Video (FLV). In: I2MTC 2009, May 5-7, pp. 648–655. IEEE Press, Singapore (2009)
3. Adobe Systems Incorporated: swf_file_format_spec_v10. published (November 2008)
4. Adobe Systems Incorporated: Video File Format Specification version 10. published (November 2008)
5. ITU-T Rec. H.264 | ISO/IEC 14496-10 AVC, Document JVT-G050, 8th Meeting: Geneva, Switzerland (May 2003)
6. http://www.tudou.com
7. http://www.youku.com
8. International standard, ISO/IEC 14496-12: Information technology — Coding of audio-visual objects —Part 12: ISO base media file format (2005)
9. International standard, ISO/IEC 14496-15: Information technology — Coding of audio-visual objects — Part 15: Advanced Video Coding (AVC) file format (2004)

Analysis of Construction Schemes with Varied Data Re-modulation Formats for Centralized Lightwave WDM-PON Employing Super-Continuum Light Source

Nai Wei[1], Dong Decun[1], Zhang Weifeng[2], Chen Shuai[1], and Zheng Wenyi[1]

[1] School of Transportation Engineering, Tongji University
Shanghai, 201804, China
[2] China Mobile Communications Corporation (CMCC),
Beijing, 100032, China
niwei.tongji@gmail.com

Abstract. This paper proposes a novel cost-effective construction scheme for centralized lightwave wavelength-division-multiplexing passive-optical-network (WDM-PON). In optical line terminal (OLT), it employs a single super-continuum light source for the whole system that the downstream data can be modulated in each wavelength channel; and at optical network unit (ONU), it uses part of the downstream as carrier to re-modulate upstream data. The scheme reduces the optical sources used in OLT and simplifies the structure of ONU, so that the construction costs can be greatly solved. Considering that the changing of modulation formats for both downstream and upstream data can have great effects on system performance, this paper also deeply analyzes those WDM-PON construction schemes of various downstream and upstream modulation formats. By simulation, the relationship between receiving power and bit error rate (BER) of 10Gb/s downstream and 10Gb/s upstream back-to-back and 20km system of all schemes are analyzed.

Keywords: WDM-PON, super-continuum light source, centralized lightwave, re-modulation, cost-effective.

1   Introduction

The function and the performance of Internet data service has improved a lot during past decades, and nowadays users require even higher transmission speed and even larger bandwidth, nevertheless, the "last mile" problem is just the bottleneck which limits the network speed and bandwidth. In this context, WDM-PON which has huge bandwidth capacity, is becomming the dominating development trend in future optical access area [1-3]. Currently, novel construction schemes for cost-effective centralized lightwave WDM-PON are proposed [1-4], those schemes can split part of the downstream power in ONU and use it as carrier to re-modulate upstream, so as to save local optical sources or amplifiers other schemes employ [5-6] and reduce construction costs. However, most researches now only focus on saving the costs in ONU but make little of light source cost saving in OLT; and only focus on one set of

data modulation format for re-modulation but lack of comparison for alternative modulation formats.

This paper proposes a novel cost-effective construction scheme for centralized lightwave WDM-PON which employs only a single super-continuum light source which can also produce multi wavelength channel as well as separated light sources or laser array for data modulation use. In condition of this, this paper also deeply analyzes various sets of data re-modulation formats that possible for centralized lightwave WDM-PON and does some comparison. By simulation on software VPI Transmission Maker, the performance of several construction schemes with a system transmission bit rate at 10Gb/s for both downstream and upstream, and varied re-modulation formats such as FSK-OOK, DPSK-OOK, DQPSK-OOK, DPSK-FSK are analyzed separately and compared with each other.

2   System Structure

The basic structure of proposed WDM-PON system has been shown in Fig.1. The whole system has OLT, Optical Distribution Node (ODN) and ONU three parts. In OLT, a super-continuum light source generator is used to produce multi wavelength channel optical carriers, then the optical carrier in each channel is modulated by DQPSK DPSK, or FSK downstream data, after that, all the signals are combined together as a WDM signal by a MUX and then sent to the SMF for downlink. In ODN, a DeMUX is used for WDM signal separation, and the downstream signal separated in each wavelength is then sent to the corresponding ONU. In ONU, part of the downstream power is separated by a coupler for receiving, and the left is re-used as carrier for re-modulating OOK or FSK upstream. The upstream transmitted from all the ONUs in the same cell are combined together again buy the MUX in ODN then sent to OLT after transmission in uplink SMF.
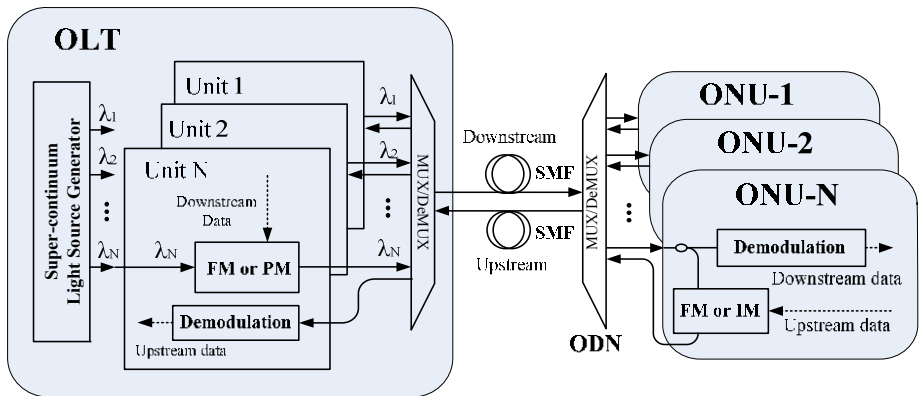

Fig. 1. System structure of proposed WDM-PON employing super continuum light source (FM: frequency modulator, PM: phase modulator, SMF: single mode fiber, IM: intensity modulator)

Although the upstream signal is modulated on the optical carrier that has downstream information, its demodulation in OLT would not be affected much by the downstream data for the modulation format is different, so as the parameters which carry downstream and upstream are mutual independent. Thus, when the upstream signal is received in OLT, using the corresponding demodulation method as how the upstream data is modulated in ONU is enough for demodulating. The OLT and ODN are connected by two SMF fibers for bidirectional transmission, and the link length is set at 20km for the link of real business-oriented system would be no more than that.

3   Performance Analysis

This part use DPSK-OOK re-modulation format which is shown in Fig. 2 as an example to depict the simulation system setup. In OLT, a super-continuum light source generator combined by an ultra-short pulse generator with a frequency at 50GHz, an optical Gaussian pulse generator with central wavelength at 1552.3nm, an optical fiber with the length at 7.783km and dispersion coefficient at 20 ps/(nm·km), a comb filter and an attenuator is set to generate 10 channel optical carrier. First use ultra-short pulses force the optical Gaussian pulse generator to generate high power optical pulses, then put the pulses into the fiber whose core area is only 20μm^2 to use the non-linear effect via their transmission to generate super-continuum. After getting the super continuum, the comb filter and the attenuator are used for shaping out 10 peaks from the super-continuum and make their power flat with each other. By reasonably set the frequency of ultra-short pulses and the power of optical Gaussian pulse generator, 10 output peaks at a power at -1dBm with 0.4nm difference in their central wavelengths can be generated. Thus, multi-channel optical carriers are acquired by just a single optical pulse generator. The analysis data in this paper have been acquired from the 6th channel whose central wavelength is 1552.52nm.
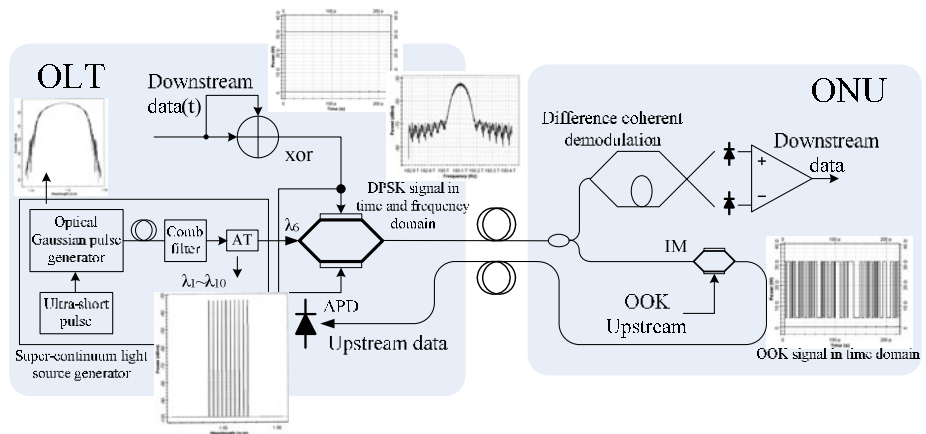

Fig. 2. Simulation system setup for DPSK-OOK re-modulation scheme (AT: attenuator, xor: exclusive or, APD: avalanched photo diode)
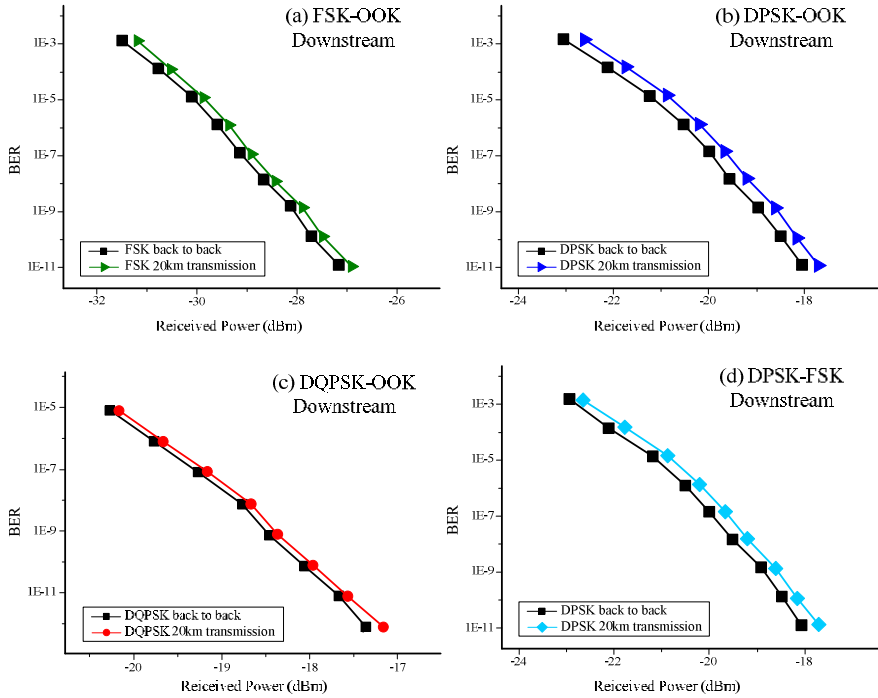
Fig. 3. BER vs received power for downstream in different re-modulation formats' case. (a) FSK-OOK re-modulation case, (b) DPSK-OOK re-modulation case, (C) DQPSK-OOK re-modulation case, (d) DPSK-FSK re-modulation case.

After acquiring the optical sources, a dual-arm Mach-Zehnder modulator (MZM) is used for modulating downstream data in each channel. By electric "exclusive or" calculation, 10Gb/s PRBS with the length 2^{23}-1 downstream is converted to difference signal. Then let the difference signal to modulate both arm of the MZM. By adjusting the drive voltage and the bias voltage, the MZM can produce 10Gb/s optical signal with phase difference at π between 1 and 0 bits [7], namely the optical DPSK signal. The bidirectional transmission link is combined by two 20km standard SMFs whose dispersion coefficient are 16.5ps/(nm·km) and dispersion slope are 0.08ps/nm^2 km. Fig. 3(b) shows the relationship between BER and received power for downstream signal in both back-to-back and 20km transmission situation.

In ONU, an optical coupler is firstly used to separate the received optical signal into two parts, one part will be act as upstream optical carrier to modulate 10Gb/s PRBS with the length 2^{15}-1 onto it by IM, thus generate the OOK upstream; the other part will be sent to difference coherent demodulator for DPSK demodulation. A difference coherent demodulator formed by a 1bit delay M-Z interferometer and a photo detector can get the original data from the optical downstream. The downstream can be used as ideal carrier for OOK re-modulation, for the power of the optical DPSK signal stays the same in each bit slot. The relationship between BER and received power for upstream signal in both back-to-back and 20km transmission situation are shown in Fig. 4(b).
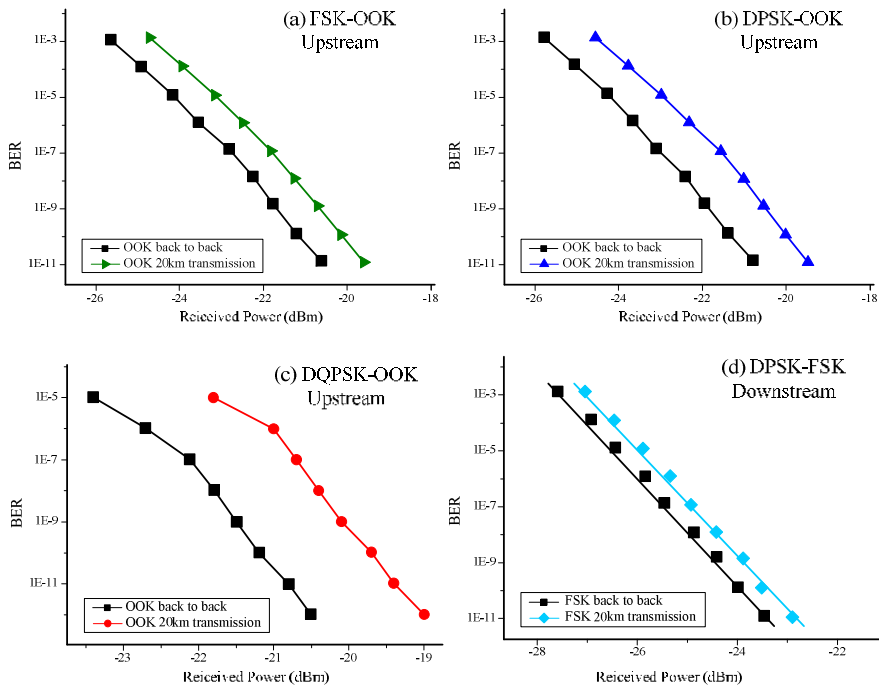
Fig. 4. BER vs received power for upstream in different re-modulation formats' case. (a) FSK-OOK re-modulation case, (b) DPSK-OOK re-modulation case, (C) DQPSK-OOK re-modulation case, (d) DPSK-FSK re-modulation case.

The relationship between BER and received power for downstream and upstream of varied re-modulation formats including FSK-OOK, DPSK-OOK, DQPSK-OOK and DPSK-FSK are shown in Fig. 3 and Fig. 4. From the analysis, it can be seen that due to the fairly short transmission distance, the downlink has not been affected a lot by dispersion problem no matter which modulation format is used. It only needs to pay a power penalty from 0.2dBm to 0.3dBm to achieve 10^{-9} BER compared with back-to-back situation. By comparison, phase modulation needs more power to get a same BER than frequency modulation, that's because the phase signal would suffer more serious non-linear effect, especially the intra-channel four wave mixing (IFWM) [8].

For upstream signal, the OOK re-modulation is done in ideal optical extinction ratio [3], and the power penalty to get 10^{-9} BER are around 1.3dBm compared with back-to-back situation, and 1.5dBm for DQPSK-OOK re-modulation case. It can be concluded that although phase or frequency modulation optical signal can be used as ideal carrier in theory, but after several kilometers' transmission there would be noise for OOK signal caused by FM or PM signal after all, and the more complicated signal used in downstream (such as DQPSK signal in this paper), the more power penalty would pay in upstream demodulation. If use FSK as re-modulation format, it only costs 0.5dBm to get 10^{-9} BER compared with back-to-back situation. So it can be draw that FSK optical signal would be affect less in the transmission link and it has relatively higher receiving sensitivity.

Those scheme discussed in this paper would meet the need of real business-oriented system when the super-continuum optical source produces multi channel optical carrier with the power at -1dBm, and it is without doubt that super-continuum optical source is simpler in construction and has higher flexibility for future system upgrade than separated lasers or laser array. And when it comes to re-modulation formats, DPSK-OOK case needs the least transmit power in OLT, and DPSK-FSK case has been affected least by the transmission link. Consider about the trend of improvement for the network capacity and adding multi-services [1-4], the OOK re-modulation format would be more flexible in network upgrade.

4   Conclusion

The advantage of the proposed cost-effective construction scheme for centralized lightwave WDM-PON employing super-continuum optical source is analyzed in this paper. The scheme with various re-modulation formats has also been deeply analyzed and compared based on simulation results. Construction suggestions are given on consider of different user demands. Part of the research result this paper shows can be valuable for future application of centralized lightwave WDM-PON and can be helpful in solving the "last mile" problem.

References

1. Yu, J., Akanbi, O., Luo, Y., et al.: A novel WDM-PON architecture with centralized lightwaves in the OLT for providing triple play services. In: Optical Fiber Communications Conference and National Fiber Optical Engineering Conference, San Diego (2007)
2. Zhang, W., Xin, X., Zhang, Q., et al.: Centralized light-wave WDM-PON employing DQPSK downstream and OOK remodulated upstream signals. The Journal of China Universities of Posts and Telecommunications 17(4), 125–128 (2010)
3. Nai, W., Dong, D., Xin, X., et al.: Centralized Lightwave WDM-PON Employing DPSK/FSK Orthogonally Modulated Downstream and OOK Re-modulated Upstream. In: 2nd International Conference on Wireless Network and Information Systems, Chongqing (2010)
4. Deng, N., Chan, C., Chan, L., et al.: A WDM Passive Network with Centralized Light Sources and Multicast Overlay. IEEE Photonics Technology Letters 20(2), 114–116 (2008)
5. Moon, J., Choi, K., Mun, S., et al.: An automatic wavelength control method of a tunable laser for a WDM-PON. IEEE Photonics Technology Letters 21(5), 325–327 (2009)
6. Ji, H., Yamashita, I., Ktayama, K.: Bidirectional transmission of downstream broadcast and upstream baseband signals over a single wavelength in WDM-PON using mutually injected FPLDs and RSOA. IEEE Photonics Technology Letters 20(20), 1709–1711 (2008)
7. Zhao, J., Xin, X., Yu, C., et al.: Optimization of key parameters in 622-Mb/s Amplitude shift keying labeled 40-Gb/s retnrn to zero Differential Phase Shift Keying Optical Switching Network. Semiconductor Photonics and Technology 14(1), 17–21 (2008)
8. Liu, F., Su, Y.: DPSK/FSK hybrid modulation format and analysis of its nonlinear performance. Journal of Lightwave Technology 26(3), 357–364 (2008)

Design of Optical Raindrop Spectrometer Based on Embedded Microcontroller[*]

Shangchang Ma, Qian Zhu, Bifeng Yang, Yanjun Zhan, and Sujuan Zhang

Chengdu University of Information Technology (CMA. Key Laboratory of Atmospheric Sounding), NO.24, Block 1, Xuefu Road, Chengdu 610225, P.R. China
mscjs@cuit.edu.cn

Abstract. Raindrop spectra distribution plays an important role in soil erosion, rainfall intensity, rainfall type, and so on. Traditional measurement of raindrop size distribution is based on filter paper, which can not achieve real-time, rapid and accurate observation. This paper proposes an optical raindrop spectrometer, which is designed based on embedded microcontroller. An embedded microcontroller is set as the control center of the system, combined with optical detection technology, high-speed signal acquisition technology, digital signal processing technology and embedded software design technology to realize online observation of raindrop size and falling speed, compute spectral distribution, draw distribution figures. According to raindrop size distribution, rainfall intensity and rainfall is calculated. Research production is also the basis for future research of precipitation type identification.

Keywords: Raindrop spectra, raindrop size, photo detector, signal processing, embedded microcontroller.

1 Introduction

Raindrop spectra (also called raindrop size distribution) is the number distribution of raindrops in unit volume according to their diameters, it is comprehensive result of raindrop formation, falling, growth, crushing and evaporation process. Raindrop spectra can be described by M-P distribution [1], logarithmic normal distribution [2] and Gamma distribution [3] functions, one of the most commonly used is M-P distribution, and distribution function is shown as

$$n(d) = n_0 \times e^{-\lambda d} \tag{1}$$

M-P distribution is proposed by Canada meteorologists Marshall and Palmer in 1948. In Eq.(1), $n(d)$ is spectral distribution density function, refers raindrop number contained in unit volume, also called concentration, d is raindrop diameter, n_0 and λ are constants relate to precipitation property.

Traditional technologies for measuring raindrop size distribution are the use of filter paper, flour pellets, and raindrop camera. Due to the lack of automatic measuring and recording devices, these methods can not achieve the requirements of real-time, precision, reliability, and so on. This paper proposes an optical raindrop spectrometer, which is designed based on embedded microcontroller. In the system, an embedded microcontroller is set as the control center, combined with optical detection technology, high-speed signal acquisition technology, digital signal processing technology and embedded software design technology, online observation of raindrop size and falling speed are realized, spectral distribution is computed and graphic expressed. According to raindrop size distribution, rainfall intensity and rainfall is calculated. Research production is also the basis for future research of precipitation type identification.

2   Principle of Optical Raindrop Spectrometer

Scientists from many fields of research have been interested in measuring the size and velocity of particles for a long time. A large number of drop sizing instruments are described in literatures [4] [5] [6]. They can be divided into several groups, depending on the physical principle used: groups based on impact techniques, imaging techniques or single particle extinction.

Instruments in the third group, also known as optical drop counters, are based on photoelectrical detection technology, they offer the possibility of measuring each drop's diameter and fall velocity [7] [8]. The principles of these instruments are illustrated in Fig.1.
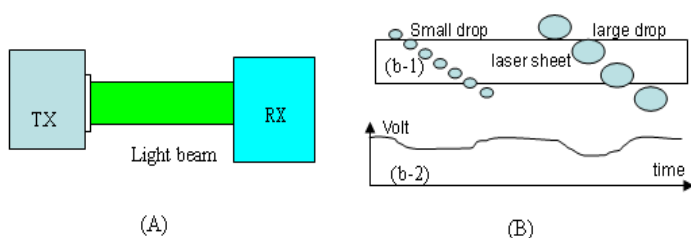

Fig. 1. Principle of optical raindrop spectrometer. (A) Illustrate figure of photoelectric system; (B) Signals while drops falling through the light beam. (b-1) Small and large drops, (b-2) raw signal from the receiver.

In Fig.1, transmitter (TX) yields a parallelepiped light beam. This beam is focused on a photodiode (in receiver RX) which generates an electrical signal. Assuming the constant intensity of the transmitted light beam, the quiescent current of the photodiode is also a constant in the absence of drops, therefore the receiver produces a DC voltage signal. Drops passing through the light beam cause a decrease of this signal by extinction and therefore a short reduction of the amplitude of the signal, the voltage decrease depend linearly on the fraction of the light beam blocked. Fig.1 (B) schematically shows the signals of two drops of different size. The amplitude of the signal deviation is a measure of drop size; the duration of the signal allows an estimate of drop velocity.

It is difficult to determine the drop parameters, i.e., diameter and velocity, from the raw signal in Fig.1 (b-2), especially in condition of low signal to noise ratios for small drop size. To overcome this problem, many researchers focus their attention on algorithms studying: pulse shape analytical method for start and end point of signal decrease detection; effective peak-finding algorithm for determining the inter-drop separation; threshold selection method to guarantee effective measure of small drops; drop size and velocity spectrum analysis, and so on [9] [10]. The authors studied and simulated the signal while raindrops falling through the light beam [11], the amplitude of the signal can be calculated by:

$$f = F \times (1 - \frac{s}{S})$$
(2)

In Eq.2, F is the amplitude of the signal without raindrop falling through the light beam; S and s is the total area of cross section of the light beam and area of cross section of part of the raindrop which in the light beam, respectively.

3   Design of Optical Raindrop Spectrometer

Principle of the optical raindrop spectrometer is shown as Fig.1, which consists of two parts: infrared laser signal generating head, infrared laser signal receiving and processing system, the distance between the two modules is about 30cm. Infrared laser signal generating head produce infrared laser sheet with 7.1KHz period and 785nm wavelength. Size of the laser sheet is about 30mm x 20mm x 1mm. Key technology of this module is guaranteeing the laser energy of the sheet with uniform distribution as far as possible which is the basis of exact measurement of raindrops information.
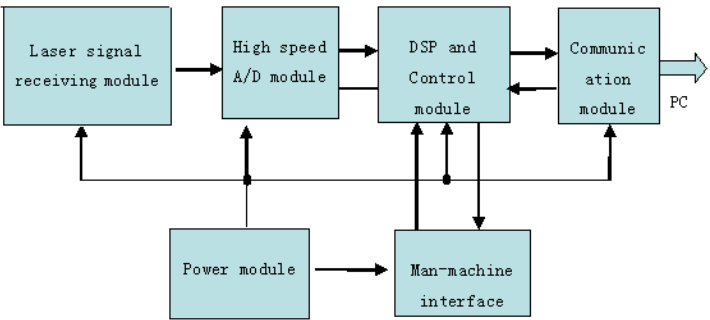

Fig. 2. Structure of laser signal receiving and processing system

Structure diagram of infrared laser signal receiving and processing system is is shown in Fig.2, which receiving laser signals, perform specific DSP algorithms, computing the raindrops size and falling velocity distribution, and then distinguish rainfall patterns, calculation rainfall intensity and volume. This system is also realize human-machine interface and other kinds of control function.

Contrast experiments are done between the experimental prototype and German OTT company's laser raindrops spectrometer in the comprehensive meteorological observation field of Chengdu university of information technology. Observation result of big raindrops above 1.2mm has good uniformity, but little raindrops cannot achieve correct observation. Further improvement of overall design is need to achieve better observation results, including mechanical system, optical systems, electronic systems, DSP algorithm, and so on.
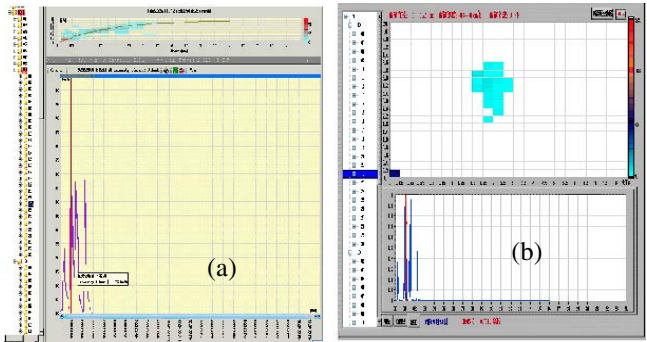

Fig. 3. Experimental result one: observed on September 22, 2010. (a) observed by OTT raindrop spectrometer; (b) observed by instrument described in this paper.
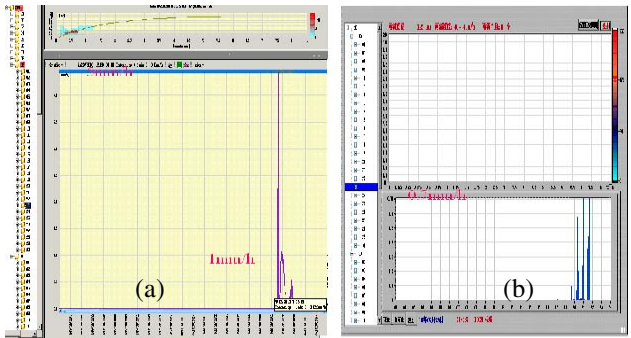

Fig. 4. Experimental result one: observed on September 23, 2010. (a) observed by OTT raindrop spectrometer; (b) observed by instrument described in this paper.

4   Conclusion

This paper proposes an optical raindrop spectrometer design program, which is based on embedded microcontroller, and combined with optical detection technology, high-speed signal acquisition technology, digital signal processing technology and embedded software design technology. The equipment can realize online observation of raindrop size and falling speed for raindrops above 1mm, but can not for little raindrops, which need to further research.

References

1. Marshall, J.S., Palmer, W.M.: The dist ribution of raindrops with size. J. Meteor. 5, 165–166 (1948)
2. Levin, L.M.: On t he size dist ribtuion function for cloud droplet s and rain drops. Dokl. Alad. Naul. SSSR 94, 1045–1053 (1954)
3. Ulbrich, C.W.: Natural variations in t he analytical form of the raindrop size distribution. J. Climate Appl. Meteor. 22, 1764–1775 (1983)
4. Grossklaus, M., Uhlig, K., Hasse, L.: An Optical Disdrometer for Use in High Wind Speeds. Journal of Atmospheric and Oceanic Technology 15(4), 1051–1059 (1998)
5. Hauser, D., Amayenc, P., Nutten, B.: A New Optical Instrument for Simultaneous Measurement of Raindrop Diameter and Fall Speed Distributions. Journal of Atmospheric and Oceanic Technology 1,3, 256–269 (1984)
6. Hamad, F.A., Pierscionek, B.K., Bruun, H.H.: A dual optical probe for volume fraction, drop velocity and drop size measurements in liquid-liquid two-phase flow. Measurement Science and Technology 11(9), 1307–1318 (2000)
7. Everest, D.: Simultaneous Measurements Of Drop Size And Velocity In Large-Scale Sprinkler Flows Using Laser-Induced Fluorescence And Mie Scattering. Journal of Flow Visualization and Image Processing 10(3-4) (2003)
8. Burguete, J., Playan, E., Montero, J., Zapata, N.: Improving Drop Size And Velocity Estimates Of An Optical Disdrometer: Implications For Sprinkler Irrigation Simulation. Transactions of the ASABE 55, 2103–2116 (2007)
9. Montopoli, M., Marzano, F.S., Vulpiani, G.: Analysis and Synthesis of Raindrop Size Distribution Time Series From Disdrometer Data. IEEE Transactions on Geoscience and Remote Sensing 46, 466–478 (2008)
10. Denby, B., Gole, P., Taniewicz, J.: Structured neural network approach for measuring raindrop sizes and velocities. In: Proceedings of the IEEE Signal Processing Society Workshop, vol. 31, pp. 567–576 (1998)
11. Ma, S.C., Yang, B.F., Zhan, Y.J., He, J.X., Wang, B.Q.: Signal Simulation for Optical Spherical Drop Counting. In: International Conference on Information Technology and Computer Science, vol. 2, pp. 146–150 (2009)

Integrated Fault Diagnosis Method of Mobile Robot

Liu Yutian[*] and Chen Jungan

Department of Electronic and Information Engineering,
Zhejiang Wanli University, Ningbo, 315100, China
`lyt808@163.com`

Abstract. An Integrated fault diagnosis method of mobile robot is proposed. The movement states of mobile robot are classified to static state, rectilinear movement state, and three kinds of turning states. Integrating Kalman filters and expert system, the proposed fault diagnosis method discusses several modes of faults in the corresponding movement states. According to the probability of different fault modes, the faults can be detected. Compared with other fault diagnosis methods, the integrated fault diagnosis method improves the capability of avoiding the appearance of misdiagnosing and missed diagnosis. This proposed method has been implemented on a mobile robot and the simulation results show the effectiveness and superiority of the method.

Keywords: mobile robot, integrated fault diagnosis, movement states, particle filter.

1 Introduction

After more than 30 years development, fault diagnosis technology have been one of the most important and hot problems in the area of artificial intelligence. Although a mass of theories and methods have been achieved, there are many problems[1-8], to sum up, focusing on the following aspects: diagnosis knowledge acquisition, uncertainty in diagnosis procedure, the learning ability, the self-adaptability. The main causes is, the imperfect of the existing fault diagnosis methods, such as difficulty of knowledge acquirement in expert system, weak interpreting ability, and the complexity of diagnosis objects for its difficulty to determine the logic relationships between structure and function.

The above-mentioned problems can't be resolved by a single fault diagnosis method or other method mixed by several fault diagnosis methods. To solve the problems existing in intelligent fault diagnosis technology, integrating different fault diagnosis technology to develop the combination property of diagnosis system is the inevitable trend of the development of intelligent fault diagnosis technology. In this paper, Kalman filters and expert system are integrated to implement the fault diagnosising.

The remainder of the paper is organized as follows. In section 1, we give the kinematic model of mobile robot and classify the movement states and fault modes of mobile robot. In section 2, the proposed integrated fault diagnosis is discussed. In

---

section 3, the proposed fault diagnosis method is implemented to the mobile robot, and the experiment results from simulation are analyzed. Finally, conclusions are presented in section 4.

2   Movement States and Fault Modes of Mobile Robot

2.1   Kinematic Model of Mobile Robot

The kinematics of mobile robot is shown in Fig 1, and equation (1), (2) and (3). Kinematics model of mobile robot describes the motion constraints of the system and the relationship between measurements given by multiple sensors. It's important for fault diagnosis.

$$\theta_{k+1} = \theta_k + \Delta\theta \tag{1}$$

$$\omega = \frac{v_R - v_L}{L} \tag{2}$$

$$V = \frac{v_R + v_L}{2} \tag{3}$$

Here, θ denotes the rotation angle of the body. ω denotes the yaw rate of the robot. L denotes the axle length between the two wheels. v_R, v_L denote the setting speed of right and left driving wheels. V denotes the speed of the robot. v_R, v_L and ω are measured with right encoder, left encoder and gyroscope respectively.
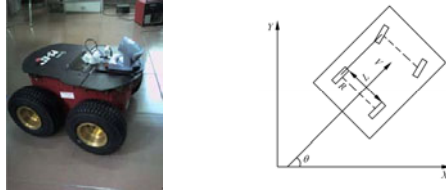

Fig. 1. The prototype of the robot and kinematic model of mobile robot

2.2   Movement States of Mobile Robots

The appearance of misdiagnosing and missed diagnosis is common in the existing fault diagnosis method. One cause is adopting the same fault diagnosis method to mobile robot in different movement states. To avoid these misdiagnosing and missed diagnosis, we proposed to classify the movement states of mobile robots[9].

According to the rates of left driver and right driver, we define five movement states, including static state, rectilinear movement state, and three kinds of turning states, represented by c1, c2, c3, c4, c5 as follows.

c1 denotes the static state: $v_R = v_L = 0$;

c2 denotes the rectilinear movement state: $v_R = v_L \neq 0$

c3 denotes the turning state 1: $v_L \neq 0,\ v_R = 0$

c4 denotes the turning state 2: $v_L = 0,\ v_R \neq 0$

c5 denotes the turning state 3: $v_R \neq v_L \neq 0$

2.3   Fault Modes

Since the fault modes are different in the different movement states of mobile robot, we should analyze the fault modes according to the movement states. All the possible fault modes in different movement states are show in Fig 2.
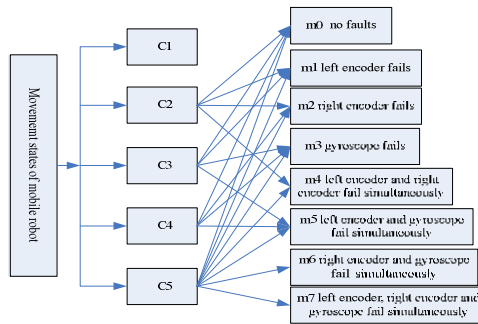

Fig. 2. Fault modes in different movement states. For example, in the C2 movement state (the rectilinear movement state), the gyroscope fault is ignored, for this fault is difficult to detect and has not big influence to the rectilinear movement state. Then, the set of fault modes should be processed in the C2 movement state include { m_0, m_1, m_2, m_4 }. In the same way, we can get the set of fault modes in the C3, C4, and C5.

3   Integrated Fault Diagnosis

3.1   Basic Principle

The basic idea of the fault diagnosis method proposed in this paper is that, using Kalman filters based fault diagnosis method to implement the preliminary diagnosis, then on the base of the preliminary diagnosis result, integrating expert system fault diagnosis module, selecting the proper knowledge in the knowledge base to inference the diagnosis result, if the diagnosis result is confirmed, the progress of fault diagnosis can be end.

3.2   Integrated Fault Diagnosis

Based on the configuration of Fig.3, the integrated fault diagnosis algorithms are summarized as follows.

- According to the characteristics data to judge the movement states of mobile robot, using Kalman filters to estimate the system state and the probability of each fault mode, giving the result.

- On the base of the result, integrating expert system fault diagnosis module, selecting the proper knowledge in the knowledge base to inference the diagnosis result, if the diagnosis result is confirmed, the progress of fault diagnosis is completed. If not, there may be misdiagnosis or new fault mode.
- If there is misdiagnosis, the process of fault diagnosis should be repeated. If there are new fault modes, the new fault modes should be added to the fault diagnosis system, and the process of fault diagnosis should be restarted, until the fault diagnosis result is derived.
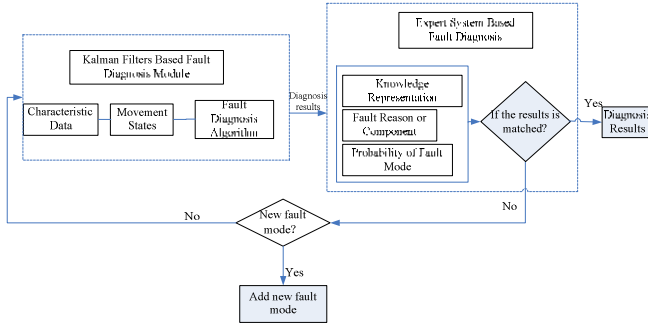

Fig. 3. The configuration of Integrated Fault Diagnosis

3.3   The Algorithm of Integrated Fault Diagnosis

3.3.1   Kalman Filters Based Fault Diagnosis Module

There are two modules in the integrated fault diagnosis. One is Kalman filters based fault diagnosis module. In this module, a group of Kalman filters is used to estimate the system state of different movement states, calculate the probability of each fault modes in the movement state. Based on the probability, the primary fault diagnosis result can be known.

In practice, the output values v_R, v_L and ω can be measured with right encoder, left encoder and gyroscope respectively. The measurement vector, system state vector, and the oprimal estimation vector are expressed as follows.

$$Z = [v_L \quad v_R \quad \omega]^T \tag{4}$$

$$X = [v_L \quad v_R \quad \omega] \tag{5}$$

$$\hat{Z} = [\hat{v}_L \quad \hat{v}_R \quad \hat{\omega}]^T \tag{6}$$

The probability of the i_{th} fault mode is defined by $p_i(t-1)$. The estimation of system state at time t-1 in the i_{th} fault mode is defined by $X_i(t-1)$. The state estimation covariance matrix at time t-1 in the i_{th} fault mode is defined by $P_i(t-1)$. Then, the probability of the i_{th} fault mode and the estimation of system state can be derived by the following algorithm.

Firstly, initialize the probability of the fault modes and system state

$$p_i(t/t-1) = \sum_{j=0}^{7} M_{ji} p_j(t-1) \tag{7}$$

$$\hat{X}_i(t/t-1) = \sum_{j=0}^{7} c_{ij} X_j(t-1) \tag{8}$$

$$\hat{P}_i(t/t-1) = \sum_{j=0}^{7} c_{ij}[P_j(t-1)+(\hat{X}_i(t/t-1)-X_j(t-1))(\hat{X}_i(t/t-1)-X_j(t-1))^T] \tag{9}$$

Here, $c_{ij} = M_{ji} \dfrac{p_j(t-1)}{p_i(t/t-1)}$

Secondly, Kalman filters is used to estimate the system state,

$$X_i(t/t-1) = A(m_i)\hat{X}_i(t/t-1) \tag{10}$$

$$P_i(t/t-1) = A(m_i)\hat{P}_i(t/t-1)A^T(m_i)+Q \tag{11}$$

$$K_i(t) = P_i(t/t-1)H_i^T(t)S_i^{-1}(t/t-1) \tag{12}$$

$$X_i(t) = X_i(t/t-1) + K_i(t)(Z_i(t/t-1) - H_i(t)X_i(t/t-1)) \tag{13}$$

$$P_i(t) = P_i(t/t-1) - K_i(t)H_i(t)P_i(t/t-1) \tag{14}$$

$$S_i(t/t-1) = H_i(t)P_i(t/t-1)H_i^T(t) + R(t) \tag{15}$$

Here, $A(m_i)$ is the system state matrix, P_i is the covariance matrix of state estimation. K_i is the gain matrix of Kalman filter. Q is the covariance matrix of system noise. R is the covariance matrix of measurement noise. H is the output matix. I is identity matrix.

Thirdly, update the probability of fault modes,

$$p_i(t) = \frac{p_i(t/t-1)L_i(t)}{\sum_{j=0}^{7} p_j(t/t-1)L_j(t)} \tag{16}$$

Here, L_i denotes the likelihood function of the i_{th} fault mode.

$$L_i(t) = |2\pi S_i(t/t-1)|^{-1/2} \times \exp[-\frac{1}{2}Z_i^T(t/t-1)S_i^{-1}(t/t-1)Z_i(t/t-1)] \tag{17}$$

According to (16), which fault modes is appeared cand be derived.Set proper threshold $\varepsilon > 0$. $p_i > \varepsilon$ means the i_{th} fault mode is detected, here i=0,1,…7.

Finally, the system state is given by

$$X(t) = \sum_{j=0}^{7} p_j(t)X_j(t) \tag{18}$$

3.3.2   Expert System Inferencing Module

Another module of integrated fault diagnosis is expert system inference module. This module is integrated to confirm the primary diagnosis result given by the above module.

The most usual knowledge representation method of fault diagnosis expert system is as follows[10-12]:

    Rule(RNO, Goal,Conclusion,RCF,[COND],Logic)
    COND(BNO,TEXT,CCF)

Here, RNO denotes the rule number, Goal denotes the goal of the reasoning, Conclusion denotes the conclusion of the reasoning. RCF denotes the creditability of the rule, expressed by ([lr,ur],[lrf,urf]). [lr,ur] denotes the minimum estimate and maximum estimate of RCF when the condition is appeared respectively. [lrf,urf] denotes the minimum estimate and maximum estimate of RCF when the condition is not appeared respectively. [COND] denotes the rule condition table. Logic denotes the logic combination of rule condition. BNO denotes the number of condition. TEXT denotes the condition. CCF denotes the creditability of condition, and CCF=[lc,uc], denotes the minimum estimate and maximum estimate respectively.

As we can see, integrated the advantages of Kalman filters based fault diagnosis and expert system based fault diagnosis, the fault diagnosis method proposed above, overcoming the shortcomings of Kalman filters and expert system, has improved the ability of fault diagnosis.

4   Simulations and Results Analysis

4.1   Experimental Equipment

To demonstrate the feasibility of the algorithm proposed here, we consider its application to mobile robot as Fig 1.The simulation experiment is implemented with Matlab, and the failure is simulated through setting the measurement value as zero.
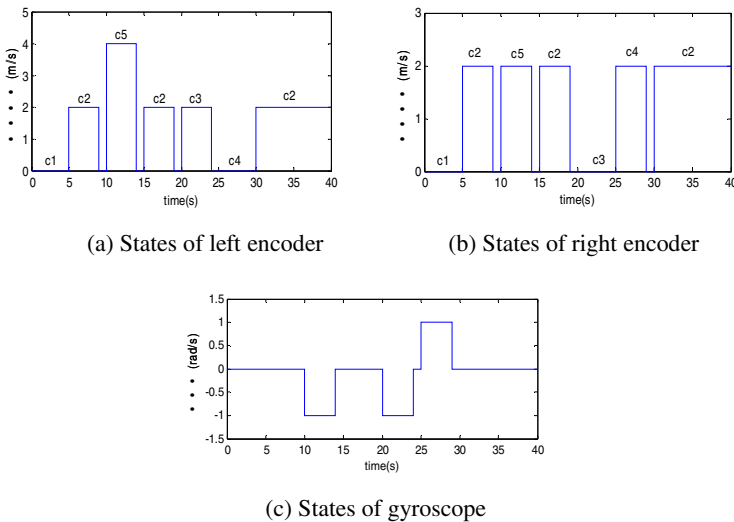

(a) States of left encoder

(b) States of right encoder

(c) States of gyroscope

Fig. 4. States of Mobile Robot

In the whole process, the mobile robot is set to work from static state, to rectilinear movement state, and three kinds of turning states. The experiment outputs of left encoder, right encoder and gyroscope are shown in Fig 4.

As show in Fig 4, the outputs of left encoder, right encoder and gyroscope is measured in ideal work condition. In the whole process, the mobile robot is set to move as follows: $c1 \rightarrow c2 \rightarrow c1 \rightarrow c5 \rightarrow c1 \rightarrow c2 \rightarrow c3 \rightarrow c2 \rightarrow c4 \rightarrow c1 \rightarrow c2$. In the initial state, the mobile robot is static, then, it works in turning state. At last, it is in rectilinear movement state.

4.2   Experiment Results

To comparing with [19], we set the same parameters as [19] to the integrated fault diagnosis algorithm. The experiment results are showed in Table 1.

Table 1. Experiment Results

No	Fault mode	Typical fault Component	Diagnosis result
1	left encoder fails	left encoder	same
2	right encoder fails	right encoder	same
3	gyroscope fails	Gyroscope	same
4	left encoder and right encoder fail simultaneously	left encoder, right encoder	different
5	left encoder and gyroscope fail simultaneously	left encoder, gyroscope	same
6	right encoder and gyroscope fail simultaneously	right encoder, gyroscope	same
7	left encoder, right encoder and gyroscope fail simultaneously	left encoder, right encoder, gyroscope	same

The experimental results show the property of the integrated fault diagnosis algorithm. To a certain extent, the integrated fault diagnosis method can avoid the misdiagnosing and missed diagnosis. The proposed fault diagnosis method wouldn't deal the normal rectilinear movement state as the fault mode 3(gyroscope fails), and wouldn't miss diagnosing the previous faults when other fault is appeared.

5   Conclusion

In this paper, we have presented integrated fault diagnosis method to a mobile robot. We classified the failures into eight modes, and defined five movement states. The integrated fault diagnosis method is implemented by Kalman filters and expert system. The simulation results on a mobile robot are presented to show that the integrated fault diagnosis method works well for several fault modes.

References

1. Wang, H.: Fault detection and diagnosis for unknown nonlinear systems: a generalized framework via neural networks. In: Proceedings of the IEEE International Conference on Intelligent Processing Systems, pp. 1506–1510 (1997)
2. Klanear, G., Skrjanc, I.: Tracking-error model-based predictive control for mobile robots in real time. Robotics and Autonomous System 55, 460–469 (2007)
3. Mehranbod, N., Soroush, M., Panjapornpon, C.: A method of sensor fault detection and identification. Journal of Process Control 15(3), 321–339 (2005)
4. Mo, Y., Xiao, D.: Hybrid system monitoring and diagnosing based on particle filter algorithm. Acta Automatic Sinica 29(5), 641–648 (2003)
5. Blom, H.A.P., Bloem, E.A.: Exact Bayesian and particle filtering of stochastic hybrid systems. IEEE Transactions on Aerospace and Electronic Systems 43(1), 55–70 (2007)
6. He, J., Qiu, J.: Integrated fault diagnosis and fault-tolerant control for nonlinear system. Journal of Mechanical Engineering 45(5), 70–78 (2009)
7. Chen, M.Z., Zhou, D.H.: Particle filtering based fault prediction of nonlinear systems. In: IFACSymposium Proceedings of Safe Process, Washington (2003)
8. Li, Z., Cai, J., Hu, S.: H_∞ fuzzy output feedback fault-tolerant control for nonlinear fuzzy systems. Journal of Southeast University (Natural Science Edition) 39(1), 32–36 (2009)
9. Liu, Y., Jiang, J.: Fault detection and diagnosis of mobile robots in multi- movement states. Chinese Journal of Scientific Instrument 28(9), 1660–1667 (2007)
10. Wu, J., Liu, C.: An expert system for fault diagnosis in internal combustion engines using wavelet packet transform and neural network. Expert Systems with Applications 36(3), 4278–4286 (2009)
11. Li, M., He, P., Meng, C.: Intelligent integrated fault diagnosis expert system of screw pump well. Journal of Harbin Institute of Technology 42(7), 1038–1041 (2010)
12. Rafiee, J., Tse, P.W., Harifi, A.: A novel technique for selecting mother wavelet function using an intelli gent fault diagnosis system. Expert Systems and Application 6(3), 4862–4867 (2009)

Delay Performance of Voice Call Continuity (VCC) for Circuit-Switched to Packet-Switched Domain Transfer

Milad Rabiei, Reza Berangi, and Mahmoud Fathi

Computer Engineering Department, Iran University of Science and Technology
rabiei.milad@gmail.com, {rberangi,mahfathy}@iust.ac.ir

Abstract. In this paper, we analyze the session initiation protocol (SIP) based delay of voice call continuity (VCC) signaling for circuit-switched (CS) to packet-switched (PS) domain transfer. For the analysis, we consider universal mobile telecommunications system (UMTS) and worldwide interoperability for microwave access (WiMAX) networks. In our delay analysis, we take into account three types of delays: transmission delay, processing delay, and queuing delay. The results show that in low channel rate networks, the main delay of VCC signaling is the delay incurred due to the transmission delay while for high channel rate networks, transmission delay is negligible and the dominant delays are processing and queuing delays.

Keywords: Voice call continuity, packet-switched domain, circuit-switched domain, delay analysis.

1   Introduction

The voice call continuity (VCC) feature is proposed by the 3rd generation partnership project (3GPP) to enable a voice call to be transferred between circuit-switched (CS) and packet-switched (PS) domains. In order to support domain transfer, the voice call continuity application server (VCC AS) is inserted into the signal path of the call at the call establishment time. In the domain transfer time, this VCC AS executes and manages domain transfer [2].

The unlicensed mobile access (UMA) architecture is compared with the VCC architecture and the delay of VCC is calculated in [6]. However, the delay is calculated by a very simple and non accurate method. The session initiation protocol (SIP) session setup delay for voice over IP (VoIP) service in 3G wireless networks is studied in [3]. The wireless link transmission is analytically modeled with and without radio link protocol (RLP) with TCP (Transmission Control Protocol) as transport layer protocol in [4].

In this paper, we analyze the SIP-based VCC signaling delay for CS-to-PS domain transfer shown in Fig. 1 for different UMTS and WiMAX channel rates. The delay consists of three parts: transmission delay, processing delay, and queuing delay.

The rest of the paper is organized as follows: In Section 2, we describe the VCC signaling flows for CS-to-PS domain transfer. In Section 3, we present our delay analysis. In Section 4, numerical results are presented. Conclusions are given in Section 5.

Fig. 1. VCC signaling procedure for CS-to-PS domain transfer (adapted from [1], [5])

2   VCC Signaling Flows for CS-to-PS Domain Transfer
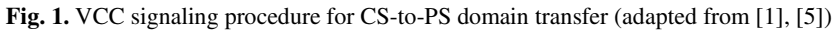
In Fig. 1, correspondent node (CN) is in a PS access network and source node (SN) which is in a CS network has originated a voice call and the call is anchored at VCC AS. The call is ongoing in the CS domain. As a result of changes in radio conditions or availability of a PS access network, the SN decides that the ongoing call in the CS domain will be transferred to the PS domain. In order to execute domain transfer, some signaling should be exchanged between SN and CN. By arriving signaling 54, PS bearer is established while CS bearer is still active. By exchanging some signaling (signaling 55 to signaling 63) between network entities, SN releases the CS bearer

and the call will be continued through PS domain. In our delay analysis, we only consider the signaling flows until the PS bearer is established. In other words, the delay of exchanging signaling 1 to signaling 54 is considered [1].

3   Delay Analysis of VCC Signaling

In this section, we analyze the delay of VCC for CS-to-PS domain transfer. The delay consists of three parts: transmission delay, processing delay, and queuing delay.

3.1   Transmission Delay

We only consider wireless link transmission delays. We consider TCP as transport layer protocol for SIP messages. In wireless systems, the RLP is used to improve the bit error rate (BER) performance. We consider channel rates of 19.2 kbps and 128 kbps for UMTS, and 4 Mbps and 24 Mbps for WiMAX. Thus, RLP is utilized on UMTS whereas it is not considered for WiMAX network due to much higher bandwidth availability [7].

We use Signaling Compression (SigComp) for SIP messages compression [9]. The compressed size of SIP messages are shown in Table 1.

The number of frames per packet (K) is required to be calculated for every specified channel rates. In UMTS, the RLP frame duration or also known as inter-frame time (τ) is assumed to be 20 ms. In case of WiMAX, the frame duration and inter-frame time is assumed to be 2.5 ms. The value of K for particular signaling messages can be calculated as:

$$\text{K} = \frac{\text{message size}}{\text{frame size}} = \frac{\text{message size(byte)}}{\text{channel rate}\left(\text{byte}/\sec\right)\times\tau(\sec)} \tag{1}$$

The *K* value of SIP messages for different channel rates are shown in Table 1.

Table 1. K Value of SIP Messages for Specified Channel Rates

SIP Message	Compressed Size (byte)	Channel Rate			
		19.2 Kbps	128 Kbps	4 Mbps	24 Mbps
INVITE	810	17	3	1	1
reINVITE	810	17	3	1	1
SIP 183	260	6	1	1	1
PRACK	260	6	1	1	1
SIP 100	260	6	1	1	1
SIP 200	100	3	1	1	1
SIP ACK	60	2	1	1	1

Transmission Delay with RLP (UMTS). We exploit the delay model for TCP packet transmission with RLP which is proposed in [4]. The transmission delay with RLP is given as:

$$D_{RLP} = D + (K-1)\tau + \frac{K(P_f(1-p))}{P_f^2} \times \left[\sum_{j=1}^{n} \sum_{i=1}^{j} P(C_{ij}) \left(2jD + (\frac{j(j+1)}{2} + i)\tau \right) \right] \qquad (2)$$

where D denotes the end-to-end frame propagation delay over the radio channel, p denotes the probability of a frame being in error, and n denotes the maximum number of RLP retransmissions. In equation (2), the probability of transmitting a frame successfully over the RLP is noted by P_f and can be calculated as follow:

$$P_f = 1 - p(p(2-p))^{n(n+1)/2} \qquad (3)$$

Also, in equation (2), the probability of the first frame received correctly at the destination, being the ith retransmission frame at the jth retransmission trial is noted by $P(C_{ij})$, and can be calculated as follow:

$$P(C_{ij}) = p(1-p)^2 (p(2-p))^{\frac{j(j-1)}{2}+i-1} \qquad (4)$$

Transmission Delay without RLP (WiMAX). We use the delay model for TCP packet transmission without RLP which is proposed in [4]. The transmission delay without RLP is given as:

$$D_{noRLP} = (K-1)\tau + \frac{D}{(1-q^{N_m})(1-2q)} + \frac{1-q}{1-q^{N_m}} D \left[\frac{q^{N_m}}{1-q} - \frac{2^{N_m+1}q^{N_m}}{1-2q} \right] \qquad (5)$$

where $q = 1 - (1 - p)^K$ represents the TCP packet loss rate, and N_m denotes the maximum number of TCP retransmissions.

Total Transmission Delay. As seen in Fig. 1, in VCC signaling for CS-to-PS domain transfer, 7 messages are exchanged between SN and Proxy-Call Session Control Function (P-CSCF) of the visited IMS network and 7 messages are exchanged between P-CSCF of the terminating IMS network and CN. We assume CN is in WiMAX network. When SN is transferred to UMTS network, the VCC signaling transmission delay $D_{transmission-uw}$ is given by:

$$D_{transmission-uw} = 7 \times D_{RLP} + 7 \times D_{noRLP} \qquad (6)$$

When SN is transferred to WiMAX network, the VCC signaling transmission delay $D_{transmission-ww}$ in seconds is given by:

$$D_{transmission-ww} = 14 \times D_{noRLP} \qquad (7)$$

3.2 Processing Delay

We take into account a fixed processing delay for all entities. This fixed delay is the delay incurred due to the encapsulation and decapsulation of packets. For HSS, in addition to this fixed delay, processing delay consists of address lookup table delay too. When a query is sent to HSS for a particular IP address, the HSS has to look up its table for the given IP address. This lookup increases the processing delay [8]. Also,

at VCC AS, when a packet is received, relations between several functional entities are required which increase the processing delay. The processing delay for VCC signaling $D_{processing}$ can be given as:

$$D_{processing} = 4d_{proc-sn} + 14d_{proc-pcscf} + 21d_{proc-scscf} + 6d_{proc-as}$$
$$+ 5d_{proc-icscf} + d_{proc-hss} + 3d_{proc-cn} \tag{8}$$

where $d_{proc-sn}$, $d_{proc-pcscf}$, $d_{proc-scscf}$, $d_{proc-as}$, $d_{proc-icscf}$, $d_{proc-hss}$, and $d_{proc-cn}$ denote the unit packet processing delay at SN, P-CSCF, Serving-Call Session Control Function (S-CSCF), VCC AS, Interrogating-Call Session Control Function (I-CSCF), HSS, and CN, respectively. The processing delay is considered for received messages at a node, so the coefficients in equation (8) can be obtained from Fig. 1.

3.3 Queuing Delay

We assume a queue model M/M/1 and Poisson signaling arrival rate process. The processes are independent one to other. We only consider the queuing delay at the receive buffer and assume that the transmission buffer at a network node is delay free. The packet delay at SN queue is approximated as [10]:

$$E[w_{sn}] = \frac{\rho_{sn}}{\mu_{sn}(1-\rho_{sn})} \tag{9}$$

where $\rho_{sn} = \lambda_{sn}/\mu_{sn}$ represents the utilization at SN queue, μ_{sn} denotes the service rate at SN queue and λ_{sn} denotes the arrival rate at SN queue. Similarly, the packet delay at queues of other network nodes can be calculated. Thus, the queuing delay $D_{queuing}$ can be approximated as:

$$D_{queuing} = 4E[w_{sn}] + 14E[w_{pcscf}] + 21E[w_{scscf}] + 6E[w_{as}]$$
$$+ 5E[w_{icscf}] + E[w_{hss}] + 3E[w_{cn}] \tag{10}$$

where $E[w_{sn}]$, $E[w_{pcscf}]$, $E[w_{scscf}]$, $E[w_{as}]$, $E[w_{icscf}]$, $E[w_{hss}]$, and $E[w_{cn}]$ denotes the expected value of a unit packet queuing delay at SN, P-CSCF, S-CSCF, VCC AS, I-CSCF, HSS, and CN, respectively. As mentioned above, we only consider the queuing delay at the receive buffer, so the coefficients in equation (10) can be obtained from Fig. 1.

3.4 Total Delay for VCC Signaling

We calculate the total delay of VCC signaling for CS-to-PS domain transfer. The delay for VCC signaling when SN is transferred to UMTS network and CN is in WiMAX is given by:

$$D_{total-uw} = D_{transmission-uw} + D_{processing} + D_{queuing} \tag{11}$$

The delay for VCC signaling when SN is transferred to WiMAX and CN is in WiMAX is given by:

$$D_{total-ww} = D_{transmission-ww} + D_{processing} + D_{queuing} \tag{12}$$

4   Numerical Results

In this section, we present the numerical results for the delay analysis of VCC signaling for CS-to-PS domain transfer. The assumed values of parameters involved in equations are mentioned hereafter. The value of end-to-end frame propagation delay (D) is taken equal to 100 ms for UMTS. In case of WiMAX, the value of D is taken equal to 0.27 ms and 0.049 ms for 4 Mbps and 24 Mbps channel, respectively [7]. In UMTS, frame duration or also known as inter-frame time (τ) is assumed to be 20 ms. In case of WiMAX, τ is assumed to be 2.5 ms. The maximum number of RLP retransmissions (n) and the maximum number of TCP retransmissions (N_m) are both taken equal to 3 [4]. The unit packet processing delay is taken equal to 5 ms for VCC AS and HSS, and 4 ms for rest of entities. The service rate (μ) is taken equal to 200 packets/sec for VCC AS and HSS, and 250 packets/sec for rest of entities [8].
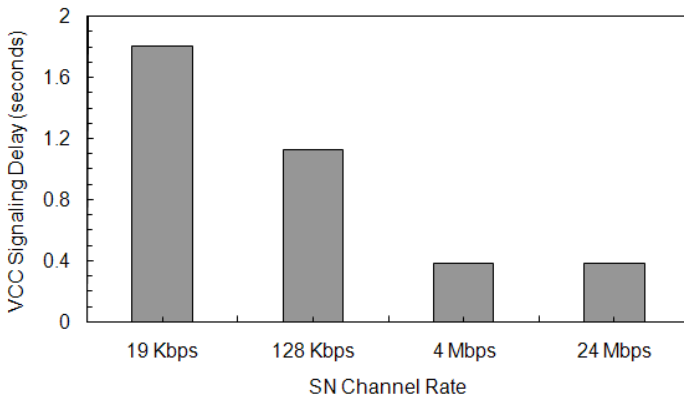

Fig. 2. VCC signaling delay when SN is transferred to different UMTS and WiMAX channel rates for fixed p and ρ
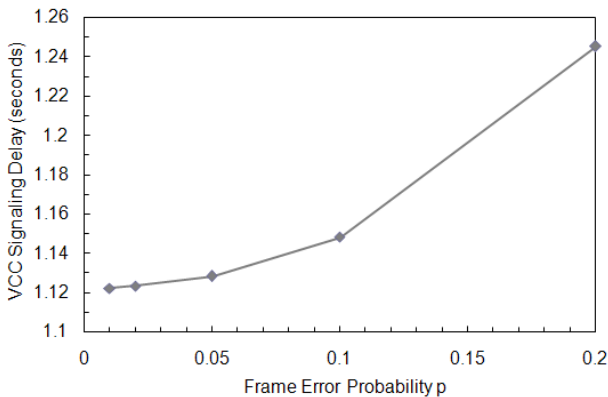

Fig. 3. Effect of changing frame error probability (p) on VCC signaling delay when SN is transferred to 128 Kbps UMTS and CN is in 4 Mbps WiMAX for fixed ρ

Fig. 2 shows the VCC signaling delay when SN is transferred to different UMTS and WiMAX channel rates for fixed frame error probability (p) and utilization at network entities (ρ). The frame error probability is taken to be 0.02. The utilization at HSS queue (ρ_{hss}) and the utilization at other network entities (ρ_{other}) are taken to be 0.7 and 0.4, respectively. It can be observed that the VCC signaling delay decreases considerably as the UMTS channel rate increases. Also, it can be observed that the VCC signaling delay is negligibly affected by changing the WiMAX channel rate.

Fig. 3 shows the impact of different frame error probabilities on the VCC signaling delay when SN is transferred to 128 Kbps UMTS network and CN is in 4 Mbps WiMAX for fixed utilization at network entities (ρ). The utilization at HSS queue (ρ_{hss}) and the utilization at other network entities (ρ_{other}) are taken to be 0.7 and 0.4, respectively. It can be observed that the VCC signaling delay increases with increasing frame error probability.
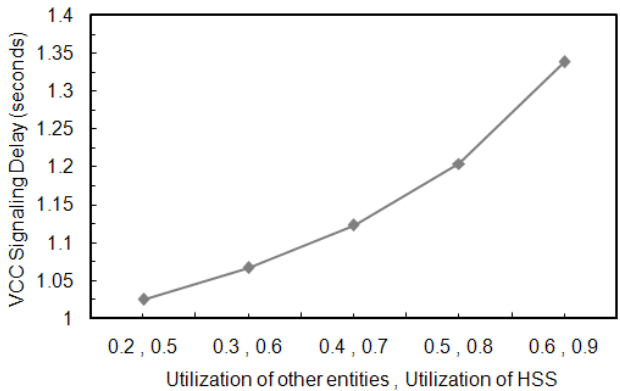

Fig. 4. Effect of changing utilization (ρ) on VCC signaling delay when SN is transferred to 128 Kbps UMTS and CN is in 4 Mbps WiMAX for fixed p

Fig. 4 shows the impact of different utilizations on the VCC signaling delay when SN is transferred to 128 Kbps UMTS network and CN is in 4 Mbps WiMAX for fixed frame error probability (p). The frame error probability is taken to be 0.02. It can be observed that the VCC signaling delay increases with increasing utilization at network entities.

5   Conclusion

In this paper, we analyzed the delay of VCC signaling for CS-to-PS domain transfer for different UMTS and WiMAX channel rates. The delay consists of three parts: transmission delay, processing delay, and queuing delay. The results indicate that the VCC signaling delay decreases considerably as the UMTS channel rate increases whereas the VCC signaling delay is negligibly affected by changing the WiMAX channel rate. Also, the VCC signaling delay increases with increasing frame error probability and/or utilization at network entities.

References

1. 3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Voice Call Continuity (VCC) between Circuit Switched (CS) and IP Multimedia Subsystem (IMS); Stage 3, Technical Specification 3GPP TS 24.206 version 7.4.0 (2007-12) (2007)
2. 3GPP, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Voice Call Continuity (VCC) between Circuit Switched (CS) and IP Multimedia Subsystem (IMS); Stage 2, Technical Specification 3GPP TS 23.206 version 7.5.0 (2007-12) (2007)
3. Fathi, H., Chakraborty, S., Prasad, R.: Optimization of SIP Session Setup Delay for VoIP in 3G Wireless Networks. IEEE Transactions on Mobile Computing 5(9), 1121–1132 (2006)
4. Das, S., Lee, E., Basu, K., Sen, S.: Performance Optimization of VoIP Calls over Wireless Links using H.323 Protocol. IEEE Transactions on Computers 52(6), 742–752 (2003)
5. 3GPP. Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 5). TS 24.228 (v5.15.0), (September 2006)
6. Snehal, S., Kale, V., Schwengler, T.: Comparing Unlicensed Mobile Access (UMA) and Voice Call Continuity (VCC) Architectures. In: IEEE Consumer Communications and Networking Conference (January 2009)
7. Banerjee, N., Wu, W., Basu, K., Das, S.: Analysis of SIP-based Mobility Management in 4G Wireless Networks. Elsevier Computer Communications 27(8), 697–707 (2004)
8. Munir, A.: Analysis of SIP Based IMS Session Establishment Signaling for WiMAX-3G Networks. In: Fourth International Conference on Networking and Services (ICNS 2008), pp. 282–287 (2008)
9. Price, R., Bormann, C., Christoffersson, J., Hannu, H., Liu, Z., Rosenberg, J.: Signaling Compression (SigComp). RFC 3320 (January 2003)
10. Medhi, J.: Stochastic Models in Queueing Theory. Academic Press, An imprint of Elsevier Science (2003)

Speed Up the Image Registration with PDE Model and Parallel AOS Scheme

Murong Jiang[1], Jian Li[2], Zexian Zhang[1], Jie Zhang[3], and Ruilin Guo[1]

[1] School of Information Science and Engineering, Yunnan University,
Kunming 650091, China
[2] Yunnan Jiaotong College, Kunming 650101, China
[3] Yunnan Bureau of Meteorolgy, Kunming 650034, China
`jiangmr@ynu.edu.cn, lj3194@126.com`

Abstract. Image registration is to find a suitable space transformation that aligns two or more images of the same scene taken at different times. As the image size is increasing, the numerical approaches based on the pixel matrix may stepup the computation complexity, and it is difficult to perform the large size registration on a single computer in the limited time. PDE-based registration is employing the partial differential equation driven by a similarity measure to minimize the distance between the corresponding pixel points. During the minimization process, Additive operator splitting (AOS) scheme is usually be used. In this paper, we discuss a multithreading method to perform AOS scheme and apply it to the parallel image registration computing with OpenMP and MPI on a dual core cluster. Some experimental results show that this method can produce the large size parallel image registration and save the time consume efficiently.

Keywords: image registration; parallel computing; AOS scheme; multithread programming.

1   Introduction

Additive Operator Splitting (AOS) scheme, proposed by T. Lu, P. Neittaanmaki and X-C Tai [1-2] and J. Weickert[3], has widely been used in the matrix computation, especially in PDE-based image processing. Its essential idea is to replace the inverse of the sum by the sum of inverse, and the complexity is $O(n)$. The implementaion is to transform a $m \times n$ matrix into a column vector of size $m \cdot n$ stacked atop one another from left to right, then split the the whole process in a sequence of one dimensional processed.

Most implementations for image registration are produced by defining a similarity measure between two given images, then minimizing an energy functional that combines both similarity and regularity measures. The main time consuming is on the matrix computation over the iterative procession. Many researchers employ HPC approaches for image parallel registration to reduce the execution time. For example, Fumihiko et al[5] produced a data distributed parallel algorithm to align large-scale three dimensional images on a 128-CPU cluster of PCs interconnected by Myrinet

and Fast Ethernet switches, Warfield et al[6] provided a parallel nonrigid algorithm based on the workpile paradigm running on a cluster of two Sun Enterprise Server 5000s, Rohlfing et al[7] discussed a numerical optimization technique to accelerate nonrigid registration on a 64-CPU SGI Origin 3800, Butz et al[8] presented a parallel affine registration based on genetic optimization on a 20-CPU cluster of Pentium III 550-MHz PCs. Weickert et. al[4] implemented a three-dimensional AOS scheme on an SGI Power Challenge XL with 8 processors to filter a 3D ultrasound image of a 10-week old foetus. All their works are related to the data-parallel processing over the pixel matrices and can be finished in a short time by some special parallel computer on a number of PCs cluster. In 2001, Bernd Fischer and Jan Modersitzki[9] promoted a intensity-driven approaches based on a variational fomulation, which helps us use the diffusion PDE model to describe the registration problem to perform the large size 2D registration on a single multi-core computer[10].

In this paper, we discuss a multithreading method to perform AOS scheme and apply it to the parallel image registration computing with OpenMP on a dual core cluster. First, we discuss the PDE-based registration equation and its AOS scheme, then built a cluster composed of 4 nodes and split the image into 4 blocks, use MPI function dispatch each pair block to the different node and produce the parallel registration with two and four threads created by OpenMP, then gather all the results and merge to the output image. At last, we give out some numerical experiments on meteorological objective tracking and landslide processing.

2   Parallel Registration Computing

2.1   Mathematical Model

Let $I_1(x+u(x))-I_2(x)$ be the measurement of the intensity distance between source image $I_1(x)$ and target image $I_2(x)$ for the displacement function $u(x):R^2 \to R^2$ at each $x \in \Omega \subset R^2$, then the registration problem may be described as the minimizing the following energy functional[11]

$$\min_{u(x),\sigma(x)} \int_\Omega \frac{\lambda}{2} |\nabla u(x)|^2 \, dx + \int_\Omega \frac{\mu}{2} |\nabla \sigma(x)|^2 \, dx$$
$$+ \int_\Omega [\frac{1}{2\sigma^2(x)} |I_1(x+u(x))-I_2(x)|^2 + \ln \sigma(x)]dx \qquad (1)$$

Where $\sigma(x,t)$ is the scale function λ and μ are the weight parameters.

By the use of variational method and an artificial time t, we have the following equations:

$$\partial_t u(x,t) = \lambda \Delta u(x,t) + \frac{1}{\sigma^2(x,t)}(I_2(x)-I_1(x+u(x,t)))\nabla I_1(x+u(x,t)), \qquad (2)$$

$$\partial_t \sigma(x,t) = \mu \Delta \sigma(x,t) + \frac{1}{2\sigma^3(x,t)}(I_1(x+u(x))-I_2(x))^2 - \frac{1}{\sigma(x,t)}. \qquad (3)$$

with the boundary and initial conditions:

$$\frac{\partial u(x,t)}{\partial \vec{n}} = 0, \quad \frac{\partial \sigma(x,t)}{\partial \vec{n}} = 0, \quad x \in \partial\Omega \times R^+$$

$$u(x,0) = 0, \quad \sigma(x,0) = \sigma_0, \quad x \in \Omega \tag{4}$$

Then minimizer of Equ.(1) is the steady state solution of Equ.(2)(3) satisfied $\partial_t u(x,t) = 0$ and $\partial_t \sigma(x,t) = 0$.

2.2   AOS Scheme

Equ. (2)(3) can be wrote as following:

$$w_t(x,t) = \alpha \Delta w(x,t) + f(w(x,t)) \tag{5}$$

$$w(x,0) = w_0(x) \tag{6}$$

$$\partial_{\vec{n}} w(x,t)\,|_{\partial\Omega} = 0 \tag{7}$$

where $w = (u, \sigma)$, f is called external force term and computed from the intensity of images after transformation. α is the weight parameter. The Laplace operator Δ is defined as the sum of two second partial derivatives respect to the coordinates like $\Delta = \partial^2_{x_1} + \partial^2_{x_2}$ with the center difference approximation and the mesh width $h = 1$.

$$\partial^2_{x_1} w = w(x_1 - 1, x_2) - 2w(x_1, x_2) + w(x_1 + 1, x_2) \tag{8}$$

$$\partial^2_{x_2} w = w(x_1, x_2 - 1) - 2w(x_1, x_2) + w(x_1, x_2 + 1) \tag{9}$$

Expending every term of Equ. (8) and (9) on Ω, it is easy to get

$$\partial^2_{x_1} w = Aw, \qquad \partial^2_{x_2} w = wA \tag{10}$$

and A is a typical band-diagonal matrix like

$$A = \begin{bmatrix} -2 & 1 & 0 & \cdots & 0 \\ 1 & -2 & 1 & \cdots & 0 \\ 0 & 1 & -2 & \ddots & \\ & & \ddots & \ddots & 1 \\ 0 & & & 1 & -2 \end{bmatrix} \tag{11}$$

Obviously, rotate the second term of (10) we have $(\partial^2_{x_2} w)^T = Aw^T$ which has the similar form as $\partial^2_{x_1} w$.

It is well known that the discretization of Equ. (5) with explicit scheme needs high number of iterations, so we consider the semi-implicit scheme discribed as[10]:

$$w^{k+1} = (I - \tau \sum_{l=1}^{2} A_l)^{-1}(w^k + \tau f(w^k)) \tag{12}$$

where τ is the time step size, $A_1 = \alpha A$ and A_2 is a A_1-like matrix which rotated two times. Equ. (12) is an unconditional stable scheme[1-3].

The essential idea of AOS scheme is to replace the inverse of the sum by the sum of inverse. Then we transform Equ. (12) into its AOS scheme, i.e.

$$w^{k+1} = \frac{1}{2} \sum_{l=1}^{2} (I - 2\tau A_l)^{-1}(w^k + \tau f(w^k)) \tag{13}$$

The matrix $I - 2\tau A_l$ is a strictly diagonally dominant which can be efficiently inverted by Thomas algorithm.

Compute w^{k+1} using (13) can emply the following equations:

$$(I - 2\tau A_1)v_1^k = w^k + \tau f(w^k) \tag{14}$$

$$(I - 2\tau A_2)v_2^k = w^k + \tau f(w^k) \tag{15}$$

$$w^{k+1} = (v_1^k + v_2^k)/2 \tag{16}$$

It's easy to see that Equ. (14) and (15) can be computed by different processes.

2.3   Parallel Computing Platform

Windows Compute Cluster Server 2003 (WCCS 2003) is a high performance computing platform supported by Microsoft Co. This cluster system includes Windows Server 2003 Compute Cluster Edition, MS MPI, Job Management, Cluster Management and Visual Studio 2005 Team Suit.

According to the statute of WCCS 2003, we built a small cluster with 4 nodes using Ethernet switch to connect. Each with AMD Athlon™ 64x2 Dual Core processors connected via a 100Mbps switched Ethernet. The cluster architecture and the parameters of each node are shown as Figure 1 and Table 1.
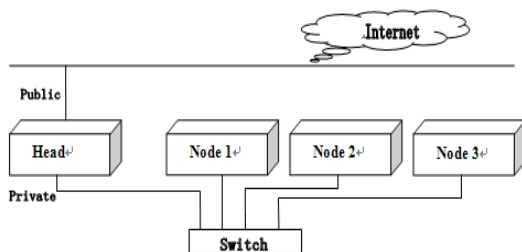

Fig. 1. Cluster architecture

2.4   Parallel Implementation on a Dual-Core Cluster

In order to perform the large size image registration, we use two steps to implement the parallel computing. First, we use the block partition to block the image into 4

smaller matrices, then register each pair of matrices shown as Figure 2. Second, during the iterations in the sequence algorithm, we use two threads to produce AOS scheme for Equ. (14) and (15) (see Figure 3).

Table 1. The parameters of each node

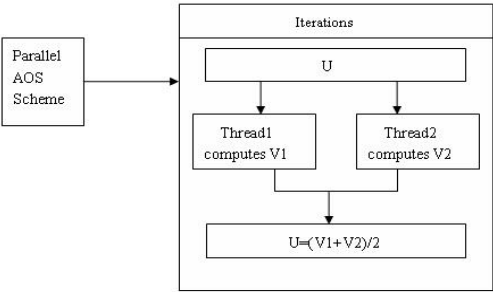| Node Type	CPU	Frequency	Memory
Head Node	AMD Athlon(tm)64 X2 Dual 4800+	2.50GHz	2GB
Other Node	AMD Athlon(tm)64 X2 Dual 4600+	2.40GHz	1GB
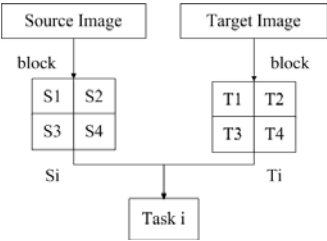
Fig. 2. Block the images

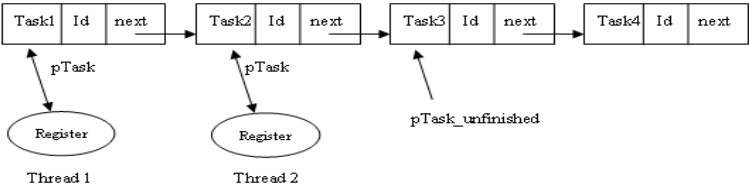**Fig. 3.** Parallel AOS scheme

Fig. 4. Task queue

According to the dual-core computer characters and the image size, we create the task queue include 4 threads (see Figure 4). Each thread gets a task and computes until all tasks have been finished. The marks of subtasks are defined as Figure 2 and the blocked image registration is shown as Figure 5. The parallel registration process is stepped as Figure 6.
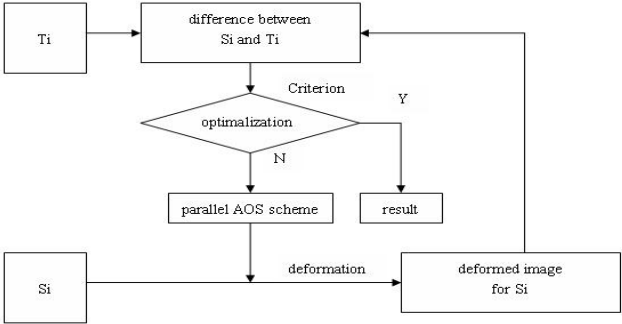

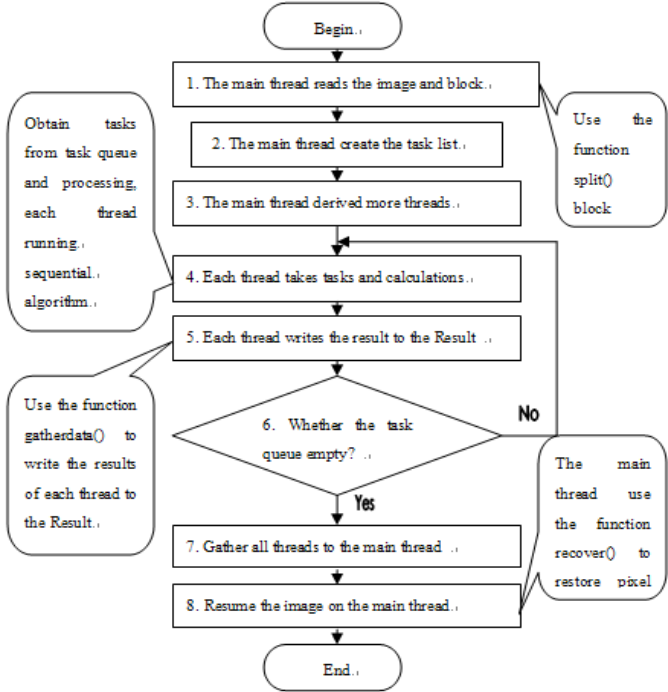**Fig. 5.** Register each pair of the block images

Fig. 6. Parallel image processing diagram

From Figure 6 we see that, while the image size is $m \times n$, step 1 block the image into $k_1 \times k_2$, each block needs to perform input data $(m/k_1) \times (n/k_2)$, the time is $O((m \times n)/(k_1 \times k_2))$. Step 3 and step 7 send and receive data, the time is $t_s + t_w \cdot ((m \times n)/(k_1 \times k_2))$, where t_s is the static start up time and t_w is perword transfer time. Step 4 is the sequential computing by using the registration algorithm, the computation is $O((m \times n)/(k_1 \times k_2))$. The last step combines and outputs the image. In the cluster environment, each word transfer time is very small, and the data latency is also very low, so the total computational complexity of parallel image registration is $O((m \times n)/(k_1 \times k_2))$.

3   Numerical Experiments

Experiment 1: Meteorolgical Objectives Tracking

Meteorological image registration plays the essential role in weather forecast, atmospheric research and disasters monitor. Furthermore, meteorological objectives are complexity and moving quickly which may cause it difficulty to distinguish.

In Doppler Weather Rader image processing, the shape of the meteorological objective is the important parameter for determining the objective characteristics like moving, speeding, strength and limitation evolving. In order to obtain the shape, we firstly separate objectives, extract the boundary so that each objective can be analyzed as the independent one. By registering the meteorological objectives between the different times, we can get the moving speed, the direction of movement, and intensity change of the meteorological objectives and so on.

Figure 7 is the Meteorological objective tracking procession. The original image came from the Doppler Rader data image of Yunnan Region on Jun. 25, 2010. The image size is 1000×1000.
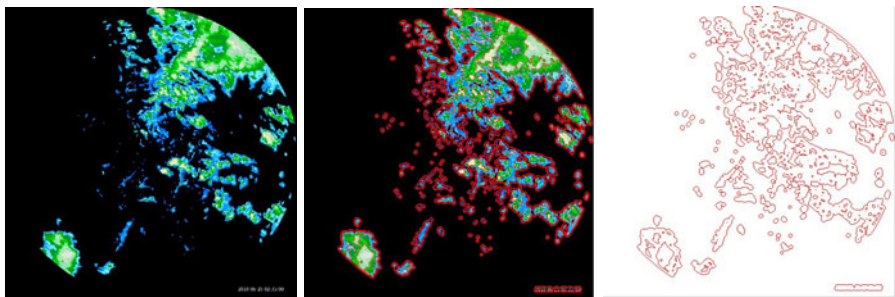
(a) Original image   (b) The meteorological objectives   (c) Extract the boundary

Fig. 7. Meteorological objective tracking

Experiment 2: The landslide Processing

The slope inspection takes the important effect on keeping the road smoothly and safety. Once the landslide happens, we need to find out the slide reason and restore

the original scene for the inspecting region. Figure 8 is the landside image registration result[12]. The image size is 2048×2048.

Fig. 8. Landsilde image registration

Table 2 shows the consumed time between different register ways for producing the Experiment 2.

Table 2. Comparison of the consumed time

Register Ways	Parallel structure	Main Threads Number	Max Threads Number	Core Usage	Consumed Time (Seconds)
Sequential	No Parallel	One	One	One	240.940
OpenMP	Parallel Task & Parallel AOS Scheme	Two	Four	Two	158.234
		Two	Six	Two	157.934
		Four	Eight	Two	157.755
MPI & OpenMP	Parallel job & Parallel Task & Parallel AOS Scheme	Four	Eight	Two (One Nodes)	158.625
	Parallel job & Parallel AOS Scheme	Four	Eight	Eight (Four Nodes)	75.756

4   Conclusion

In this paper, we have presented a multithreading method to perform the parallel implementation for image registration with PDE model and AOS scheme by using MPI on a 4 nodes dual-core cluster. The experimental results shown that this method can drop the number of iterations, reduce the computation complexity and save the computing time.

References

 1. Lu, T., Neittaanmaki, P., Tai, X.-C.: A parallel splitting up method and its application to Navier- Stokes equations. Applied Mathematics Letters 4(2), 25–29 (1991)
 2. Lu, T., Neittaanmaki, P., Tai, X.-C.: A parallel splitting up method for partial differential equations and its application to Navier-Stokes equations. RAIRO Math. Model. and Numer. Anal. 26(6), 673–708 (1992)
 3. Weickert, J., Romeny, B., Viergever, M.: Efficient and reliable scheme for nonlinear diffusion filtering. IEEE Trans. Image Processing V7, 398–410 (1998)
 4. Weickert, J., Zuiderveld, K.J., Romeny, H., Niessen, W.J.: Parallel Implementations of AOS Schemes: A Fast way of Nonlinear Diffusion Filtering. In: Proc. 1997 IEEE International Conf. on Image Processing, vol. 3, pp. 396–399 (1997)
 5. Fumihiko, I., Kanrou, O., Kenichi, H.: A data distributed parallel algorithm for nonrigid image registration. Parallel Computing 31, 19–43 (2005)
 6. Warfield, S., Jolesz, F., Kikinis, R.: A high perform- ance computing approach to the registration of medical imaging data. Parallel Computing 24(9/10), 1345–1368 (1998)
 7. Rohlfing, T., Maurer, C.R.: Nonrigid image registration in shared-memory multiprocessor environments with application to brains, breasts, and bees. IEEE Trans. Inform. Technol. Biomed. 7(1), 16–25 (2003)
 8. Butz, T., Thiran, J.-P.: Affine Registration with Feature Space Mutual Information. In: Niessen, W.J., Viergever, M.A. (eds.) MICCAI 2001. LNCS, vol. 2208, pp. 549–556. Springer, Heidelberg (2001)
 9. Fischer, B., Modersitzki, J.: Fast Diffusion Registration, Contemporary Mathematics, pp. 1–12 (2001)
10. Han, J.F.: Fast Diffusion Registration, Tutorials to Scientific Computing, SS (2005)
11. Jiang, M.R., Lin, Y.Y.: Monomodal registration with adaptive parameter computing. In: International Conference on Modelling, Identification and Control, Shanghai, June 29-July 2 (2009)
12. Chen, L.: Image Registration based on multicores parallel architecture, Master Degree Dissertation, Yunnan University (2010)

High-Integrity MapReduce Computation in Cloud with Speculative Execution

Jing Xiao[1] and Zhiwei Xiao[2]

[1] School of Information Security, Shanghai JiaoTong University
[2] Software School, Fudan University
xjtt2000@sjtu.org
zwxiao@fudan.edu.cn

Abstract. Cloud computing involves processing a huge amount of data using massively, distributed computing resources. However, the massive and distributed nature of cloud computing also make the integrity of computation upon easily be easily broken either by deliberate attacks or unconscious machine failures. In this paper, we propose to provide high-integrity feature to MapReduce computation using speculative execution. The key idea of our approach is selectively replicating MapReduce tasks on a random computation node, and comparing the hash of the execution results to determine if the integrity of the task is compromised. A preliminary prototype, called Nessaj, has been implemented on Hadoop MapReduce framework. Experimental results show that Nessaj can detect and recover from our randomly injected attacks in high probability. The performance overhead is also moderate.

1 Introduction

Cloud computing has been popular for years, which is evidenced by a number of commercialized cloud platforms including Amazon's EC2 [1], Saleforce.com and Microsoft Azure. To simply the programming of cloud computing, MapReduce, invented and popularized by Google, has been used in various usage scenarios such as Web Searching, Machine Learning and Statistical Machine translation. This is due to its simplicity and elegance of MapReduce in expressing large scale computation using mostly two primitives: Map and Reduce.

However, deploying MapReduce in cloud platforms also creates several key challenges. Among them, the integrity of computation is of great importance to the usefulness of the MapReduce tasks. For example, if computation of a single MapReduce is tampered with, the result of the entire computation might be inaccurate and even useless, especially for some convergence-based computation such as K-Means. Unfortunately, there is currently still very little research towards this issue.

Tampering with the computation integrity is a real threat to current cloud platform for the following reasons. First, the multi-tenancy nature of cloud platform makes that the computation from one user might be co-hosted with others and even an attacker. This gives the possibility that the attacker might leverage security vulnerabilities of the cloud stack and tampered with the execution integrity. There has already a number of security vulnerabilities uncovered in CVE, including those in Xen [2] [3], VMWare [4], not to mention those in Linux and user-level software. Second, to lower

the cost of cloud, cloud service providers usually adopts commodity hardware, which is usually not stable and might fail stealthily [5]. Even a single bit error in memory or storage might make the overall result manliness.

Being aware of this problem, this paper proposes a transparent approach to improve the execution integrity of MapReduce computation on the cloud, while not sacrificing its simplicity and elegance. The proposed approach, called Nessaj, stealthily and randomly creates a number of replicated MapReduce tasks on randomly assigned nodes, and compares the results to verify the execution integrity.

We have implemented a working prototype on Hadoop MapReduce framework. Our evaluation using a small scale cluster and a simulator indicates that the performance overhead is moderate and the randomly injected errors are all detected.

The rest of the paper is organized as follows. Section 2 presents an overview of MapReduce, the Hadoop implementation as well as the data integrity issue in Hadoop that motivates the work of this paper. Section 3 describes the design issues of speculative execution and the implementation of Nessaj. Section 4 presents the performance evaluation results. Section 5 relates Nessaj to previous work. Finally, we conclude the paper in Section 6.

2   Background and Motivation

2.1   MapReduce

MapReduce is a programming model on the parallel processing domain, aiming at helping programmers to write parallel applications to process petabytes of data. MapReduce abstracts a program as two phases: Map and Reduce. In the Map phase, a user-defined map function is applied to each unit of the input data, generating pairs. Then the pairs with the same key are all aggregated by a user-defined reduce function in the Reduce phase.

2.2 An Overview of Hadoop

Apache Hadoop is the most popular open-source implementation of the MapReduce model, using the Java language. Currently there are hundreds of thousands of companies and organizations are deploying Hadoop clusters to process massive amount of data[6], including big ones like eBay, Yahoo! and FaceBook. The core of the Hadoop project consists of a MapReduce framework, and a persistent storage Hadoop Distributed File System (HDFS), which is inspired by the Google File System [7] used by Google's MapReduce framework.

HDFS is a distributed chunked file system, in which data are split into pieces of chunks, typically 64 or 128 megabytes, and distributed among the cluster. HDFS also support a configurable file replication to ensure data availability and speed up data access.

The Hadoop MapReduce framework consists of JobTracker as a master node, scheduling and managing the running MapReduce applications, and TaskTrackers as slave nodes, performing the actual MapReduce works. Users submit their MapReduce jobs to JobTracker, and then JobTracker splits the jobs into MapTasks and ReduceTasks and schedules them to run on TaskTrackers. MapTasks load input from

HDFS, perform the Map phase of MapReduce, and generate intermediate   data onto their local file systems. ReduceTasks then fetch these intermediate data, aggregate them with the reduce function, and save the final MapReduce results back to the HDFS.

2.3 Data Integrity in Hadoop

All the persistent data of Hadoop are stored in the HDFS, which replicates data with multiple copies and thus ensures data integrity and availability. For the intermediate data generated by the MapTasks, Hadoop only temporally saves them on the local disks of TaskTrackers. Upon a failure to access such intermediate data, Hadoop simply restarts the MapTask generating these data. Such mechanism works fine on the data availability, but it fails to ensure data integrity.

If the intermediate data were modified by malicious software or operators before used by ReduceTask, Hadoop cannot recognize such situation and would generate a wrong final result. This can be a serious problem for applications that analyze a large amount of raw data and generate just a brief summary report. The intermediate data of this kind of applications are relatively much less than the input data. So changes of some of the intermediate data can cause the final result to be totally different from the correct result.

Our threat model is that one or several machines of the MapReduce cluster are controlled by malicious software or operators, who gain the privilege and modify the intermediate data generated by the MapReduce framework. We assume that the number of the machines being malicious controlled is relatively minor in the cluster. Unconscious machine failures like disk IO faults can also cause a similar impact. The data integrity issue under such attacks can be addressed by leveraging the speculative execution mechanism in MapReduce and Hadoop. The scheduler or JobTracker can speculatively start some replications for a single task, compare the intermediate data of them, and then accept the major result as the correct one. This approach is based on the observation that the attacker can only modify a minor number of outputs, if the speculative executions are distributed among the cluster. Such a speculative approach can provide high data integrity level, though not ensuring the integrity of all data.

3   Design and Implementation

In this section, we would discuss some important design considerations and present our preliminary prototype, called Nessaj, based on the Hadoop MapReduce framework.

3.1 Ensuring Data Integrity with Speculative Execution

We only speculate MapTasks because the potential compromised intermediate data on local file systems are all generated by MapTasks. When scheduling, the scheduler randomly chooses some of the MapTasks to be speculatively executed, and then accepts the major result as the correct one. Though the basic idea to ensure data integrity with speculation is quite straightforward, some details are worth noting. Our goal is to provide a high data integrity level, while maintaining a moderate performance. So there is a tradeoff between the effect of speculation and the system performance.

When to Start Speculation? The schedule of the speculative execution can directly affect the system performance. In Hadoop, ReduceTasks can copy the intermediate data generated by a MapTask once it completes. But for MapTasks being speculatively executed, ReduceTasks cannot fetch the intermediate data until all speculative replications complete and a correct result is accepted by the scheduler. If the portion of tasks being speculated is high, it is better to start all the speculative replications of the same task at the same time, because in this case the intermediate result is soon available if all replications complete at nearly the same time. But if there is a little number of tasks being selected to speculate, proponing the speculation and giving higher priority to non-speculative tasks can help the ReduceTasks start copying early.

Where to Execute Speculative Tasks? Ideally we should schedule the speculative tasks randomly among the whole cluster, to achieve a high probability to defend the attacks. However, it is expensive to run a task on a node without the input data present locally, because such a task needs to fetch the input data from other nodes through networking. Considering such data transferring overhead, we choose to schedule the speculative tasks to the nodes which have the chunks of the input data if possible. This policy is nearly as effective as the total random fashion, because all data chunks are replicated over three different nodes in a typical HDFS configuration, and so the probability of data compromising from the same source is low.

How to Handle Failure? It is possible that the scheduler fails to find a major result when there are at least two different results with the same number of tasks. In this case, the scheduler should start another speculative task until it can find a major result or reach the threshold of the number of speculative tasks. The scheduler would just fail the whole job if it cannot find a correct result after finishing the maximum number of speculative tasks.

3.2   The Prototype: Nessaj

We have implemented a preliminary prototype, called Nessaj, by extending the Hadoop MapReduce framework with speculative execution support for data integrity.

Architecture. We leverage the existing speculation and output committing mechanisms in Hadoop to implement Nessaj, and thus Nessaj retains the main control flow of Hadoop. Output committing is an optional phase supported by Hadoop, it makes a task enter the COMMIT_PENDING status before completion, and wait for the JobTracker to decide whether it can commit or not. The result of the task is unavailable to downstream tasks until it is commit.

Nessaj employs the propounding policy for speculative execution under the observation that the actual speculative ratio must be low, because there are quite little amount of attacked machines. So Nessaj would first schedule normal tasks and then the speculative ones. When speculative tasks finish their works, Nessaj forces them to enter the committing phase before completion. The speculative task then computes the MD5[8] value for its result, reports its status to the JobTracker along with the MD5 value, and waits for the JobTracker to decide whether it can commit. The JobTracker should first wait for all the running speculative replications of the same task to enter the committing phase, and then it can sort and accept the major MD5

value. If a correct result is accepted, JobTracker would randomly select a task with that value, and then inform that task to commit and kill other tasks. Otherwise JobTracker would start another speculative task until it can make a decision.

Implementation. To implement Nessaj, we firstly add a new output committer to perform the new committing logic, including the computation of MD5 value. Secondly, we extend the task status object to carry the MD5 value for committing tasks. Thirdly, we track the progressing of speculation in the corresponding TaskInProgress objects for each task, and implement the decision logic for commitment in JobInProgress. Finally, we also make the JobTracker and Task objects to be aware of our speculative execution support.

4   Evaluation

We evaluate both the effect and performance of Nessaj, by conducting experiments on a simulator as well as a small cluster.

4.1   Experiment Environment

To evaluate the performance of Nessaj, we conduct the experiments on a small-scale cluster with 1 master node and 6 slave nodes. Each machine is equipped with two 12-core 1.9GHz AMD processors, 64GB memory, four 500GB SCSI disks and a 1000M NIC. All nodes are connected with a switcher using 1000M network. The operation system is Debian squeeze with a Linux 2.6.37.1 kernel. We use Hadoop version 0.20.1 running on Java SE Runtime 1.6.0. The file replication number of HDFS is set to 3 and the size of each file chunk is configured as 64MB.

The effect of the Nessaj is determined by the degree of speculation as well as the amount of machines being attacked and the power of the malicious software or operators. So we implement a simple simulator to gain a deep insight of the speculation policy of Nessaj on clusters of larger scale.
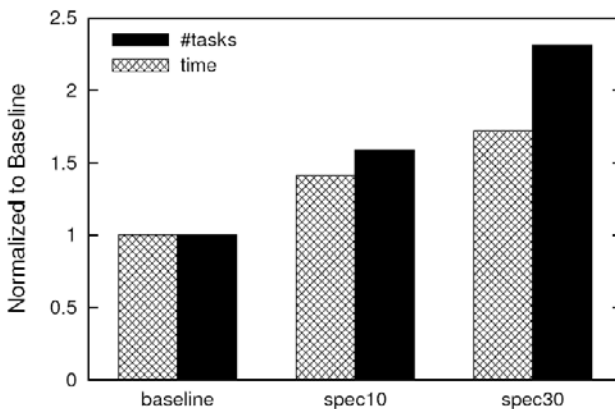

Fig. 1. The Performance of Speculation on 7 Nodes. Baseline denotes the run without speculation, while spec10 and spec30 denote speculating 10% and 30% tasks respectively

	Spec 30%	Spec 10%	BaseLine	Spec 30%	Spec 10%	BaseLine
#slave	100	100	100	100	100	100
#slave_att	10	10	10	5	5	5
#err_inject	47.03	40.31	35.86	23.74	20.26	17.43
err_not_det%	0.70%	0.91%	1.00%	0.34%	0.46%	0.48%
err_det_tot%	46.63%	18.90%	0.00%	47.81%	18.66%	0.00%

Fig. 2. The Effect of Speculation on 100 Nodes. We compare speculating 30% tasks(Spec 30%), 10% tasks(Spec 10%) and no speculation(Baseline). We denote the number of slaves being attacked as #slave_att, the number of errors injected as #err_inject, the ratio of errors not detected in total tasks as err_not_det%, and the ratio of errors detected in total errors injected as err_det_tot%.

4.2   The Performance of Speculation

We evaluate the performance of speculation with K-Means using 16GB input data. We assume one machine is controlled and injected an error with a probability of 0.1. All the injected errors are detected in our experiments. As Figure 1 shown, the speculation introduces a moderate execution time overhead as about 41% and 72% when speculating 10% and 30% tasks respectively. The run time overhead mainly comes from the increase of the number of running tasks, as Nessaj starts about 59% and 131% more tasks for speculative execution. The overhead of the MD5 computation for the intermediate data is negligible (no more than 20ms in our K-Means experiment), because the intermediate data is computed immediately after flushing to disk and thus enjoys a good temporal data locality.

4.3   Speculation on Larger Scale

We simulate the effect of speculative execution in different scales and setups, including the scale of clusters, the number of running tasks, as well as the ratio of speculative tasks, the ratio of nodes being attacked, and the probability that the result of one task is modified. Figure 2 shows the simulated result on a 100-machine scale. The degree of speculation determines the ratio of errors detected. Our current preliminary speculation policy can limit the damage of data integrity to about 0.34% when the ratio of machines being attacked is low (5%). But as the number of attacked machines doubles, this damage also increases by nearly one time. On the 500-machine scale, speculation can still ensure the data integrity to the level as the 100-machine scale. But there are 14% 24% of the simulated jobs fail due to reach the threshold of maximum speculative tasks.

5   Related Work

MapReduce [9] has been widely deployed in many applications, other than the web-search domain, such as machine learning [10], statistical machine translation [11] and scientific data analysis [12]. Speculative execution has also been implemented in

Hadoop [13] for the purpose of accelerating program execution, in contrast for fault tolerance as done in this paper. To improve the precision of speculative execution, Zaharia et al. [14] optimizes Hadoop with an algorithm called LATE, to enable a heterogeneity-aware scheduler for heterogeneous environments such as Amazon's EC2. To improve the security and privacy of MapReduce applications, Roy et al. [15] propose Airavat, which combines decentralized information flow control to MapReduce. However, they cannot detect or prevent attacks to execution integrity of MapReduce applications.

6   Conclusion

In this paper we ananlyzed the data integrity in MapReduce clusters, which can be easily broken either by deliberate attacks or random machine failures. We proposed to ensure the data integrity in MapReduce computation using speculative execution. We extended the existing speculative execution mechanism in the Hadoop MapReduce framework to protect the data integrity of the MapReduce computation results. We have evaluated our preliminary prototype Nessaj in a small cluster as well as a simulator. Experiment results showed that Nessaj successfully detected all the injected errors, with a moderate performance overhead.

References

1. Amazon Inc.: Amazon Elastic Compute Cloud (Amazon EC2), `http://aws.amazon.com/ec2/` (2008)
2. Common Vulnerabilities and Exposures: Xen guest root can escape to domain 0 through pygrub, `http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4993` (2007)
3. Common Vulnerabilities and Exposures: Vulnerability in xenserver could result in privilege escalation and arbitrary code execution, `http://support.citrix.com/article/CTX118766.access` (2007)
4. Kortchinsky, K.: Hacking 3d (and breaking out of vmware) (2009)
5. Schroeder, B., Pinheiro, E., Weber, W.: DRAM errors in the wild: a large-scale field study. In: Proceedings of the Eleventh International Joint Conference on Measurement and Modeling of Computer Systems, pp. 193–204. ACM, New York (2009)
6. Apache Wiki: Applications and organizations using hadoop, `http://wiki.apache.org/Hadoop/PoweredBy`
7. Ghemawat, S., Gobioff, H., Leung, S.: The Google file system. ACM SIGOPS Operating Systems Review 37(5), 29–43 (2003)
8. Rivest, R.: The MD5 message-digest algorithm. Request for Comments (RFC1320). Internet Activities Board, Internet Privacy Task Force (1992)
9. Dean, J., Ghemawat, S.: MapReduce: simplified data processing on large clusters. Communications of the ACM 51(1), 107–113 (2008)
10. Chu, C., Kim, S., Lin, Y., Yu, Y., Bradski, G., Ng, A., Olukotun, K.: Map-reduce for machine learning on multicore. In: Advances in Neural Information Processing Systems: Proceedings of the 2006 Conference, vol. 281. MIT Press, Redmond (2007)

11. Dyer, C., Cordova, A., Mont, A., Lin, J.: Fast, easy, and cheap: Construction of statistical machine translation models with MapReduce. In: Proceedings of the Third Workshop on Statistical Machine Translation at ACL, pp. 199–207 (2008)
12. Ekanayake, J., Pallickara, S., Fox, G.: MapReduce for Data Intensive Scientific Analyses. In: IEEE Fourth International Conference on eScience, 2008. eScience 2008, pp. 277–284 (2008)
13. Bialecki, A., Cafarella, M., Cutting, D., O'Malley, O.: Hadoop: a framework for running applications on large clusters built of commodity hardware (2005),
`http://lucene.apache.org/hadoop`
14. Zaharia, M., Konwinski, A., Joseph, A., Berkeley, U., Katz, R., Stoica, I.: Improving MapReduce Performance in Heterogeneous Environments. In: Proc. OSDI (2008)
15. Roy, I., Setty, S., Kilzer, A., Shmatikov, V., Witchel, E.: Airavat: Security and privacy for MapReduce. In: Proceedings of the 7th USENIX Conference on Networked Systems Design and Implementation, USENIX Association (2010)

Cognitive Radio Access Based on Multiparameter Matching Ability Estimation*

Kunqi Guo[1], Lixin Sun[1], Yong Lee[2], and Shilou Jia[3]

[1] School of Computer Science and Telecommunication Engineering, Jiangsu University
Jiangsu 212013, China
[2] Shanghai Institute of Microsystem and Information Technology, Chinese Academy
of Sciences, Shanghai 200050, China
[3] Communication Research Center, Harbin Institute
of Technology, Harbin 150001, China

Abstract. In this paper, we focus on the channel usage efficiency for secondary user in cognitive radio networks. We formulate the optimization objective as the total reward maximization by Partially Observable Markov Decision Processes (POMDPs). The total reward is maximized by considering multidimensional context parameters including allowable channel transmission rate, queue delay and arrival rate. Match Ability is proposed considering above context parameters. A heuristic greedy algorithm is proposed for each secondary user to access sensed channels based on the local maximum match ability. By combining the utility function of average waiting time with match ability, we improve the global scheduling delay fairness. We demonstrate by simulation results that as the average arrival rate of secondary user increases, the large stable region of low delay can be efficiently maintained by varying utility function of the average waiting time.

Keywords: Cognitive radio, match ability, utility function, average waiting time.

1 Introduction

A novel solution to radio spectrum underutilization problems is to adopt cognitive spectrum access. It can be done by two steps: sensing frequency bands that are not used by the primary users and accessing current idle frequency band. To achieve this goal in an autonomous manner, multiple user cognitive radio networks need to adopt a feasible scheme that can be adaptive to dynamic wireless network characteristics to use radio spectrum most efficiently. In general, in cognitive radio networks, when driven by service requirement, each secondary user starts to sense each channel of primary users in any given time slot, with probable sensing results for each channel of primary users including: (1) Accurately sensed to be idle, or to be active, and (2) Wrongly sensed to be idle, or to be used. In case (2), the idle channel usage efficiency can be degraded because the same channel is simultaneously used by more than two

---

users, or not be utilized by secondary users. For single secondary user, a channel of primary user system is determined for access selection only according to the sensed result. It can be completed by detecting the signal in frequency bandwidth of primary users at physical layer. For how to use idle channels of primary users efficiently, a great deal of effort has been made by considering spectrum detecting method, accessing strategy and traffic tail characteristics estimation in time domain respectively. In [1] and [2], a hierarchical cognitive network is considered for cognitive user transmission opportunities in multiple channel communication system. The queue tail distribution of cognitive users is estimated for the detection of channels of primary users in [3], with closed-form expressions under two primary users.

While there has been much investigation for channel usage in cognitive radio networks including opportunistic access, spectrum sharing and stable and efficient access method [4, 5, 6, 7], there remains a lack of optimizing channels used by secondary users that considers the *match* between allowable transmission rate and service quality of secondary user. It is a complex multiple variants optimization problem we will face in this paper. Using Partially Observable Markov Decision Processes (POMDPs), we investigate the optimization objective that is formulated as the total reward maximization. The optimization implementation based on POMDP is to obtain the expected total reward by taking a sequence of decision actions. In our objective optimization for channel access, each access decision is made based on the multiparameter match estimation considering channel condition of primary user, average queue waiting time and average traffic arrival rate of secondary user. To address this, we propose a novel channel access scheme using multidimensional parameters *match ability maximization*. In this scheme, for each secondary user, the statistical relationship between context parameters and the quality of service is derived according to queue theory. In cognitive radio network, the interference to primary users may be increased due to the transmission power enhanced by a secondary user using a worse idle channel. In addition, a secondary user will reduce the utilization efficiency of channels being in better condition because its current service queue length is shorter. Thus, the trade-off between channel condition and queue length should jointly be combined for spectrum resource scheduling decision. It becomes more important for secondary user in cognitive radio networks because of the constrained opportunistic spectrum utilization. In this paper, we investigate the optimization for this trade-off realization by taking multiple context parameters into consideration. We decouple the optimization objective realization into three low complexity sub-problem solutions including the control of the service arrival rate of secondary user, idle channel utilization and the total trade-off strategy. To our knowledge, as yet, it is not researched. First, considering cognitive radio characteristics, we propose a novel metric *Match Ability* for each secondary user to make decision of how to use the sensed channel. *Match Ability* is constructed according to the required bit-error-ratio (BER) and the achievable transmission rate on the sensed channels while considering the interference caused to its neighboring primary users. For single secondary user, *Match Ability* (*MA*) performs mapping between channel selection and the achieved quality of service (QoS). By this mechanism, each secondary user access sensed channels based on *greedy Match Ability maximization (GMAM)*. However, the total performance needs to be improved by considering that two secondary users (or more) having different queue conditions

and the same estimated *MA* request to use the same channel. To adapt well to the trade-off between queue delay and channel efficiency, we use extended *Match Ability* called *EMA* that is based on the principle of the utility maximization. In this scheme, we combine queue delay with *MA* of each secondary user by the utility function of queue delay. In addition, one of advantages of our methods is that it allows us to use conventional Proportionally fair scheduling (*PF*) as centralized management control by only replacing the single parameters with the integrated parameter *MA*, which can adapt well to the channel efficiency maximization requirement.

2   System Description and Optimization Formulation

2.1   System Description

We consider a multiple channels cognitive radio networks with *M* primary users and *N* secondary users (cognitive users). In primary user system, each primary user has a channel (frequency band) to exclusively and randomly use. The same spectrum channel can be shared at the same time between secondary user and primary user. For the same channel sharing, two schemes are considered in our optimization objective implementation. The framework for channel access in secondary user system is shown in Fig. 1.
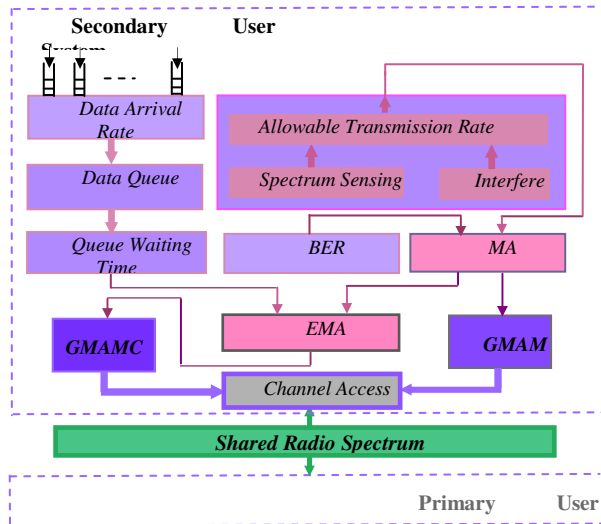

Fig. 1. Framework for Channel Access in Secondary User System

The first one is the distributed spectrum access that one secondary user decides whether or not to access a sensed channel based on *GMAM*. With the *GMAM* based distributed way, one secondary can take shorter time from sensing to accessing channel. However, the total optimization depends on the *optimum match* between the allowable channel transmission ability and the queue length waiting to be transmitted.

By combining *GMAM* for channel sensing with the queue delay state, *GMAMC* achieves the global balance ability by controlling *greedy maximization degree* used in *GMAM*.

2.2 Optimization Formulation

A POMDP denotes an observation (estimation) and decision process taking a sequence of actions to maximize the reward value under uncertain estimated factors. Let S, A, and O, be a set of states, a set of actions and a set of observations (estimated parameters). If the system is currently in a state $s \in S$, after an action (decision) is taken, the system is driven into a new state s' from s and as a result, a reward value $R(s,a)$ is obtained. Due to uncertain predicted parameters, the end state s' can be modeled as a conditional probability function $T(s,a,s') = p(s'|s,a)$. The optimization objective is to maximize the total reward: $\max \sum_{s \in S, a \in A} R(s,a)$. Let $S_j[k] = 1$ and $S_j[k] = 0$ denote the idle and busy condition of the channel of primary user j in time slot k respectively. Taking channel usage efficiency as the system optimization goal, we represent the system state S by the vector $[S_i, S_2, ... S_M]$. I_{ij} is the interference caused by secondary user i using channel j to primary user j. We by $I_{threshold}$ denote the maximum interference threshold that primary user can tolerate. For each secondary user, we consider two channel access schemes including the distributed access action and the centralized control. The set of access actions is expressed by A. Let $a_{ij} = 1$ and $a_{ij} = 0$ denote the distributed access and the centralized control scheme respectively for access channel j adopted by secondary user i. Each secondary user can access one channel by one of two ways indicated by $a_{ij} \in A = \{0,1\}$. Let $r_{ij}(a_{ij})$ be the required reliable transmission rate of secondary user i over channel j by accessing mode a_{ij}. By choosing the appropriate access scheme, our objective is to maximize the total system reward in terms of transmission rate

$$\max \sum_{i=1}^{N} \sum_{j=1}^{M} r_{ij}(a_{ij}) \tag{1}$$

$$\text{s.t.} \quad 1) \sum_{i} I_{ij} < I_{threshold} \quad ; 2) \ a_{ij} \in A = \{0,1\}$$

In the above formulation, $\sum_{i} I_{ij} < I_{threshold}$ guarantees that the total interference caused by secondary user to each primary user is under the specified condition. However, the channel utilization efficiency can be reduced due to a channel access determined only according to a hard two states decision mechanism that is the busy and idle condition. Dynamic network environment makes it feasible to allocate the same channel at the same time to a secondary user and a primary user due to time-varying user location diversity. We consider a discrete optimization system that time

is divided into slots of fixed length T_s. For the current condition of each channel, we adopt the following definition.

$$S_{ij}[k] = \begin{cases} 1, & \text{if } I_{ij}[k] + \sum_{n \neq i} I_{nj}[k] < I_{threshold} \\ 0, & \text{if } I_{ij}[k] + \sum_{n \neq i} I_{nj}[k] \geq I_{threshold} \end{cases} \tag{2}$$

where $i, n \in \{1,2,...,N\}$, $j \in \{1,2,...,M\}$. In (2), $S_{ij}[k] = 1$ and $S_{ij}[k] = 0$ represent idle and busy condition of channel i in time slot k respectively. It means that a secondary user access a channel of primary users by considering the total interference including the interference already suffered by secondary user i and the interference to be caused by secondary user i due to using this channel.

For each secondary user, from the effective bandwidth theory, we can formulates the probability that the packet delay violates the delay requirements as

$$\Pr\{W_i > D_{\max}\} \approx e^{-\theta \delta D_{\max}} \tag{3}$$

where $D_{\max}$ is the delay requirement and θ is a positive constant referred to as *QoS* exponent, δ is a constant jointly determined by the arrival process and service process. It means that a large θ implies that a stringent delay requirement can be guaranteed by the system while a small θ implies that a loose delay requirement can be guaranteed by the system. We express by $q_i[k]$ and λ_i the amount of bits of secondary user i waiting for service at time kT_s and the average arrival bit rate respectively. According to Little's principle, we obtain the average waiting time for secondary user i, W_i by $W_i = q_i / \lambda_i$ where $q_i = \lim_{N \to \infty} \sum_{k=0}^{N-1} q_i[k] / N$. By the time low-pass window with length T_w, we obtain the average queue length of secondary user i over the time window, $\overline{q}[k] = (1 - \rho_w)\overline{q}_i[k-1] + \rho_w q_i[k]$, where $\rho_w = T_s / T_w$. Using this time window, the average waiting time for secondary user i at time kT_s, $W_i[k]$ is estimated by $W_i[k] = \overline{q}_i[k] / \lambda_i$. Thus, the average waiting time at end of time slot k is the function of the service arrival rate, the average queue length and the obtainable transmission rate.

3   Channel Access

During time slot k, secondary user i can decide whether to access channel j based on the maximization of *Match Ability* (*MA*) adopting distributed self-decision. Secondary user i using the channel j can get *Match Ability* MA_i^j, $MA_i^j[k] = R_i^j[k]S_{ij}[k]$ where $S_{ij}[k]$ is given by (2) and $R_i^j[k]$ is the achievable transmission rate of secondary user i using channel j that can satisfy the required *bit-error-rate* (BER_i) at receiving end. If QAM modulation is used, we can estimate $R_i^j[k]$ by $R_i^j[k] = \log_2\left(1 - \left(1.5\gamma_i^j[k] / \ln 5BER_i\right)\right)$, where $\gamma_i^j[k]$ is the *SINR* of the transmission link

of the secondary user i using channel j during time slot k. Let $h_{ij}[k]$ and $g_{ij}[k]$ represent the pathloss power gain and the normalized composite of shadowing and fading random variable with unit mean of the transmission link from secondary user i to primary user j respectively. Let where $P_i[k]$ be the transmitting power of secondary user i. If secondary user i complete one transmission during time slot t by $R_i^j[k]$, then we can obtain the power of interference received at primary user $I_{ij}[k]$ by $I_{ij}[k] = P_i[k]h_{ij}[k]g_{ij}[k]$. To reduce complexity, we propose low complexity heuristic distributed algorithm based on *greedy match ability maximization (GMAM)* search that is formulated by

$$SU[k] = \arg\max\left\{ MA_i^j[k] \right\} \tag{4}$$

where $i = 1,2,...,N$; $j \in D_i[k]$. By (7), each secondary user at end of current time slot k, selects the channel with the *local maximum match ability* out of channels that can be sensed that we call MA-Weight Channel Access (*GMAM*) in this paper.

Trade off between resource efficiency and fairness can be realized by maximizing system utility function [8]. Due to the balance ability of maximizing utility, we use the utility function to determine the access priority for secondary users having the requirement of using the same channel. The utility function for this purpose is $U_i(W_i[k]) = W_i^b[k]; i = 1,2,...,N$. Let ρ_w be small enough. Since $\Delta U(W_i[k])$ corresponds to the utility addition that should be maximized during current time slot. Let $EMA_i^j[k]$ be the extended *Match Ability* at time slot k of secondary user i denoted by $EMA_i^j[k] = W_i^{b-1}[k]MA_i^j[k]$. To obtain the better global performance, first, we need find *the global optimal trade-off parameter* G_{opt}. It can be realized efficiently by *binary search*. Secondly, allocate channel j to the secondary user i which can satisfy: $\min\left\{ \left| G_{opt} - (W_i^{b-1}[k]M_i[k]/\lambda_i) \right|; i = 1,2,..,N \right\}$. Thus, the channel j is likely allocated to a secondary user that has $W_i^b[k]M_i[k]/\lambda_i$ approximating to G_{opt} that is called GMAMC with low complexity because of using the efficient sorting-search [9].

4   Performance Evaluation

In our simulation, each channel used by secondary users is assumed to suffer slow fading. Let the *BER* required by the receiving end of each secondary user be 10^{-6}. It is assumed for *GMAM* that each secondary user can know the interference of its neighboring primary users through its *local spectrum sensing*. An ON-OFF model is used to model the traffic streams of secondary user. The length of time slot is 2 *ms*. The ON period is modeled as Pareto distribution and an exponential distribution is used for OFF duration. The frequency bandwidth of each channel is 20 kHz. Four different rates $\Omega = (1, 2, 5.5, 11)Mbps$ are used for *MA maximization based adaptation* transmission in secondary user system (SUS). First, we consider a square area of size $500 \times 500m$ in which 10 secondary users and 10 primary users are randomly deployed. Let $b = 1, 2, 3$ respectively for the utility function (10). Figure 2 shows the obvious

differences between *GMAM* and *GMAMC* in terms of queuing delay under the average arrival rate $\lambda_i = 60kbps$ of SUS. The best result is achieved by *GMAMC* with $b = 3$. Let *SU* denote the number of secondary users. Figure 3 and 4 show the average delay under different average arrival rates in SUS.
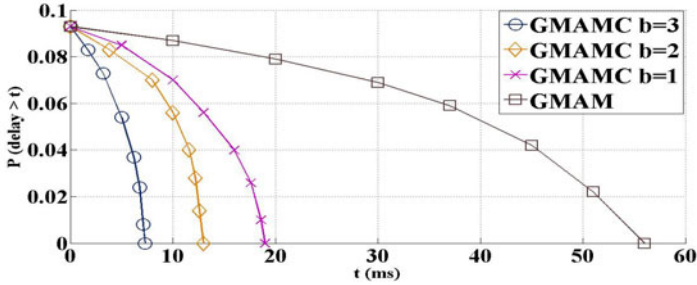

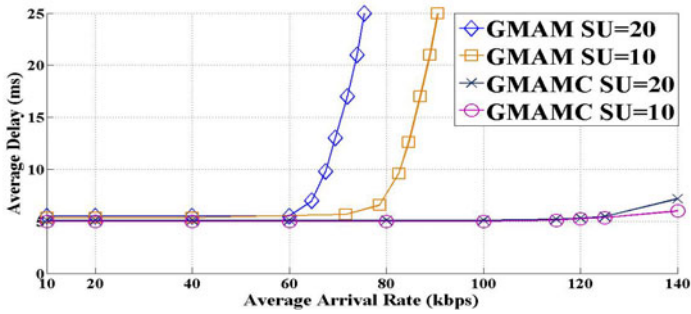**Fig. 2.** Delay probability difference between *GMAMC* and *GMAM*

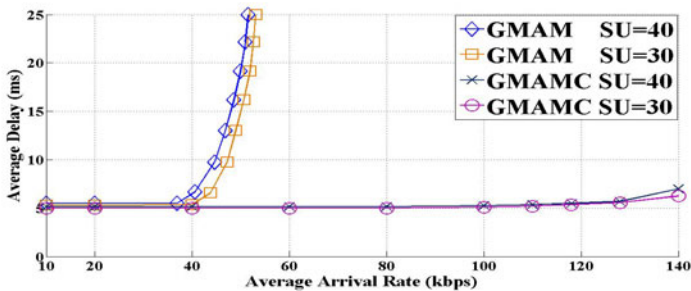**Fig. 3.** Delay performance under SU=10 and SU=20

Fig. 4. Delay performance under SU=30 and SU=40

Let the exponent of utility function b be $1, 2, 3, 4$ and 5 respectively. It can be seen in Figure 5 that the maximum lower delay stable region of about 7 ms is maintained from 40 to 180 *kbps* by *GMAMC* setting $b = 5$ of the average arrival rate in SUS.
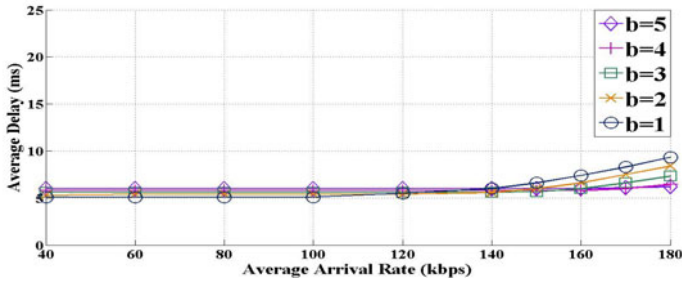
Fig. 5. Delay stable region of *GMAMC* with different trade-off exponent *b*

This is due to the adaptive trade-off between channel access efficiency and queue delay fairness by maximizing the utility function of queue delay.

5   Conclusion

In this paper, we propose an efficient distributed channel access scheme for secondary user in cognitive networks using the optimal match between allowable transmission ability and the required service quality. In addition, the large queue delay stable region is maintained by the proposed delay utility maximization based centralized control. Combining the schemes proposed in this paper with time window control based traffic control is our future research.

References

1. Zhao, Q., Tong, L., Swami, A., Chen, Y.: Decentralized cognitive MAC for opportunistic spectrum access in Ad Hoc networks: a POMDP framework. IEEE JSAC 25(3), 589–600 (2007)
2. Zhao, Q., Sadler, B.M.: A survey of dynamic spectrum access. IEEE Signal Processing Magazine 55(5), 2294–2309 (2007)
3. Laourine, A., Chen, S., Tong, L.: Queuing analysis in multichannel cognitive spectrum access: a large deviation approach. In: IEEE Infocom 2010 Preceedings (2010)
4. Chang, N., Liu, M.: Competitive analysis of opportunistic spectrum access strategies. In: Proc. IEEE INFOCOM 2008 (April 2008)
5. Wu, Y., Tsang, D.: Distributed power allocation algorithm for spectrum sharing cognitive radio networks with QoS guarantee. In: Proc. IEEE INFOCOM 2009 (April 2009)
6. Cao, L., Zheng, H.: Stable and efficient spectrum access in next generation dynamic spectrum networks. In: Proc. IEEE INFOCOM 2008 (April 2008)
7. Geirhofer, S., Tong, L., Sadler, B.M.: Cognitive Medium Access: Constraining Interference Based on Experimental Models. IEEE JSAC 26(1) (January 2008)
8. Song, G., Li, Y.(G.): Cross-layer optimization for OFDM wireless. networks—Part I: Theoretical Framework. IEEE Trans. Wireless Communications 4(2) (March 2005)
9. Kruse, R.L., Ryba, A.J.: Data Structures and Program Design in C++. Prentice-Hall, Englewood Cliffs (1999)

Superconvergence Analysis for Nonlinear Viscoelastic Wave Equation

Mingzhi Fan[1], Fenling Wang[1], and Dongwei Shi[2]

[1] School of Mathematics and Statistics, Xuchang University,
Xuchang 461000, People's Republic of China
[2] Department of Mathematics, Henan Institute of Science and Technology,
Xinxiang 453003, People's Republic of China
{fanmz,WFL}@xcu.edu.cn,
shidw99@163.com

Abstract. In this paper, a nonconforming finite element method for nonlinear viscoelastic wave equation is studied. By use of the new technique and sharp estimates, the superclose properties in L^2 norm and H^1 norm are derived, respectively. Moreover, the global superconvergence in H^1 norm is obtained through interpolated postprocessing technique.

Keywords: nonlinear viscoelastic wave equation, nonconforming finite element, superclose and superconvergence.

1 Introduction

Consider the following nonlinear viscoelastic wave equation

$$\begin{cases} u_{tt} - \nabla \cdot (a(u)\nabla u + b(u)\nabla u_t) = f(u), & (X,t) \in \Omega \times (0,T], \\ u(X) = 0, & (X,t) \in \partial\Omega \times (0,T], \\ u(X,0) = u_0(X), u_t(X,0) = u_1(X), & X \in \Omega, \end{cases} \quad (1)$$

where Ω is a convex polygonal domain in $\mathbb{R}^2$ with Lipschitz continuous boundary $\partial\Omega$, $[0,T]$ is the time interval, $u_0(X), u_1(X)$ are given functions, $a(u)$ and $b(u)$ denote viscosity and elasticity coefficients, respectively. Assume that

(i) there exist positive constants a_0, a_1, b_0, b_1 such that
$0 < a_0 \leq a(u) \leq a_1, 0 < b_0 \leq b(u) \leq b_1,$
(ii) $a(u), b(u)$ and $f(u)$ satisfy Lipschitz condition, i.e. there exists positive constant L such that $|\xi(u_1) - \xi(u_1)| \leq L|u_1 - u_2|$, $u_1, u_2 \in R, \xi = a, b, f,$
(iii) $a(u), b(u)$ and $f(u)$ are smooth functions.

As is known to all, there are many studies on superconvergence properties of conforming elements for linear differential equations (see[1]-[3]). [1]-[2] focused on the superconvergence and extrapolation of bilinear finite element for elliptic equation, Sobolev equation and viscoelastic wave equation. [3]showed that the superconvergence and extrapolation of ACM finite element for viscoelastic wave

equation discussed the superconvergence and extrapolation of bilinear finite element for elliptic equation, Sobolev equation and viscoelastic wave equation. [4]-[6] gave the error estimates of a nonconforming finite element for elliptic equation and Sobolev equation. In this paper, we establish a nonconforming finite element scheme for nonlinear viscoelastic wave equation(1), and derive superclose results in L^2 norm and H^1 norm by higher accuracy analysis, average-valued technique and the orthogonal property of the element. At the same time, the superconvergence result in H^1 norm is also gained through interpolated postprocessing technique.

2   Construction of the Element and Approximation Formulation

Let $\hat{K} = [-1,1] \times [-1,1]$ be a reference element on $\xi - \eta$ plane and $\hat{A}_1 = (-1,-1), \hat{A}_2 = (1,-1), \hat{A}_3 = (1,1), \hat{A}_4 = (-1,1)$ be its four vertices.

Next, we define the finite elements $\{\hat{K}, \hat{P}, \hat{\Sigma}\}$

$$\hat{P} = span\{1, \xi, \eta, \varphi(\xi), \varphi(\eta)\}, \hat{\Sigma} = \{\hat{v}_i, i = 1, 2, 3, 4, 5\},$$

where $\hat{v}_i = \dfrac{1}{|\hat{l}_i|} \displaystyle\int_{\hat{l}_i} \hat{v} d\hat{s}$, $\hat{v}_5 = \dfrac{1}{|\hat{K}|} \displaystyle\int_{\hat{K}} \hat{v} d\xi d\eta$, $\quad \varphi(t) = \frac{1}{2}(3t^2 - 1)$.

For all $\hat{v} \in H^1(\hat{K})$, the interpolation function $\hat{I}\hat{v}$ which are well-posed can be expressed as follows:

$$\hat{I}\hat{v} = \hat{v}_5 + \frac{1}{2}(\hat{v}_2 - \hat{v}_4)\xi + \frac{1}{2}(\hat{v}_3 - \hat{v}_1)\eta + \frac{1}{2}(\hat{v}_2 + \hat{v}_4 - 2\hat{v}_5)\varphi(\xi) + \frac{1}{2}(\hat{v}_3 + \hat{v}_1 - 2\hat{v}_5)\varphi(\eta).$$

Let $\Omega \subset \mathbb{R}^2$ be a convex polygonal domain with boundaries $\partial\Omega$ parallel to the axes, and Γ_h be a family of decomposition of Ω with $\bar{\Omega} = \bigcup_{K \in \Gamma_h} K$. $\forall K \in \Gamma_h$, let $O_K = (x_K, y_K)$ be the center of K, and h_x, h_y be the perpendicular distances between O_K and two sides of K which are parallel to the two coordinate planes, respectively. The K can be written as

$$K = [x_K - h_x, x_K + h_x] \times [y_K - h_y, y_K + h_y], \ h_K = \max\{h_x, h_y\}, \ h = \max_{K \in \Gamma_h} h_K.$$

The affine mapping $\mathcal{F}_K : \hat{K} \to K$ is defined as follows:

$$\begin{cases} x = x_K + h_x\xi, \\ y = y_K + h_y\eta. \end{cases}$$

Then, the associated finite element spaces V_h is defined by

$$V^h = \{v; v|_K = \hat{v} \circ \mathcal{F}_K^{-1}, \hat{v} \in \hat{P}, \forall K \in T_h, \int_F [v]ds = 0, F \subset \partial K\},$$

where $[v]$ denotes the jump of v across the boundary F, if $F \subset \partial\Omega$, then $[v] = v$.

The interpolation operator $I_h : H^1(\Omega) \rightarrow V^h$ is defined as $\forall v \in H^1(\Omega), I_h|_K = I_K, I_K v = (\hat{I}\hat{v}) \circ \mathcal{F}_K^{-1}$.

The weak form of (1) is to find $u \in H_0^1(\Omega)$ such that

$$\begin{cases} (u_{tt}, v) + (a(u)\nabla u, \nabla v) + (b(u)\nabla u_t, \nabla v) = (f(u), v), & \forall v \in H_0^1(\Omega), \\ u(X, 0) = u_0(X), u_t(X, 0) = u_1(X), & X \in \Omega. \end{cases} \quad (2)$$

The semi-discrete procedure of the nonconforming finite element method for (2) is to find $u^h \in V^h$ satisfying

$$\begin{cases} (u_{tt}^h, v) + (a(u^h)\nabla_h u^h, \nabla_h v)_h + (b(u^h)\nabla_h u_t^h, \nabla_h v)_h = (f(u^h), v), & \forall v \in V^h, \\ u^h(X, 0) = I_h u_0(X), u_t^h(X, 0) = I_h u_1(X), \end{cases}$$

$$(3)$$

where ∇_h denotes gradient which is defined piecewisely, that is $(\nabla_h u, \nabla_h v)_h = \sum_K \int_K \nabla u \nabla v dx dy$.

3 Superclose and Superconvergence Results

At first, we present two lemmas which are important to get superclose result.

Lemma 1. (see[7]) $\forall v \in V^h, \quad \|v\|_0 \leq C\|v\|_h$.

Lemma 2. (see[5])   For each $\varphi \in H_0^1(\Omega) \cap H^3(\Omega), \quad v \in V^h$, we have

$$|\sum_K \int_{\partial K} \frac{\partial \varphi}{\partial n} v ds| \leq Ch^2 |\varphi|_3 \|v\|_h, (\nabla_h \eta, \nabla_h v)_h = 0.$$

Theorem 1. Let u, u^h are solutions of (2) and (3), respectively. Assume that $a(u), b(u) \in W^{1,\infty}$, $u, u_t \in H^3(\Omega), u_{tt} \in H^2(\Omega)$, then we get the following optimal estimate

$$\|u^h - I_h u\|_h + \|u_t^h - I_h u_t\|_0 \leq Ch^2 \{\int_0^t (\|u_{tt}\|_2^2 + \|u\|_3^2 + \|u_t\|_3^2) ds\}^{\frac{1}{2}}.$$

Proof. Let $u - u^h = u - I_h u + (I_h u - u^h) = \eta + \theta, v \in V^h$, by (2) and (3), we see

$$(\theta_{tt}, v) + (a(u^h)\nabla_h \theta, \nabla_h v)_h + (b(u^h)\nabla_h \theta_t, \nabla_h v)_h$$
$$= -(\eta_{tt}, v) + ((a(u^h) - a(u))\nabla_h u, \nabla_h v)_h + ((b(u^h) - b(u))\nabla_h u_t, \nabla_h v)_h$$
$$- (a(u^h)\nabla_h \eta, \nabla_h v)_h - (b(u^h)\nabla_h \eta_t, \nabla_h v)_h + (f(u) - (f(u^h), v)$$
$$+ \sum_K \int_{\partial K} (a(u)\frac{\partial u}{\partial n} + b(u)\frac{\partial u_t}{\partial n}) v ds = \sum_{i=1}^6 A_i. \quad (4)$$

Choosing $v = \theta_t$ in (4) and using Young inequality, there holds

$$|A_1| \leq ch^2 \|u_{tt}\|_2 \|\theta_t\|_0 \leq ch^4 \|u_{tt}\|_2^2 + \|\theta_t\|_0^2. \quad (5)$$

Noting that $a(u)$ and $b(u)$ satisfy Lipschitz condition and using Cauchy inequality and Young inequality, we gain

$$|A_2| \le C\|u^h - u\|_0 \|u\|_{L^\infty(H^1)} \|\theta_t\|_h \le Ch^4 \|u\|_2^2 + c\|\theta\|_0^2 + C\|\theta_t\|_h^2, \qquad (6)$$

similarly

$$|A_3| \le Ch^4 \|u\|_2^2 + C\|\theta\|_0^2 + C\|\theta_t\|_h^2. \qquad (7)$$

Let $\overline{\Phi}|_K = \dfrac{1}{|K|} \displaystyle\int_K \Phi \, dx dy$, where $|K|$ is the area of K, then we get

$$|\Phi - \overline{\Phi}| \le Ch, \quad \Phi \in W^{1,\infty}. \qquad (8)$$

By Cauchy inequality, Young inequality, Lemma 2 and (8), we have the following estimates

$$
\begin{aligned}
|A_4| &= |((a(u^h) - a(u) + a(u) - \overline{a(u)} + \overline{a(u)})\nabla_h \eta, \nabla_h \theta_t)| \\
&\le |((a(u^h) - a(u))\nabla_h \eta, \nabla_h \theta_t)| + |((a(u) - \overline{a(u)})\nabla_h \eta, \nabla_h \theta_t)| \\
&\le C\|u^h - u\|_0 |\eta|_h |\theta_t|_h + Ch|\eta|_1 |\theta_t|_h \\
&\le Ch(\|\eta\|_0 + \|\theta\|_0)|u|_2 |\theta_t|_h + Ch^2 |u|_2 |\theta_t|_h \\
&\le Ch^4 |u|_2^2 + +C\|\theta\|_0^2 + C|\theta_t|_h^2 \\
&\le Ch^4 \|u\|_2^2 + C\|\theta\|_0^2 + C|\theta_t|_h^2,
\end{aligned} \qquad (9)
$$

similarly

$$|A_5| \le Ch^4 \|u\|_2^2 + C\|\theta\|_0^2 + C|\theta_t|_1^2, \qquad (10)$$

noting that $f(u)$ satisfies Lipschitz condition and using Cauchy inequality and Young inequality, we have

$$
\begin{aligned}
|A_6| &= |(f(u) - f(u^h), \theta_t)| \le C\|u - u^h\|_0 \|\theta_t\|_0 \\
&\le Ch^4 \|u\|_2^2 + C(\|\theta\|_0^2 + \|\theta_t\|_0^2),
\end{aligned} \qquad (11)
$$

by Lemma 2, then we gain that

$$|A_7| \le Ch^2(\|u\|_3 + \|u_t\|_3)\|\theta_t\|_h \le Ch^4(\|u\|_3^2 + \|u_t\|_3^2) + \|\theta_t\|_h^2. \qquad (12)$$

Based on (5)-(12), (4) can be rewritten as

$$
\begin{aligned}
(\theta_{tt}, \theta_t) &+ (a(u^h)\nabla_h \theta, \nabla_h \theta_t)_h + (b(u^h)\nabla_h \theta_t, \nabla_h \theta_t)_h \\
&\le Ch^4(\|u_{tt}\|_2^2 + \|u\|_3^2 + \|u_t\|_3^2) + C(\|\theta\|_0^2 + +\|\theta_t\|_0^2 + \|\theta_t\|_h^2),
\end{aligned} \qquad (13)
$$

that is,

$$
\begin{aligned}
(\theta_{tt}, \theta_t) &+ a_0(\nabla_h \theta, \nabla_h \theta_t)_h + (b(u^h)\nabla_h \theta_t, \nabla_h \theta_t)_h \\
&\le Ch^4(\|u_{tt}\|_2^2 + \|u\|_3^2 + \|u_t\|_3^2) + C(\|\theta\|_0^2 + \|\theta_t\|_0^2 + \|\theta_t\|_h^2) \\
&\quad + (a_0 - a(u^h)\nabla_h \theta, \nabla_h \theta_t),
\end{aligned} \qquad (14)
$$

then, we gain

$$(a_0 - a(u^h)\nabla_h \theta, \nabla_h \theta_t)_h \le C(\|\theta\|_h^2 + +\|\theta_t\|_h^2). \qquad (15)$$

Using (15), Lemma 1 and noting that $b(u)$ is bounded, (14) becomes

$$
\begin{aligned}
&\frac{1}{2}\frac{d}{dt}\|\theta_t\|_0^2 + \frac{a_0}{2}\frac{d}{dt}\|\theta\|_h^2 + b_0\|\theta_t\|_h^2 \\
&\leq Ch^4(\|u_{tt}\|_2^2 + \|u\|_3^2 + \|u_t\|_3^2) + C(\|\theta\|_h^2 + \|\theta_t\|_0^2) + b_0\|\theta_t\|_h^2,
\end{aligned}
\tag{16}
$$

by Gronwall's lemma, we derive that

$$
\|\theta_t\|_0^2 + \|\theta\|_h^2 \leq Ch^4\{\int_0^t (\|u_{tt}\|_2^2 + \|u\|_3^2 + \|u_t\|_3^2)ds.
$$

The proof is completed.

In order to gain the global superconvergence estimate, we adopt the interpolation postprocessing operator $\prod_{2h}$ (see[6]) which satisfies the following formula on $\bar{K}$

$$
\prod_{2h}\omega|_{\bar{K}} \in Q_2(\bar{K}), \forall \omega \in C(\bar{K}),
\tag{17}
$$

where $\bar{K} \in T_h$ consists of four neighboring elements, $Q_2(\bar{K})$ is the space of biquadratic polynomial on $\bar{K}$ and $C(\bar{K})$ is the space of continuous function on $\bar{K}$. The operator $\prod_{2h}$ satisfies

$$
\prod_{2h}I_h\omega = \prod_{2h}\omega,
\tag{18}
$$

and

$$
\begin{cases}
\prod_{2h} : H^1(\bar{K}) \to P_2(\bar{K}), \\
\int_{l_i}(\prod_{2h}u - u)ds = 0, \ , i = 1,2,3,4. \\
\int_{K_1 \bigcup K_3}(\prod_{2h}u - u)dxdy = 0, \quad \int_{K_2 \bigcup K_4}(\prod_{2h}u - u)dxdy = 0.
\end{cases}
\tag{19}
$$

Lemma 3. (see[6]) The following estimates are true for the interpolation operator $\prod_{2h}$

$$
\prod_{2h}I_h u = \prod_{2h}u,
\tag{20}
$$

and

$$
\|\prod_{2h}u - u\|_1 \leq Ch^2\|\omega\|_3, \omega \in H^3(\Omega),
\tag{21}
$$

$$
\|\prod_{2h}v\|_1 \leq C\|v\|_1, \forall v \in V^h.
\tag{22}
$$

Theorem 2. Suppose that u, u^h are solutions of (2) and (3), respectively and $u, u_t \in H^3(\Omega), u_{tt} \in H^2(\Omega)$, there yields

$$
\|\prod_{2h}u^h - u\|_1 \leq Ch^2\{[\int_0^t (\|u_{tt}\|_2^2 + \|u\|_3^2 + \|u_t\|_3^2)ds]^{\frac{1}{2}} + \|u\|_3\}.
\tag{23}
$$

Proof. By Theorem 1 and Lemma 3, there holds

$$
\begin{aligned}
\|\prod_{2h}u^h - u\|_1 &\leq \|\prod_{2h}u^h - \prod_{3h}I_h u\|_1 + \|\prod_{2h}I_h u - u\|_1 \\
&= \|\prod_{2h}(u^h - I_h u)\|_1 + \|\prod_{2h}u - u\|_1 \leq C\|(u^h - I_h u)\|_1 + ch^2\|u\|_3 \\
&\leq Ch^2\{[\int_0^t (\|u_{tt}\|_2^2 + \|u\|_3^2 + \|u_t\|_3^2)ds]^{\frac{1}{2}} + \|u\|_3\}.
\end{aligned}
\tag{24}
$$

We complete the proof.

References

1. Lin, Q., Lin, J.F.: Finte Element Methods: Accuracy and Improvement. Science Press, Beijing (2006)
2. Lin, Q., Zhang, S.H., Yan, N.N.: Asymptotic error expansion and defect correction for Sobolev and Viscoelasticity type equations. J. Comput. Math. 16(1), 51–62 (1998)
3. Shi, Y.H., Shi, D.Y.: Superconvergence analysis and extrapolation of ACM finite element methods for Viscoelasticity equation. Appl. Math. 22(3), 534–541 (2009)
4. Lin, Q., Tobiska, L., Zhou, A.H.: Superconvergence and extrapolation of nonconform low order finite elements applied to the poisson equation. IMA J. Numer. Anal. 25, 160–181 (2005)
5. Shi, D.Y., Mao, S.P., Chen, S.C.: An anisotropic nonconforming finite element with some superconvergence results. J. Comput. Math. 23(3), 261–274 (2005)
6. Shi, D.Y., Wang, H.H., Guo, C.: Anisotropic rectangular nonconforming finte element analysis for Sobolev equations. Appl. Math. & Mech. 29(9), 1203–1214 (2008)
7. Shi, D.Y., Zhang, Y.R.: A nonconforming anisotropic finite element approxiemation with moving grids for stokes problem. J. Comput. Math. 24(5), 561–578 (2006)

Design of Acid Rain Observing Instrument Based on LPC2368

Sujuan Zhang[1,2,*], Jihua Hong[2], and Shangchang Ma[1,2]

[1]CMA. Key Laboratory of Atmospheric Sounding, 610225, Chengdu, China
[2]Chengdu University of Information Technology, 610225, Chengdu, China
{suezsj,mscjs}@cuit.edu.cn, hongjihuamail@126.com

Abstract. The acid rain observation system usually includes the measurements and analysis of pH value and electric conductivity. The measuring principles of pH value and electric conductivity are discussed in the paper. An acid rain observing instrument is developed, which uses ARM microcomputer LPC2368 as control core, and pH composite glass electrode, platinum black electric conductivity electrode and platinum resistance –Pt100 as sensitive devices. It not only has high measuring accuracies by using the AD7792 as analog-digital conversion chip, but also has advantages in low cost, small volume and low power consumption. In addition, SD card is adopted to store the measuring data and CAN bus is used to communicate with PC to build acid observing network. The tests indicate that the acid rain observing instrument services high measuring accuracies for the pH value and electric conductivity of acid and provides important reference information for environmental monitoring.

Keywords: acid rain, pH value, electric conductivity.

1 Introduction

Acid rain usually refers to the atmospheric precipitation in which the pH of water is less than 5.6. Rain, snow, hall, and other forms of precipitation containing the mild solutions of sulfuric and nitric acids fall to the earth as acid rain [1].The pollution of acid rain has become one of the main factors resulted in the global ecological crisis. Acid rain observation provides precious data for the analysis on the temporal and spatial distribution and the long-term trend of acid rain. Acid rain observation also provides an important scientific evidence for air pollution control and acid rain control. It is mainly including the measurements and analysis of pH value and electric conductivity. The regional background atmosphere stations also observe the chemical constituents of acid rain [2].

2 Measuring Principle and Method

The acidity and alkalinity of atmospheric precipitation are both expressed by pH value. Generally, pH value is the negative logarithm of hydrogen ion concentration inside liquid which is measured at room temperature 25℃.

The automatic measuring method of pH value mainly refers to potential measurement method with pH composite glass electrode. It makes quantitative analysis of measured liquid by measuring the electromotive force of galvanic cell. The voltage of galvanic cell consists of two half-cells: one is called reference electrode, the potential of which is only related to the ionic activity of the reference solution, and another is called measuring electrode, which contacts to the measured liquid. The voltage between the two electrodes satisfies Nernst equation [3], so

$$E = E_O + KT(PH_x - PH_O)   \tag{1}$$

A composite glass electrode is used in this paper, which consists of glass electrode and AgCl electrode. Glass electrode is used as indicator electrode while AgCl electrode is used as reference electrode. Galvanic cell is generating when composite glass electrode is inserted in the measured liquid. Measure the voltage of the glass electrode and the temperature of the rain and put them into the formula (1), and get

$$V = K(273.15 + t)(PH_x - PH_O)   \tag{2}$$

The conductive capacity of atmospheric precipitation reflects the precipitation is clean or polluted, which is used electric conductivity for measurement representation. The electric conductivity of rain solution is usually expressed by the K, and measured by an electric conductivity electrode, which consists of a pair of parallel electrodes, with known area and space.

Generally, the measurement result of the electric conductivity is measured under room temperature 25℃. Based on the large number experimental results, the formula of temperature compensation for electric conductivity is expressed by [4]

$$k_{25} = \begin{cases} k_t /(0.0169t + 0.5583) & 1 \le t \le 10 \\ k_t /(0.0180t + 0.5473) & 11 \le t \le 20 \\ k_t /(0.0189t + 0.5281) & 20 \le t \le 30 \\ k_t /(0.022t - 0.45) & \text{others} \end{cases}   \tag{3}$$

3 System Design and Implementation

3.1 System General Design

The system composition block diagram of the acid rain observing instrument is shown as Fig. 1. LPC2368 is an ARM-based microcontroller which incorporates 10/100 Ethernet MAC, USB 2.0 Full Speed interface, UARTs, CAN channels, SPI interface, Synchronous Serial Ports (SSP), I^2C interfaces, I^2S interface, SD/MMC memory card interface, 10 bit A/D converter etc. AD7792 contains a low noise 16-bit Σ-Δ ADC with three differential analog inputs, an low noise programmable gain instrumentation amplifier, and two programmable current sources.
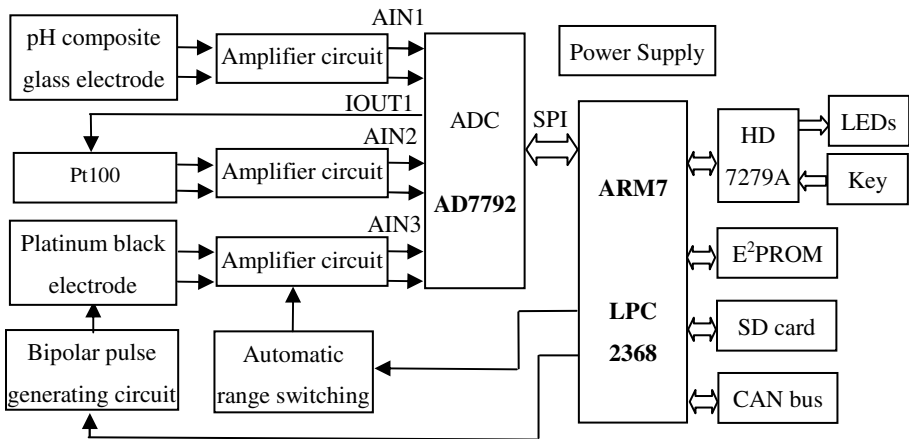
Fig. 1. System composition block diagram

The pH composite glass electrode is used for measuring pH value. The voltage across the composite glass electrode is transferred into AIN1 on the AD7792 for data acquisition after being amplified. The platinum black electrode is applied in the measurement of electric conductivity. The excitation source adopts bipolar pulse to reduce the electrode polarization. The resistance between the two electrodes is measured by using the operational amplifier method and the output voltage of amplifying circuit is transferred into AIN2 on the AD7792. The platinum resistance-Pt100 is used for measuring temperature of the rain solution. The excitation source adopts the one excitation current-OUT1of the AD7792, and the voltage between the Pt100 where current is flowing through is transferred into AIN3 on the AD7792 after differential amplification.

LPC2368 accomplishes the data acquisition control by communicating with the AD7792 through SPI bus, calculates the collected data to get pH value, electric conductivity and temperature of rain solution, which are stored in E2PROM chip or SD card and displayed on the LED digitrons. The system can select the calibration function or automatic measurement function by keystroke identifying. The LEDs display and keystroke identifying are accomplished by using HD7279A, which is an intelligent control chip for 8-bit LED digitrons and 64-key keyboard with serial interface. The system also has a CAN bus interface which can be used to communicate with PC to build acid observing network.

3.2   Hardware Circuit Design

3.2.1   P.h Value Measurement Circuit Design

The galvanic cell which is generating while composite glass electrode is inserted in the measured liquid is a signal source with high internal resistance, reached to $10^{12}\Omega$. The input current is so weak (about pA scale) that the measuring amplifier circuit has to have large enough input impedance to obtain the accuracy voltage signal of the

electrode. The CA3140 BiMOS operational amplifier is used in the amplifying circuit for the measuring signal, which combines the advantages of high voltage PMOS transistors with high voltage bipolar transistors on a single monolithic chip. The two output potentials of the pH electrode are amplified symmetrically by using the two CA3140 amplifiers. It is not needed to translate differential signal to single signal because the AD7792 supports differential analog input.

3.2.2   Electric Conductivity Measurement Circuit Design

The platinum black electrode whose electrode constant is equal to 1 is used in the paper. The excitation source is needed in the process of measuring the electric conductivity of the rain solution. In order to reduce the electrode polarization as low as possible, 1KHZ bipolar pulse signal is used as excitation source. The resistance of the electrodes is measured by using the operational amplifier method which can switch measuring range by selecting different feedback resistances automatically. The bipolar pulse signal frequency is controlled by LPC2368. The 1V reference voltage signal is generated by the MC1403, through a unity –gain voltage follower, and then through an inverting amplifier. The output voltages of unity gain voltage follower and of the inverting amplifier connect to the input pins of the CD4051 and one of them will be selected to connect to the output of the CD4051 controlled by LPC2368. The output voltage then through a unity gain voltage follower is the needed$\pm$1V bipolar pulse source and its frequency is related to the starting timer values of LPC2368.

When the electric conductivity electrode is inserted in the solution whose measurement range is between 0 to 50mS·m^{-1}, the resistance of the electrode can be varied from 20 Ω to100 MΩ. According to that the ADC can measure voltage from 0 to 2.5V, 8 measuring ranges are designed to improve the accuracy. Measuring ranges switching is implemented through two CD4051s which are digitally controlled by LPC2368. One CD4051 is used to switch feedback resistances, and the other CD4051 is used to lead the voltage across the feedback resistances to eliminate the interference signal caused by "ON" resistance of CD4051.

3.2.3   Temperature Measurement Circuit Design

Temperature measurement uses 4-wire platinum resistance Pt100 to eliminate the interference signal caused by the lead wires of the resistance. The excitation current OUT1 of the AD7792 flows through the platinum resistance, then connects to the ground of the AD7792 as a current loop. With using 1 mA excitation current, the voltage across the platinum resistance is about from 100 to 120 mV. The voltage signal needs amplifying with impedance matching, and then connects to AIN2 on the AD7792. The differential amplifying circuit with two OP07 ultra low offset voltage operational amplifiers is similar with the amplifying circuit design of pH electrode. Here is not illustrated in detail.

3.2.4   Data Store Circuit Design

The system adopts E2PROM chip--AT24C512 for storing calibrating parameter data, and SD card for storing measuring result data. LPC2368 incorporates I^{2}C interface and SD/MMC memory card interface, that makes the circuit connect simply.

3.3   Realization of Software Function

The system consists of measurement function and calibration function. The software program is partitioned several modules, such as initialization, pH value sampling, electric conductivity sampling, temperature sampling, key scanning, displaying, data processing, data storage and data sending subroutine, etc.

The system initialization subroutine initializes timer, interruption, AD7792, SD/MMC modules. In key scanning subroutine, the key values are got through interruption, and decide to implement the measurement or calibration function.

In pH sampling subroutine, the AD7792 is controlled by LPC2368 with SPI interface to accomplish the A/D conversion on AIN1 channel. Electric conductivity sampling subroutine is used to control bipolar pulse generating, automatic range switching, and electric conductivity sampling. Bipolar pulse frequency is generated from the PWM of LPC2368, the positive and negative level is controlled by CD 4051.Range switching is controlled by two pieces of CD 4051. The AD7792 is controlled by LPC2368 to accomplish the A/D conversion on AIN2 channel. The temperature sampling subroutine is responsible for sampling voltage in temperature sensor circuit, the 1mA constant current source is generated from the IOUT1 of AD7792, and the AD7792 accomplish the A/D conversion on AIN3.

In data processing subroutine, the calculation parameters are accessed from AT24C512. The pH value, conductivity and temperature are sampled several times and got average. Temperature compensation is taken into consideration as pH value and electric conductivity of acid rain calculated. In displaying subroutine, the data of rain pH value, conductivity and temperature are extracted in decimal, each part of data is sent to HD7279A by interruption from timer to be displayed in real-time. In data storage subroutine, the measuring time, pH value, electric conductivity value and the temperature value is stored into the SD card as the measuring result is determined.

Table 1. Experiment results of the acid rain observing instrument

Temperature t （℃）			pH			Electric conductivity (mS·m^{-1})		
Actual value	Measuring value	Absolute error	Actual value	Measuring value	Absolute error	Actual Value	Measuring value	Absolute error
15.1	14.9	1.32%	5.98	5.97	0.17%	57.22	56.76	0.80%
14.9	14.8	0.67%	5.97	5.98	0.18%	56.36	56.79	0.76%
15.2	15.0	1.32%	6.01	6.02	0.17%	57.05	57.16	0.19%
14.8	14.7	0.68%	5.99	6.01	0.33%	56.18	56.32	0.30%
15.0	15.1	0.67%	6.02	6.03	0.17%	56.57	57.03	0.81%

4   Tests and Conclusions

The experiment was used with three sensors: pH composite glass electrode, platinum black electric conductivity electrode and platinum resistance Pt100. Five rain solution samples were measured by using two groups of different instruments. One is the acid

rain observing instrument system designed in this paper and the other is consisted by the pH special meter and electric conductivity special meter. Given the measurements by the pH special meter and electric conductivity special meter are the actual values, and the other group measurements are the measuring values. Compared with the two measurements, the experiment results are shown as table 1.

The tests indicate that the acid rain observing instrument is well corresponding to the pH special meter and electric conductivity special meter. The acid rain observing instrument can measure the pH value and electric conductivity by one time. It also has the automatic temperature compensation function and the calibration function, which makes the acid rain observing instrument featuring high measuring accuracy, convenient operation.

References

1. China Meteorological Administration, Acid Rain Observing Standard, China Meteorological, pp. 1-3 (2005)
2. Ding, G., Xu, X., Wang, S., et al.: Database from the Acid Rain Network of China Meteorological Administration and Its peliminary Analyses. Quarterly Journal of Applied Meteorology, 85–94 (2004)
3. Yang, S., Yin, J., Zhong, C., et al.: Study and Implementation of pH Intelligent Measuring Technology. Instrument Technique and Sensor, 7–9 (2003)
4. Jia, K., Zhang, X., Lin, B., et al.: The Intelligent on-line Conductivity Analyzer Based on MSC1210 Single Chip Compute. Process Automation Instrument 28(5), 7–9 (2007)

A Elastic Plastic Damage Model for Concrete Considering Strain Rate Effect and Stiffness Damping

Qi Hu[1], Li Yun-Gui[2], and Lu Xilin[3]

[1] Institute of structural Engineering and Disaster Reduction,
Tongji University, Shanghai, China
`qihu_810@163.com`
[2] Institute of building Engineering software,
China Academy of Building Research, Beijing, China
`liyungui@china.com`
[3] Institute of structural Engineering and Disaster Reduction,
Tongji University, Shanghai, China
`lxlst@mail.tongji.edu.cn`

Abstract. Concrete exhibits strain-rate sensitivity during dynamic tests. In this paper, the elastic plastic damage model for concrete under static loading, previously proposed by the authors, is extended to account for the concrete strain-rate dependency on the basis of the viscous regularization. Stiffness damp stress is introduced to the model to consider the energy dissipation at the material scale. Tension plastic strain is introduced to the model to slow down subsidence and damage development. The proposed model is developed in ABAQUS. The nonlinear analysis of Koyna concrete dam indicates that the stiffness damp effect can observably enhance the stability of the dynamic implicit analysis. The introduction of tension plastic strain can also improve the calculation stability and efficiency, as well the strain-rate sensitivity can affect the displacement reflection of the structure and improve the calculation stability.

Keywords: stiffness damp, strain-rate sensitivity, concrete, constitutive model.

1 Introduction

Concrete structures are likely to suffer dynamic loads like impacts, earthquakes, explosions and so on. Concrete exhibits strain-rate sensitivity under dynamic loads, which visible effects (when compared to quasi-static tests) are substantial gains in the peak strengths, as well as decrease of the stress-strain non-linearities. Researchers began to notice that phenomenon a long time ago, and proposed a lot of theories to describe the concrete constitution behavior under dynamic loads, most of which are complex in algorithm. The most widely used models are still the empirical models[1].

Faria et. al. (1998)[2] incorporated the capability for simulating the concrete rate-sensitivity into their model, via slight modifications on the kinematics for the damage thresholds and with the addition of fluidity parameters and flow functions as in a classic Perzina regularization. Wu et. al. (2005)[3] proposed a concrete model including rate-sensitivity in a similar way to Faria et. al. (1998), and showed the effect of rate-sensitivity through numerical simulation. Damage Mechanics can essentially

describe the macroscopic nonlinear behaviors of concrete caused by the development
of microcracks, in which the evolvement of damage variable is used to simulate the
development of microcracks inside the concrete material. This is done to extend the
evolvement of the damage variables with rate dependent viscous regularization to
describe the retarded development of microcracks caused by high strain rate. Based on
the above analysis, the damage variables of the proposed model[1] are extended with
rate-dependent viscous regularization, so as to describe the rate-sensitivity.

Damping is a peculiar energy dissipation mechanism, which happens during
structure vibration. Presently, the Rayleigh damping is the most widely used; it
assumes that the damping matrix is a linear combination of the mass matrix and the
stiffness matrices. Because the mass-proportional damping matrix introduces a
physically inadmissible dissipation under rigid body motions, and it alone could not
provide sufficient dissipation to suppress the high-frequency numerical noises, many
researchers[3,4] just account for the stiffness-proportional damping matrix.

In this paper the plastic-damage model proposed by author[1] is extended into its
rate-dependent version to embody the strain rate effect. Regarding the energy
dissipations, a damping model on the material scale is proposed and incorporated into
the developed rate-dependent plastic-damage model. Finally, the effects of stiffness
damping and strain rate on structural analysis in ways of structural displacement and
stability is discussed through numerical simulation.

2   Plastic Deformation

To consider the tension plastic strain $\varepsilon_{ij}^{\ p}$ in [1,2] is amended to the following form:

$$d\varepsilon_{ij}^{\ p} = \beta_p E \cdot H(H(d(d^-)) + H(d(d^+))) \left\langle I_{\bar{\sigma}_{ij}} : d\varepsilon_{ij} \right\rangle D_0^{-1} : I_{\bar{\sigma}_{ij}} \tag{1}$$

β_p controls the proportion of plastic strain. β_p can be determined as follows:

$$\beta_p = 0.1 + 0.45 \cdot (1 - H(\bar{\hat{\sigma}}_2) \cdot \sqrt{\bar{\hat{\sigma}}_2/\bar{\hat{\sigma}}_3} + 0.45 \cdot (1 - H(\bar{\hat{\sigma}}_1)) \cdot \sqrt{\left|\bar{\hat{\sigma}}_1/f_c\right|} \tag{2}$$

Fig.1 shows the influence of β_p on the uniaxial tension constitutive curve. We can
see from Fig.1 that with the increase of β_p the tension plastic strain is increase.
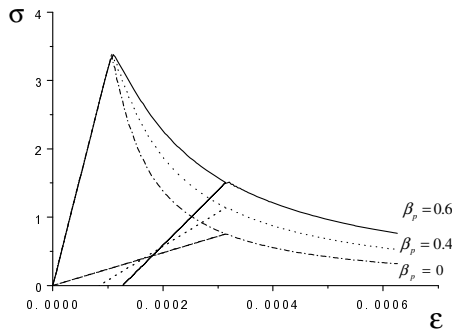

Fig. 1. The Influence of β_p on tension curve under uniaxial loading

3   Damping

To account for the energy dissipation on the material level, this paper introduces stiffness damping into the proposed plastic damage constitutive model, only considering stiffness damping in Rayleigh damping, the damping of undamaged material is as follows:

$$\bar{\sigma}_{vis} = \beta_k \cdot E_{0ijkl} \cdot \dot{\varepsilon}_{ij} \tag{3}$$

Where β_k is the stiffness combination coefficient, E_{0ijkl} is elastic modulus and $\dot{\varepsilon}$ is strain rate, viscous damping stress σ_{vis} can be calculated as :

$$\sigma_{vis} = (1-d) \cdot \bar{\sigma}_{vis} = \beta_k \cdot (1-d) \cdot E_{0ijkl} \cdot \dot{\varepsilon}_{ij} \tag{4}$$

In the plastic damage constitutive model:

$$\sigma_{ij} = (1-d)\bar{\sigma}_{ij}, \quad \bar{\sigma}_{ij} = E_{0ijkl}\varepsilon_{ij}^e = E_{0ijkl} \cdot (\varepsilon_{ij} - \varepsilon_{ij}^p) \tag{5}$$

total stress can be expressed as:

$$\sigma_{tot} = \sigma + \sigma_{vis} = (1-d) \cdot (\bar{\sigma} + \bar{\sigma}_{vis}) \tag{6}$$

4   Applications

The proposed model is used to analyze the Koyna concrete dam. The parameters of the material are $\rho_0 = 2643 kg/m^3$, $E_0 = 31027 MPa$, $v_0 = 0.2$, $\beta_p = 0.5$, the tensile strength is estimated to be $f_t = 2.9 MPa$, the compressive strength $f_c = 24.1 MPa$ The stiffness damping parameter is b=0.0033 to provide 3 percent damping at the fundamental vibration period. The full reservoir is represented by added masses at the upstream face nodal points. The finite element mesh of the dam, shown in Fig. 2, uses 760 four-node plane stress quadrilateral isoparametric elements.

Table 1. The nature frequency of Koyna concrete dam

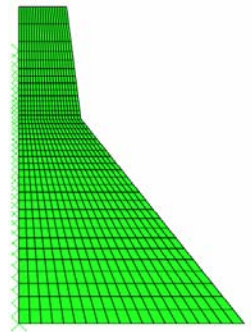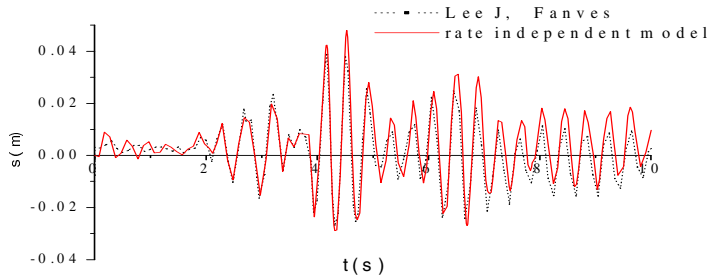| vibration model	nature frequency （rad/s）		
	this model	Chopra A.K[6]	Wu Jianying
1	18.86	19.27	18.85
2	49.98	51.5	49.95
3	68.16	67.56	68.13
4	98.26	99.73	98.23

Fig. 2. Koyna concrete dam

Fig. 3. The result of rate independent model

In Fig. 3 the numerical result is compared with the results of Lee.J and Fanves G.L(1998)[5]. We can see from Fig. 3 that the results match well.
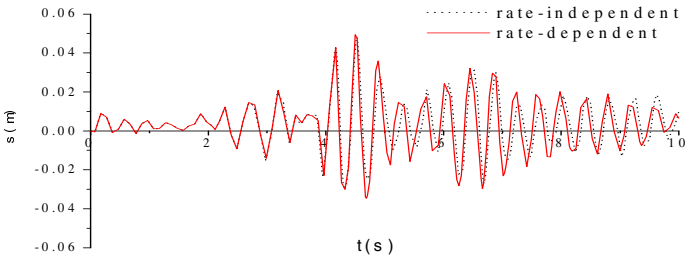

Fig. 4. The displacement of the top of the dam

From Fig. 4 we can see that the result of the rate dependent model is slightly bigger than the rate independent model, which agrees with Wu.et.al. (2006)[3].

5   Conclusion

In this paper, the elastic plastic damage model for concrete under static loading proposed by the authors is extended to account for the strain-rate effect through viscous regularization of the damage threshold. Stiffness damp stress is incorporated into the model to consider the energy dissipation at the material scale. Tension plastic strain is introduced to the model to retard subsidence and damage development. The proposed model is developed in ABAQUS and the simulation of Koyna concrete dam indicates that the model of this paper is efficient when analyzing practical structure.

References

1. Qi, H., Li, Y.-G., Lu, X.: A Elastic Plastic Viscous-Damage Model for Concrete Considering Strain Rate Effect and Application. In: The 3rd International Conference on Computational Intelligence and Industrial Application, vol. 3, pp. 146–151 (2010)
2. Faria, R., Oliver, J., Cervera, M.: A strain-based plastic viscous-damage model for massive concrete structures. Int. J. Solids and Structures 35(14), 1533–1558 (1998)
3. Wu, J., Li, J.: Unified elastoplastic damage model for concrete. Journal of Architecture and Civil Engineering 22(4), 15–21 (2005) (in Chinese)
4. Faria, R., Vila Pouca, N., Delgado, R.: Seismic benchmark of a R/C wall: numerical simulation and experimental validation. Journal of Earthquake Engineering 6(4), 473–498 (2002)
5. Lee, J., Fanves, G.L.: A plastic-damage concrete model for earthquake analysis of dams. Earthquake Engineenng and Structural dynamics 27(9), 937–956 (1998)
6. Chopra, A.K., Chakrabarti, P.: The koyaa earthquake and the damage to koyna dam. Bulletin of the Seismological Society of America 63(2), 381–397 (1973)

Some Properties of the Continuous Single-Valley Expansion Solution to the Feigenbaum's Functional Equation[*]

Huaming Wu[1] and Risong Li[2]

[1] School of Mathematics and Computational science,
Zhanjing Normal College, Zhanjiang, 524048, China
`wuhuam3329@126.com`
[2] School of science, Guangdong Ocean University, Zhanjiang,
524025, China

Abstract. In this paper, some fundamental properties of the continuous single-valley expansion solution to Feigenbaum's functional equation were obtained. For $\lambda \in (0,1)$ and $p \geq 2$, we will discuss the completeness of the function space which consists of unique continuous single-valley expansion solution (resp. unique continuous non-single-valley expansion solution) to p-order Feigenbaum's functional equation. Let $p, q \geq 2$. It was proved that the system of equations

$$\begin{cases} f(x) = \frac{1}{\lambda} f^p(\lambda x), f(0) = 1, (\lambda \in (0,1) \ \ for \ \ decision) f(x), x \in [0,1]; \\ f(x) = \frac{1}{\lambda} f^q(\lambda x), f(0) = 1, (\lambda \in (0,1) \ for \ \ decision) f(x), x \in [0,1]. \end{cases}$$

does not have continuous single-valley expansion solution.

Keywords: Feigenbaum's map, Functional equation, Continuous single-valley expansion solution.

MR(2000) Subject Classification: 39B52.

1 Introduction

Let I be any close interval and $C^0(I, I)$ the set of all continuous self-map on I. In order to research and explain the common phenomena of a class of single parameter, Feigenbaum [1,2] put forward some geometric hypothesis on some function space. One of the fundamental and important hypothesis is to assume that the functional equation

$$\begin{cases} f(x) = \frac{1}{\lambda} f^2(\lambda x), \lambda \in (-1,1) \, for \ \ decision \\ f(0) = 1, f \in C^0([-1,1],[-1,1])) \end{cases} \tag{1.1}$$

has solution with some condictions. There are a lot of research papers on this area, for example[3,4,5]. The second class of Feigenbaum functional equtions that it is equivalent to Eqution (1.1), but more directly are given in [6]

$$\begin{cases} f(x) = \frac{1}{\lambda} f^p(\lambda x), \lambda \in (0,1) \text{ for decision} \\ \quad f(0) = 1, f \in C^0([0,1],[0,1])) \end{cases} \tag{1.2}$$

Also, an effective method to construct all continuous single-valley solution is obtained in [6]. In [7], the authors continue to study the properties of the continuous single-valley expansion solutions of Eqution 1.2 restricted on $[\lambda,1]$ and obtain an good method to construct these solutions. The paper [8] generalize the results of [7] and research the properties of the continuous single-valley expansion solutions of generalization Feigenbaum functional equtions with p order（$p \geq 2$）

$$\begin{cases} f(x) = \frac{1}{\lambda} f^p(\lambda x), \lambda \in (0,1), \text{ for decision} \\ \quad f(0) = 1, f \in C^0([0,1],[0,1])) \end{cases} \tag{1.3}$$

and give an effective method to constructed these kind of solutions.

The paper [9] generalize the results of [7,8] and research properties of the continuous single-valley expansion solutions of Equation (1.3) restricted on $[\lambda,1]$ and also and give an effective method to constructed these kind of solutions. In [10], they discuss topology conjugation of the 3 order Feigenbaum map restricted on non-wandering set. By using the subshift of finite type, they prove that for any two 3 order Feigenbaum map satisfying some condiction restricted on non-wandering set is topological conjugation. In [11], they study some properties of p order Feigenbaum map f. They prove that Kneading sequence of f is the fixed point of some transformation on signal space and f restricted on characteristic set is the factor of some transformation **subshifts of finite type**. In this paper, we continue to discuss the properties of the continuous single-valley expansion solutions of generalized Feigenbaum functional equations and obtain some basic properties.

2   Preliminaries

Definition 1 [9] f is called the continuous single-valley solution of Equation (1.3), if it satisfies

(1) f is its continuous solutions;

(2)   there is a $a \in (\lambda,1)$ such that $f(a) = 0$ and f is strictly decreasing on $[0,a]$, but strictly ascending on $[a,1]$.

Definition 2 [9] f is called the continuous single-valley expansion solution of Equation (1.3), if it satisfies

(1) f is its continuous solution;

(2) f is single-valley on $[\lambda,1]$, i.e.,   there is a $a \in (\lambda,1)$ such that $f(a) = 0$ and $f\big|_{[\lambda,a]}$ is strictly decreasing , but $f\big|_{[a.1]}$ is strictly ascending.

For the conceptions of p order Feigenbaum map and single-valley p order Feigenbaum map, please see [10]. Clearly, continuous single-valley solution must be continuous single-valley expansion solution. From the paper [9], we can see that continuous single-valley solution just has two kinds: single-valley and non-single-valley. Moreover, if f is the solution of Equation (1.3), then

$$f(x) = \tfrac{1}{\lambda^n} f^{p^n}(\lambda^n x), \quad (1.4)$$

is hold for any $n \geq 0$ and any $x \in [0,1]$.

Lemma 1 (The principle of limit exists) The monotone bounded sequence must has limit.

Definition 3 [13] Let X be a set and (Y,ρ) a metric space. Set Y^X be the set of all map from X to Y . Define

$$\tilde{\rho}: Y^X \times Y^X \to R$$

by

$$\tilde{\rho}(f,g) = \begin{cases} 1, \exists x \in X \text{ such that } \rho(f(x),g(x)) \geq 1 \\ \sup\{\rho(f(x),g(x))|x \in X\}, \text{others} \end{cases}, \quad f,g \in Y^X .$$

It is easy to prove that $\tilde{\rho}$ is a metrics of Y^X and $\tilde{\rho}$ is called the uniform convergence metrics. The topology of Y^X inducted by the uniform convergence metrics $\tilde{\rho}$ is called uniform convergence topology. Topological space $\left(Y^X, J_{\tilde{\rho}}\right)$ is called map space. When X is a topological space, $C^0(X,Y)$ the set of all continuous map as a metric subspace is called continuous map space and its metrics is called the uniform convergence metrics. And its topology is called uniform convergence topology [13]. Assume that Z_+ is the set of all positive integers, $C^0(I,I)$ uniform convergence topology. Other notions and concepts of this paper, please see [9].

Definition 4 [13] Let X be a set and (Y,ρ) a metric space. The sequence $\{f_i\}_{Z_+}$ of Y^X is called uniform convergent to map $f \in Y^X$, if for $\forall \varepsilon > 0$, $\exists N > 0$ such that when $i > N$, we have $(f_i(x), f(x)) < \varepsilon, \forall x \in X$.

Lemma 2 [13] For any close metric subspace of a complete metric space is also complete metric space.

Lemma 3 [13] Let X be a topological space and (Y, ρ) a metric space. Then the set $C^0(X, Y)$ is a close set of map space Y^X. So metric space $C^0(X, Y)$ is a complete metric space.

Lemma 4 [13] Let X be a topological space and (Y, ρ) a metric space. The sequence $\{f_i\}_{Z_+}$ of the metric space Y^X convergent to map $f \in Y^X$ if and only if $\{f_i\}_{Z_+}$ uniform convergent to map $f \in Y^X$.

3   Results and Proofs

Property 1 $f^{p^n}(\lambda) \to \lambda, (n \to \infty)$.

Proof   By (1.3), we have $f^p(0) = \lambda$ anf by (1.4), we have $f^{p^n}(0) = \lambda^n$. Therefore $f^{p^n - p}(\lambda) = f^{p^n}(0) = \lambda^n$. So $f^{p^n}(\lambda) = f^p(\lambda^n) \to f^p(0) = \lambda, (n \to \infty)$.

Property 2 For $\forall x \in [0, \lambda], 1 \le i \le p - 1$ and $\forall k \in \{0, 1, 2, \cdots\}$, we have $w \ge f^{kp}(x)$.

Proof By $f^p(x) = f^p(\lambda \cdot \frac{1}{\lambda} x) = \lambda f(\frac{1}{\lambda} x) \le \lambda$ and lemma 4, we have

$$f^i(x) > \lambda \ge f^p(x) \ i = 1, 2, \cdots, p - 1.$$

So $f^{p+1}(x) > \lambda, f^{p+2}(x) > \lambda, \cdots, f^{p+p-1}(x) > \lambda$ and

$$f^{2p}(x) = f^p(\lambda \cdot \frac{1}{\lambda} f^p(x)) = \lambda f(\frac{1}{\lambda} f^p(x)) \le \lambda,$$

i.e., $f^{p+i}(x) > \lambda \ge f^{2p}(x), 0 \le x \le \lambda, i = 1, 2, \cdots, p - 1$. Inductively, we have $f^{kp+i}(x) > \lambda \ge f^{kp}(x), 0 \le x \le \lambda, i = 1, 2, \cdots, p - 1, k = 0, 1, 2, \cdots$.

Note 1 Property 2 is a generalization of Lemma 4 in [9].

Property 3   If $f(\lambda) < f(\lambda a)$, then

(1) $f(\lambda) < f(\lambda a) < \cdots < f(\lambda^n a) < \cdots$;

(2) $f(\lambda) < f(\lambda^2) < \cdots < f(\lambda^{n-1}) < f(\lambda^n) < \cdots$;

(3) $f(\lambda) < f(\lambda a) < f(\lambda a^2) < f(\lambda^2 a)$;

(4) $f(\lambda^n a) > f(\lambda a^n), f(\lambda a^n) > f(\lambda a^{n-1}), n = 1, 2, \cdots$.

Proof   By Lemma 6 in [9], we have f is f is strictly decreasing on. Since $0 < \lambda < a < 1$,

$$\lambda^n < \lambda^{n-1}, \ \lambda^{n-1} a > \lambda^n a, \lambda a^{n-1} > \lambda a^n, \lambda^n a < \lambda a^n, n = 1, 2, \cdots, \ \lambda a^2 > \lambda^2 a.$$

434   H. Wu and R. Li

Corollary 1 If $f(\lambda) < f(\lambda a)$, then

(1) $\lim_{n \to \infty} f(\lambda^n a) = 1$;

(2) $\lim_{n \to \infty} f(\lambda^n) = 1$;

(3) $\lim_{n \to \infty} f(\lambda a^n) = 1$.

Proof   It is easy to prove by Property 3 and Lemma 1.

Property 4 If $f(\lambda) > f(\lambda a)$, then

$$f(\lambda^n a) < f(\lambda^n), f(\lambda^n a) < f(\lambda^{n+1}), n \in Z_+.$$

Proof It is easy to check.

Property 5 If $f(\lambda) > a_0$, then $f(\lambda^{k+1} a) > f(\lambda^k a), k = 1, 2, \cdots$, and

$$\lim_{k \to \infty} f(\lambda^{k+1} a) = f(0) = 1.$$

Proof   By the proof of the theorems in [9], we have $\left\{ f(\lambda^k a) \right\}_{k=1}^{\infty}$ is strictly ascending on $[a_0, 1]$. By Lemma 1, $\lim_{k \to \infty} f(\lambda^{k+1} a)$ exists. So $\lim_{k \to \infty} f(\lambda^{k+1} a) = f(0) = 1$.

Property 6 $f^{p^n}(1) \to 1, (n \to \infty)$. Therefore 1 is the return point but not period point.

Proof Since $\lim_{n \to \infty} f^{p^n}(0) = \lim_{n \to \infty} \lambda^n = 0$, $\lim_{n \to \infty} f^{p^n-1}(1) = 0$.

So $f(\lim_{n \to \infty} f^{p^n-1}(1)) = \lim_{n \to \infty} f^{p^n}(1) = f(0) = 1$.

Property 7 $0 < f(1) < 1$.

Proof If $f(1) = 1$, then $f^{p-1}(1) = 1$. By Lemma 8 in [9], we have $f^{p-1}(1) = \lambda$. So $\lambda = 1$, contradiction. Since f is strictly ascending on $[a,1]$, $f(1) > f(a) = 0$.

Property 8 $f(\lambda^n) < 1, n = 1, 2, \cdots$.

Proof ① Firstly, we prove $f(\lambda) < 1$. If $f(\lambda) = 1$, then $f(\lambda) = f(0)$. So $f^{p^n}(\lambda) = f^{p^n}(0)$. Since

$f^{p^n}(0) \to 0, (n \to \infty)$, but $f^{p^n}(\lambda) \to \lambda, (n \to \infty)$. So $\lambda = 0$, contradiction.

② If $f(\lambda^n) < 1$, then $f(\lambda^{n+1}) < 1$. If $f(\lambda^{n+1}) = 1$, then $f^p(\lambda^{n+1}) = \lambda$. So $\lambda f(\lambda^n) = \lambda$ and $f(\lambda^n) = 1$, contradiction.

Property 9 $0 < f(\lambda^n a) < 1, n = 1, 2, \cdots$.

Proof By Lemma 2.5 in [12], we have a is the unique minimum point of f . So $0 < f(\lambda^n a), n = 1, 2, \cdots$. By Lemma 2 [9], we have $f(\lambda a) < 1$. Let $f(\lambda^n a) < 1$. Now, we prove $f(\lambda^{n+1}a) < 1$. If $f(\lambda^{n+1}a) = 1$, then $f^p(\lambda^{n+1}a) = \lambda$, i.e., $\lambda f(\lambda^n) = \lambda$. So $f(\lambda^n a) = 1$, contradiction.

Property 10 If $f(\lambda) > f(\lambda a)$, then $x = 0$ is the unique maximum point of f on $[0,1]$.

Proof By Property 8 and Property 9, we have $f(\lambda^n) < 1$, $0 < f(\lambda^n a) < 1, n = 1, 2, \cdots$. By Lemma 7 of [9], f is strictly ascending on $[\lambda^n a, \lambda^n]$, and strictly decreasing on $[\lambda^{n+1}, \lambda^n a]$. So f has no maximum value on $[\lambda^n a, \lambda^n]$ and $[\lambda^{n+1}, \lambda^n a]$. Since f is strictly decreasing on $[\lambda, a]$, $f(x) \le f(\lambda) < 1, x \in [\lambda, a]$. Because f is strictly ascending on $[\lambda, a]$, $f(x) \le f(\lambda) < 1, x \in [\lambda, a]$. Since f is strictly decreasing on $[a,1]$, $f(x) \le f(1) < 1, x \in [a,1]$. Therefore , $x = 0$ is the unique maximum point of f on $[0,1]$.

Property 11 If $f(\lambda) < f(\lambda a)$, then f has a unique maximum point $x = 0$ on $[0,1]$.

Proof Since f is strictly decreasing on $[0, a]$, $f(x) < f(0) = 1, x \in (0, a]$. Because f is strictly ascending on $[a,1]$, $f(x) < f(1) < 1, x \in [a,1)$. So f has a unique maximum point $x = 0$ on $[0,1]$.

Property 12 $f(1) \ne f(\lambda)$ and the maximum value of f on $[\lambda,1]$ is $\max\{f(\lambda), f(1)\}$.

Proof ① If $f(1) = f(\lambda)$, then $f^{p^n}(1) = f^{p^n}(\lambda)$. Since $n \to \infty$, $f^{p^n}(1) \to 1$, $\lambda) \to \lambda$. So $\lambda = 1$, contradiction. ② By the definition of f, we know the maximum value of f on $[\lambda,1]$ is $\max\{f(\lambda), f(1)\}$.

Property 13 If f is the continuous single-valley solution of p order ($p \geq 2$) Feigenbaum functional Equation (1.3), then f has a unique fixed point β and $\lambda < \beta < a$.

Proof   Since $f(0) = 1 > 0, f(1) < 1$ and   by   zero   theorem,   equation $f(x) - x = 0$ has least one zero on $(0,1)$, i.e., the fixed point of f. If f has fixed point on $[a,1]$ and since $f(a) = 0 < a, f(1) < 1$, then f has fixed point q on $(a,1)$.   So $q = f(q) < f(1) < 1$,   inductively,   we   have $q = f^{p^{n}-1}(q) < f^{p^{n}-1}(1) = f^{p^{n}}(0) \to 0$, i.e., $q \leq 0$, contradiction to $q > a$. Therefore, f has just fixed point on $[0,a]$. Since f is strictly decreasing on $[0,a]$, we have f has just one fixed point $\beta(0 < \beta < a)$ on $[0,a]$. Let $\beta \in [\lambda^{n} a, \lambda^{n}], n \geq 1$, then $f(\frac{\beta}{\lambda}) = \frac{1}{\lambda}, f^{p}(\beta) = \frac{\beta}{\lambda}$, i.e., $\frac{\beta}{\lambda}$ is also the fixed point of f. But $\beta \neq \frac{\beta}{\lambda}$, contradiction to the uniqueness of the fixed point of f. Let $\beta \in [\lambda^{n+1}, \lambda^{n} a], n \geq 1$, then $\frac{\beta}{\lambda^{n-1}} \in [\lambda^{2}, \lambda a]$ is also fixed point of f. But $\beta \neq \frac{\beta}{\lambda^{n-1}}$, contradiction to the uniqueness of the fixed point of f. So β is unique and $\lambda < \beta < a$.

Corollary 2 If f is the continuous single-valley solution of p order ($p \geq 2$) Feigenbaum functional Equation (1. 3),   then f has unique fixed point β with $\lambda < \beta < a$.

Proof By Property 13 and Lemma 2.3 of [12].

Property 14 The equation system consisting of p order and q order ($p, q \geq 2$ and $p \neq q$) Feigenbaum functional equations :

$$\begin{cases} f(x) = \frac{1}{\lambda} f^{p}(\lambda x), f(0) = 1, (\lambda \in (0,1) \text{for decision}) 0 \leq f(x) \leq 1, x \in [0,1]; \\ f(x) = \frac{1}{\lambda} f^{q}(\lambda x), f(0) = 1, (\lambda \in (0,1) \text{for decision}) 0 \leq f(x) \leq 1, x \in [0,1]. \end{cases}$$
$$(*)$$

has no continuous single-valley expansion solution.

Proof If the equation system $(*)$ has continuous single-valley expansion solution and   assume   it   as f ,   then $f^{p}(\lambda) = \lambda f(1), f^{q}(\lambda) = \lambda f(1)$.   So $f^{p}(\lambda) = f^{q}(\lambda)$. Without loss generality, we assume that $p > q$. Then $f^{p-q}(f^{q}(1)) = f^{q}(1)$. By $f^{p}(1) = f(\lambda), f^{q}(1)   = f(\lambda)$, we have $f^{p}(1) = f^{q}(1)$. So $f^{p-q}(f^{q}(1)) = f^{q}(1)$. By Theorem 2 and 4 of [9],

$f^q(\lambda) = \beta, f^q(1) = \beta$.   Therefore $f^{q^n}(\lambda) = f^{q^n}(1)$.   Since

$f^{q^n}(\lambda) \to \lambda, f^{q^n}(1) \to 1, (n \to \infty)$, we have $\lambda = 1$, contradiction.

Property 15 If f is the continuous single-valley solution of p order ($p \geq 2$) Feigenbaum functional Equation (1. 3), a is the minimal value point of f on $[\lambda, 1]$ and $f(a) = 0$, then a is the unique minimal value point of f on $[0,1]$.

Proof (1) If f is single-valley, then the result is clear.

(2) If f is not single-valley, then by Lemma 7 of [9], we have f is strictly ascending on $[\lambda^n a, \lambda^n]$, and strictly decreasing on $[\lambda^{n+1}, \lambda^n a]$ ($n \geq 1$). By Lemma 2 of [9], we have

$$f(\lambda^n a) > f(\lambda a), n \geq 2,$$

$$f(\lambda a) > \qquad 0. \qquad \text{So}$$

$f(x) > 0, x \in [\lambda^n a, \lambda^n]; f(x) > 0, x \in [\lambda^{n+1}, \quad \lambda^n a]$.   Therefore, $f(x) > 0, x \in [0, \lambda]$. Since f is strictly decreasing on $[\lambda, a]$ and strictly ascending on $[a,1]$, f has unique value $f(a) = 0$ on $x = a$.

Property 16 Let $p > 2, i = 1, 2, \cdots, p-1. f^i(x) = \lambda a$ has no solution on $[\lambda, a]$, but $f(x) = \lambda a$ has unique solution on $[\lambda, a]$.

Proof By lemma 4 of [9], we have $f^i(x) > \lambda, i = 1, 2, \cdots, p-1, x \in [0, \lambda]$. Since $\lambda a < \lambda < a$, we have $f^i(x) = \lambda a$ has no solution on $[\lambda, a]$, $i = 1, 2, \cdots, p-1$. By Lemma 4 of [9], $f(\lambda) > \lambda$ and $f(a) = 0$. So $[0, \lambda] \subset f([\lambda, a])$. Because $0 < \lambda a < \lambda$, there exists $\bar{x} \in [\lambda, a]$ such that $f(\bar{x}) = \lambda a$. Since f strictly decreasing on $[\lambda, a]$, the point $\bar{x}$ such that $f(x) = \lambda a$ hold is unique.

Property 17 $f^{p^n}(a) \to a, (n \to \infty)$.

Proof By $\lambda^n \to 0, (n \to \infty)$ and f is strictly decreasing on $[a,1]$, then ① if f is single-valley, then f is strictly decreasing on $[0, a]$. Since $f^{p^n}(0) = \lambda^n$, but $f^{-1}(\lambda^n)$ has at most two point trend to a fixed point as n increase, i.e.,

$$\lim_{n \to \infty} f^{p^n}(a) = \lim_{n \to \infty} f^{-1}(f^{p^n}(0)) = \lim_{n \to \infty} f^{-1}(\lambda^n) \quad \text{exists.}$$

Since $\lim\limits_{n\to\infty} f^{p^n+1}(a) = \lim\limits_{n\to\infty} f(f^{p^n}(a)) = \lim\limits_{n\to\infty} \lambda^n = 0$ and by Property 15, we

have $\lim\limits_{n\to\infty} f^{p^n}(a) = a$. ② If f is not single-valley, then $\lambda^n (n \geq 1)$ is the

extreme value point of f, i.e, for any fully small neighborhood of λ^n, $f^{-1}(\lambda^n)$

is unique, that is $\lim\limits_{n\to\infty} f^{p^n}(a)$ exists. By the same method of ①, we have

$\lim\limits_{n\to\infty} f^{p^n}(a) = a$.

Property 18 $f^{p^n}(\lambda a) \to \lambda a, (n \to \infty)$.

Proof Since $f^p(\lambda a) = \lambda f(a) = 0$ and $f^p(\lambda x) = \lambda f(x)$, by Property 15,

f^p has unique minimum value point $x = \lambda a$ on $[0, \lambda]$. For $\lambda^n \to 0, (n \to \infty)$

and f^p strictly ascending on $[\lambda a, \lambda]$. ①if f is single-valley, then f^p is

strictly decreasing on $[0, \lambda a]$. Because $f^{p^n}(0) = \lambda^n$, we have that $f^{-p}(\lambda^n)$

has at most two point trend to a fixed point as n increase, i.e.,

$\lim\limits_{n\to\infty} f^{p^n}(\lambda a) = \lim\limits_{n\to\infty} f^{-p}(f^{p^n}(0)) = \lim\limits_{n\to\infty} f^{-p}(\lambda^n)$ exists. Since

$\lim\limits_{n\to\infty} f^{p^n+p}(\lambda a) = \lim\limits_{n\to\infty} f^p(f^{p^n}(\lambda a)) = 0$, then $\lim\limits_{n\to\infty} f^{p^n}(\lambda a) = \lambda a$. ② If f

is not single-valley, then $\lambda^n (n \geq 1)$ is the extreme value point of f. It follows that

$\lambda^n (n \geq 1)$ is the extreme value point of f^p, that is for any fully small

neighborhood of λ^n, $f^{-p}(\lambda^n)$ is unique, i.e., $\lim\limits_{n\to\infty} f^{p^n}(\lambda a)$ exists. Similarly,

$\lim\limits_{n\to\infty} f^{p^n}(\lambda a) = \lim\limits_{n\to\infty} f^{-p}(f^{p^n+p}(\lambda a)) = \lim\limits_{n\to\infty} f^{-p}(f^{p^n}(0)) = f^{-p}(0) = \lambda a$

Lemma 5 [9] Let f_0 be the continuous map on $[\lambda, 1]$, $0 < \lambda < 1$. If f_0
satisfies

① There exists $a \in (\lambda, 1)$ such that $f_0(a) = 0$ and $f_0\big|_{[\lambda,a]}$ is strictly

decreasing, $f_0\big|_{[\lambda,a]}$ is strictly ascending;

② $f_0^{p-1}(1) = \lambda, f_0^p(\lambda) = \lambda f_0(1)$;

③ Set $[A, 1] = J_0 \subset [\lambda,1]$, where $A = \min\{f_0(\lambda), a_0\}$, a_0 satisfying

$f_0^{p-1}(a_0) = 0$ and $J_0, J_1, \cdots, J_{p-2} \subset (\lambda,1]$ point wise disjoint,

$J_i = f_0^i(J_0)$ (ii) $f^i\big|_{J_0} : J_0 \to J_i$ is homomorphism, $i = 0,1,\cdots, p-2$;

④ Equation $f^{p-1}(x)=\lambda x$ has one solution $x=1$ on $(a_0,1)$. Then Equation (1.3) exists unique continuous single-valley expansion solutions f with $f|_{[\lambda,1]}=f_0$. For details, if $f_0(\lambda)<a_0$, f is single-valley; if $f_0(\lambda)>a_0$, f has infinite extreme value point. Conversely, if f_0 is some continuous single-valley expansion solutions Equation (1.3) restrict on $[\lambda,1]$, then f_0 must satisfies ①、②、③ and ④.

Property 19 Let $\lambda_i \in (0,1), i=1,2,\cdots$, and $\lim\limits_{i\to\infty}\lambda_i = \lambda \in (0,1)$. Then

① if for any $\lambda_i (i=1,2,\cdots)$ and the sequence $\{f_i\}$ consisting of the unique continuous single-valley solutions satisfying the conditions of Lemma 5 is uniform convergent to $f \in C^0(I,I)$, then f is the unique continuous single-valley solution of Equation (1.3) corresponding to λ.

② for any $\lambda_i (i=1,2,\cdots)$ and the sequence $\{f_i\}$ consisting of the unique continuous non-single-valley expansion solutions satisfying the conditions of Lemma 5 is uniform convergent to $f \in C^0(I,I)$, then f is the unique continuous non-single-valley expansion solution of Equation (1.3) corresponding to λ.

Proof For any fixed point $x \in I$, $f_i(x)=\frac{1}{\lambda_i}f_i^{\,p}(\lambda_i x)$ and $f_i(0)=1, i=1,2,\cdots$ $f_i \in C^0(I,I), i=1,2,\cdots$, since $\{f_i\}$ is uniform convergent to f, by Lemma 4, we have $f_i(x) \to f$ $(x)(i \to \infty)$, $f(x)=\lim\limits_{i\to\infty}f_i(x)=\lim\limits_{i\to\infty}\frac{1}{\lambda_i}\cdot f_i^{\,p}(\lambda_i x)$.

Therefore $\lim\limits_{i\to\infty}\frac{1}{\lambda_i}f_i^{\,p}(\lambda_i x)=\lim\limits_{i\to\infty}\frac{1}{\lambda_i}\cdot\lim\limits_{i\to\infty}f_i^{\,p}(\lambda_i x)=\frac{1}{\lambda}\cdot f^{\,p}(\lambda x)$. So $f(x)=\frac{1}{\lambda}\cdot f^{\,p}(\lambda x)$. Clearly, $f(0)=1$ (since $f_i(0)=1, i=1,2,\cdots$). By the proof of theorems in [9], we can have two cases.

① If $f_i(\lambda_i)<a_{0,\lambda_i}$, where a_{0,λ_i} with $f_i^{\,p-1}(a_{0,\lambda_i})=0$. Without loss of generality, we can assume that $a_{0,\lambda_i} \to a_0 (i \to \infty)$, $f(\lambda) \leq a_0$ and $f^{p-1}(a_0)=0$. If $f(\lambda)=a_0$, by Lemma 5, we have $f^{p-1}(a_0)=\lambda f(1)=0$. Since $f(1)>0$, $\lambda=0$, contradiction to $\lambda>0$. So $f(\lambda)<a_0$.]

② If $f_i(\lambda_i)>a_{0,\lambda_i}$, where a_{0,λ_i} with $f_i^{\,p-1}(a_{0,\lambda_i})=0$. Without loss of generality, we can assume that $a_{0,\lambda_i} \to a_0 (i \to \infty)$, $f(\lambda) \geq a_0$, and

$f^{p-1}(a_0)=0$. If $f(\lambda)=a_0$. By Lemma 5, we have $f^{p-1}(a_0)=\lambda f(1)=0$.
Since $f(1)>0$, $\lambda=0$, contradiction to $\lambda>0$. So $f(\lambda)>a_0$.

By ①, ② and the condition of Lemma 5, it is easy to prove the result.

Corollary 3 Let $p\geq 2$ be an integer . For any $\lambda\in(0,1)$, denote the set of unique single-valley solutions of $(**)$ satisfying the conditions of Lemma 5 by $C_{p,1}^0(I,I)$ and the set of continuous expansion solutions of the unique non single-valley of $(**)$ satisfying the conditions of Lemma 5 by $C_{p,2}^0(I,I)$. Then $C_{p,1}^0(I,I),C_{p,2}^0(I,I)$ are complete metric space.

$$(**)\qquad \begin{cases} f(x)=\frac{1}{\lambda}f^p(\lambda x),\lambda\in(0,1)\text{for decision} \\ f(0)=1, f\in C^0([0,1],[0,1]) \end{cases}$$

References

[1] Feigenbaum, M.J.: Quantiative universality for a class of nonlinear transformation. Stat. Phys. 19(1), 25–52 (1978)
[2] Feigenbaum, M.J.: The universal metric properties of nonlinear transformations. Stat. Phys. 21(4), 669–706 (1979)
[3] Campanino, M., Epstein, H.: On the existence of Feigenbaum's fixed point. Comm. Math. Phys. 79(2), 261–302 (1981)
[4] Collet, P., Eekmann, J.P., Lanford, O.E.: Universal properties of maps on an interval. Comm. Math. Phys. 76(2), 211–254 (1980)
[5] Yang, L., Zhang, J.: The Second type of Feigenbaum's functional equations. Scientia Sinica (Series A) 29(4), 1252–1263 (1986)
[6] Liao, G.: Solutions on the second type of Feigenbaum's functional equations. Chin Ann. Math (Series A) 9(6), 649–654 (1988)
[7] Liao, G.: On the Feigenbaum's functional equation $f^p(\lambda x)=\lambda f(x)$. Chin Ann. Math. 15B(1), 81–88 (1994)
[8] Liao, G.: A characterization of the solutions of $p-$ order Feigenbaum's functional equation with topological entropy 0. Acta Math.Sci. 16(1), 38–43 (1996)
[9] Zhang, A., Wang, L.: The Continuous Single-Valley Expansion Solutions Of The Feigenbaum'S Funcational Equation. J. of Math. 26(1), 89–93 (2006)
[10] Wang, L., Liao, G.: Topological Conjugacy on 3-order Feigenbaum's Maps. Acta Mathematica Sinica Chinese Series 49(4), 955–960 (2006)
[11] Liao, G., Wang, L., Yang, L.: Kneading Sequences and Characteristic Sets of Feigenbaum's Maps. Acta Mathematica Sinica Chinese Series 49(2), 399–404 (2006)
[12] Wang, L.: The Research F -Map. Jilin University, Jilin (2004)
[13] Xiong, J.C.: Point Topology, 2nd edn. Advanced Education Press, Beijing (1997)

Pythagorean Element on UFD and PH Curve

Huahao Shou[1], Yu Jiang[1], Congwei Song[1], and Yongwei Miao[2]

[1] College of Science, Zhejiang University of Technology, Hangzhou, China
[2] College of Computer Science and Technology, Zhejiang University of Technology
Hangzhou, China
{shh,ywmiao}@zjut.edu.cn

Abstract. Necessary and sufficient conditions are given for Pythagorean elements on unique factorization domains. Sets of easy to use polynomial coefficient based Pythagorean discriminant equations are derived for degree 2 polynomials on polynomial rings. Finally, obtained results are applied to degree 3 Pythagorean Hodograph curves in geometric modeling.

Keywords: Pythagorean equation, unique factorization domain, Pythagorean hodograph curve.

1   Introduction

The most famous indefinite equation in number theory is Pythagorean equation (Shanggao equation) [1-3]: $a^2 + b^2 = c^2, a, b, c \in Z$. The famous Fermat theorem is also originated from this equation. Although it is an old formula of number theory, it is still playing an important role in all kinds of scientific fields till now. In geometric modeling, the Pythagorean Hodograph curves (PH curves) [4,5] are defined based on Pythagorean equation on polynomial rings.

   We call the ordered array (a, b, c) Pythagorean triple (Gougu number). In general ring, the Pythagorean triple is called Pythagorean element. Because c can be determined by a and b, we also call the ordered pair (a, b) Pythagorean element. Obviously, $(a, 0)$, $(0, b)$ are Pythagorean elements. They are trivial. In this paper, we suppose that all of the rings considered include an identity element. The set which composed by all irreducible elements is denoted by $\mathrm{Irr}(R)$, and the set composed by all the units (invertible elements) is denoted by $U(R)$. One of the important properties of the unique factorization domain (UFD) is that it has greatest common divisors [2,3]. In this paper, $w \sim (a, b)$ means w is one of the greatest common divisors of a, b, and $(a, b) \sim 1$ means a, b are coprime.

2   Pythagorean Equation on Rings

In this Section we derive the necessary and sufficient conditions of the Pythagorean equation on general rings (esp. UFD).

2.1   Even Ring and Even Element

Definition 2.1.1.   Given a ring R, $a \in R$, if there is a unique $b \in R$, $a = b + b = 2b$, then a is called even element, and the b is written as $a/2$. If all elements in R are even elements, we call R even ring.

   The following theorems about the even element and the even ring is easy to prove.

Theorem 2.1.1.   Let R be an integral domain, its character $\mathrm{ch}(R) > 2$,

a is even element $\Leftrightarrow 2 \mid a$.   (1)

   If (1) holds true for all $a \in R$, we have the following theorem.

Theorem 2.1.2.   Let R be an integral domain, and then R is even element $\Leftrightarrow 2 \in U(R)$.

Remark 2.1.1. $2 \in R$ in the theorem means double identity.

Theorem 2.1.3.   A polynomial on a ring is even element if and only if its coefficients are all even elements.

Theorem 2.1.4. R is an even ring $\Rightarrow R[x]$ is also an even ring. If the character of a division ring is larger than 2, then it is an even ring.

2.2   Pythagorean Equation on UFD

Lemma 2.2.1.   Let R be a UFD, $a, b, c \in R$, a, b are coprime, then

$$c^2 \sim ab \Leftrightarrow \exists u, v \in R, a \sim u^2, b \sim v^2, c \sim vu,$$ (2)

where u, v are coprime.

Proof: "$\Leftarrow$"is obvious. So we only need to check"$\Rightarrow$". It is trivial when $c = 0$. So we suppose that $c \neq 0$. With the definition of UFD, it is easy to prove that $p^n \mid ab \Leftrightarrow p^n \mid a$ or $p^n \mid b$, if a, b are coprime where p is a prime. There is a factorization $c = p_1^{n_1} p_2^{n_2} \dots p_t^{n_t}$. $p_i^{2n_i} \mid ab \Rightarrow p_i^{2n_i} \mid a$ or $p_i^{2n_i} \mid b$. So let $p_{i_1}^{2n_{i_1}}, \dots, p_{i_r}^{2n_{i_r}} \mid a$, $p_{i_{r+1}}^{2n_{i_{r+1}}}, \dots, p_{i_t}^{2n_{i_t}} \mid b$. Note that $ab \mid c$, then $p_{i_1}^{2n_{i_1}} \dots p_{i_r}^{2n_{i_r}} \sim a$, $p_{i_{r+1}}^{2n_{i_{r+1}}} \dots p_{i_t}^{2n_{i_t}} \sim b$. Let $u = p_{i_1}^{n_{i_1}} \dots p_{i_r}^{n_{i_r}}$ $v = p_{i_{r+1}}^{n_{i_{r+1}}} \dots p_{i_t}^{n_{i_t}}$, then $a \sim u^2, b \sim v^2$, while $c \sim vu$. u, v are obviously coprime.

Lemma 2.2.2.   Let R be a UFD, $a, b, c \in R$, then

$$c^2 = ab \Leftrightarrow \exists u, v, w \in R, a = wu^2, b = wv^2, c = wuv,$$ (3)

where u, v are coprime, $w \sim (a, b)$.

Proof: We only need to prove"$\Rightarrow$". Let $d \sim (a,b)$. $a_1 = d^{-1}a$, $b_1 = d^{-1}b$ are coprime and $c_1^2 = a_1 b_1$, $c_1 = d^{-1}c$. According to lemma2.2.1, $\exists u,v \in R$ are coprime, $a_1 = \varepsilon u^2$, $b_1 = \varepsilon v^2$, $c_1 = \varepsilon uv$, i.e. $a = \varepsilon du^2, b = \varepsilon dv^2, c = \varepsilon duv$. Let $w = \varepsilon d$, then $w \sim d \sim (a,b)$.

Theorem 2.2.1. Let R be a UFD, $a,b,c \in R$, and $a+c,b$ are even elements, then $a^2 + b^2 = c^2 \Leftrightarrow \exists u,v,w \in R$, $a = w(u^2 - v^2)$, $b = 2wuv$, $c = w(u^2 + v^2)$, (4) where u,v are coprime, $w \mid (a,b)$. If a is not an even element, then $w \sim (a,b)$.

Proof: We only need to prove "$\Rightarrow$". $b^2 = c^2 - a^2 = (c+a)(c-a)$. Since $c+a, c-a, b$ are all even elements, so $(b/2)^2 = ((c+a)/2)((c-a)/2)$. According to Lemma 2.2.2, $(c+a)/2 = wu^2, (c-a)/2 = wv^2, b/2 = wuv$, i.e. $a = w(u^2 - v^2)$, $b = 2wuv$, $c = w(u^2 + v^2)$, u,v are coprime, $w \sim ((c-a)/2,(c+a)/2)$, while $((c-a)/2,(c+a)/2) \mid (a,c) = (a,b)$. If a is not   an   even   element, then $d \mid (a,c) = (a,b) \Rightarrow 2d \mid (c-a,c+a) \Rightarrow d \mid ((c-a)/2,(c+a)/2)$. As a result, $(a,b) \sim ((c-a)/2,(c+a)/2) \sim w$.

Corollary 2.2.1. Let R be a UFD, $(a,b,c) \in R$, a,b are coprime, and $a+c,b$ are even element, then $a^2 + b^2 = c^2 \Leftrightarrow \exists u,v \in R, \varepsilon \in U(R), a = \varepsilon(u^2 - v^2), b = 2\varepsilon uv, c = \varepsilon(u^2 + v^2)$ (5) where u,v are coprime.

The following corollary avoids the hypothesis about even element.

Corollary 2.2.2. Let R be a UFD, and $\mathrm{ch}(R) > 2$, $(a,b,c) \in R$, then
$$a^2 + b^2 = c^2 \Leftrightarrow \exists u,v \in R, w \in F(R), \quad a = w(u^2 - v^2), \quad b = 2wuv, \quad c = w(u^2 + v^2) \quad (6)$$
where u,v are coprime, $2w \mid 2(a,b)$.

Proof: We only need to prove"$\Rightarrow$". Obviously, $(2a,2b,2c)$ also forms a Pythagorean triple. Since $2c + 2a, 2c - 2a, 2b$ are all even element. According to Theorem 2.2.2, we have $2a = w_1(u^2 - v^2)$, $2b = 2w_1 uv$, $2c = w_1(u^2 + v^2)$, where u,v are coprime. Let $w = w_1 / 2 \in F(R)$, we get the result.

2.3   Pythagorean Element on UFD

Usually we do not take care of c, but prefer to study the relationship of Pythagorean elements a,b.

Theorem 2.3.1. Let R be a UFD, $2 \in Irr(R)$, then $(a,b) \in P(R)$, where b is an even element, a is not an even element. $\Leftrightarrow \exists u, v, w \in R, a = w(u^2 - v^2)$, $b = 2wuv$ (7) where u, v are coprime, $w \sim (a,b)$ and is not an even element.

Proof: $b^2 = c^2 - a^2 = (c+a)(c-a)$, b is an even element, then $2 \mid (c+a)(c-a)$. At least one of $a+c$ and $a-c$ is an even element. Therefore both of them are even elements. According to Theorem 2.2.2, the theorem is proved.

Theorem 2.3.1 avoids the hypothesis of c, while the following theorem derived from the Corollary 2.2.2 is more useful.

Theorem 2.3.2. Let R be a UFD, $ch(R) > 2$, then
$$(a,b) \in P(R) \Leftrightarrow \exists u, v \in R, w \in F(R), \quad a = w(u^2 - v^2), \qquad b = 2wuv \qquad (8)$$
where u, v are coprime, $2w \mid 2(a,b)$.

3   Pythagorean Polynomial

In this section, the results obtained above are applied to polynomials and PH curves in geometric modeling.

3.1   Polynomial

A trivial case is that one of the Pythagorean polynomials is constant.

Theorem 3.1.1. Let R be an integral ring, $f(x) \in R[x], \partial f(x) \geq 1, a \neq 0 \in R$, then $f(x)^2 + a$ can not be the square of a polynomial.

Proof: Assume that there is a polynomial $g(x)$, such that $g(x)^2 = f(x)^2 + a$, i.e. $(g(x) - f(x))(g(x) + f(x)) = a$. Then, $g(x) - f(x), g(x) + f(x) \in R \Leftrightarrow f(x), g(x) \in R$. It is contradictory.

Corollary 3.1.1. Let R be a UFD, $f(x), g(x) \in P(R[x])$, $\partial f(x) < \partial g(x)$, then $f(x)$ $not \mid g(x)$. Actually, $\forall a, b \neq 0 \in R$, $af(x)$ $not \mid bg(x)$.

With Corollary 2.2.1, the following theorem is obtained.

Theorem 3.1.2. Let R be a UFD, $f(x), g(x) \in R[x]$ are coprime, $f(x) + h(x), g(x)$ are even elements, then $f(x)^2 + g(x)^2 = h(x)^2 \Leftrightarrow \exists u(x), v(x) \in R[x], \varepsilon \in U(R)$, such that $f(x) = \varepsilon(u(x)^2 + v(x)^2), g(x) = 2\varepsilon u(x)v(x)$, $h(x) = \varepsilon(u(x)^2 - v(x)^2)$, where $u(x), v(x)$ are coprime.

Usually it is unnecessary that $\varepsilon \in R$. So, the following theorem is more useful, and it can be derived from Corollary 2.2.2.

Theorem 3.1.3.   Let R be a UFD, $ch(R) > 2$ the common divisions of $f(x), g(x) \in R[x]$ are   all   in R,   then $f(x)^2 + g(x)^2 = h(x)^2 \Leftrightarrow \exists u(x),$ $v(x) \in R[x]$, $w \in F(R)$, such that $f(x) = w(u(x)^2 + v(x)^2)$, $g(x) = 2wu(x)v(x)$, $h(x) = w(u(x)^2 - v(x)^2)$, where $u(x), v(x)$ are coprime.

Now, we take linear polynomial as a simple example.

Theorem 3.1.4. Let R be an integral ring, $ch(R) > 2$, $(f(x), g(x)) \in P(R[x])$, and $\partial f(x) = \partial g(x) = 1$, Then $\exists a, b \neq 0, af(x) + bg(x) = 0$. Especially, when R is a field, $f(x) \sim g(x)$.

Proof: Let $f(x) = a_0 + a_1 x$, $g(x) = b_0 + b_1 x$, $a_1, b_1 \neq 0$ and $h(x) = c_0 + c_1 x$, such that $f(x)^2 + g(x)^2 = h(x)^2$. $f(x)^2 + g(x)^2 = (a_1^2 + b_1^2)x^2 + 2(a_0 a_1 + b_0 b_1)x + a_0^2 + b_0^2 = c_1^2 x^2 + 2c_0 c_1 x + c_0^2 \Rightarrow (a_0 a_1 + b_0 b_1)^2 = c_0^2 c_1^2 = (a_1^2 + b_1^2)(a_0^2 + b_0^2) \Rightarrow a_0 b_1 = a_1 b_0$. It implies that $b_1 f(x) - a_1 g(x) = 0$.

Theorem 3.1.5. Let R be a UFD, $ch(R) > 2$. Let $f(x) = a_0 + a_1 x + a_2 x^2$, $g(x) = b_0 + b_1 x + b_2 x^2$, $h(x) = c_0 + c_1 x + c_2 x^2$. If all common divisors of $f(x), g(x)$ are in R, then $f(x)^2 + g(x)^2 = h(x)^2$, if and only if $\exists u_0, u_1, v_0, v_1 \in R, w \in F(R)$, and

$$\begin{cases} a_0 = w(u_0^2 - v_0^2), a_1 = 2w(u_0 u_1 - v_0 v_1), a_2 = w(u_1^2 - v_1^2), \\ \quad b_0 = 2wu_0 v_0, b_1 = 2w(u_1 v_0 + u_0 v_1), b_2 = 2wu_1 v_1, \\ c_0 = w(u_0^2 + v_0^2), c_1 = 2w(u_0 u_1 + v_0 v_1), c_2 = w(u_1^2 + v_1^2). \end{cases} \quad (9)$$

Now, we have an equation set:

$$\begin{cases} a_1^2 - b_1^2 = 4(a_0 a_2 - b_0 b_2), \\ \quad a_1 b_1 = 2(a_0 b_2 - a_2 b_0). \end{cases} \quad (10)$$

Proof: According to Theorem 3.1.3, $\exists u(x) = u_0 + u_1 x$, $v(x) = v_0 + v_1 x$, $w \in F(R)$, $f(x) = w(u(x)^2 - v(x)^2)$, $g(x) = 2wu(x)v(x)$, $h(x) = w(u(x)^2 + v(x)^2)$, We got (9) at once, and that implies (10).
Following theorem can help us to judge the Pythagorean polynomials only with their coefficients.

Theorem 3.1.6. Let R be a UFD, and $x^2 + 1$ has no solution on R. Let $f(x) = a_0 + a_1 x + a_2 x^2$, $g(x) = b_0 + b_1 x + b_2 x^2$, $(a_0, b_0), (a_2, b_2) \in P(R)$, their coefficients satisfy (10), then $(f(x), g(x)) \in P(R[x])$.

Proof: $x^2 + 1$ has no solution on R, so it is certainly that $ch(R) > 2$. According to Theorem 2.3.2, $(a_0, b_0), (a_2, b_2), \in P(R) \Rightarrow \exists u_0, u_1, v_0, v_1 \in R, w \in F(R)$,

$$\begin{cases} a_0 = w(u_0^2 - v_0^2), a_2 = w(u_1^2 - v_1^2), \\ \quad b_0 = 2wu_0 v_0, b_2 = 2wu_1 v_1. \end{cases}$$

a_1, b_1 can be obtained by (10). We have:

$$\begin{cases} a_1^2 - b_1^2 = X^2 - Y^2, \\ \quad a_1 b_1 = XY. \end{cases} \tag{11}$$

where X, Y are exactly the expressions of a_1, b_1 in (9).

Since $x^2 + 1$ has no solution on R, (a_1, b_1) can only has two possible solutions $(X, Y), (-X, -Y)$, in any case (9) can be satisfied. So $(f(x), g(x)) \in P(R[x])$.

Remark 3.1.1. If $x^2 + 1$ has a solution α on R, then $(Y\alpha, X\alpha)$ is also a solution. On the extension ring $R[\alpha]$, (11) is equivalent to $(a + b\alpha)^2 = (X + Y\alpha)^2$, while (10) is equivalent to $(a_1 + b_1\alpha)^2 = 4(a_0 + b_0\alpha)(a_2 + b_2\alpha)$.

Corollary 3.1.2. Let F be a field, and $x^2 + 1$ has no solution on F. Let $f(x) = a_0 + a_1 x + a_2 x^2$, $g(x) = b_0 + b_1 x + b_2 x^2$, $(a_0, b_0), (a_2, b_2) \in P(F)$. Their coefficients satisfy (10), then $(f(x), g(x)) \in P(F[x])$. If $f(x) \; not \sim g(x)$, then (10) is equivalent to $(f(x), g(x)) \in P(F[x])$.

Corollary 3.1.3. Let $\mathbb{R}$ be a real number field, and the polynomials $f(x) = a_0 + a_1 x + a_2 x^2$, $g(x) = b_0 + b_1 x + b_2 x^2$ are on $\mathbb{R}$, whose coefficients satisfy (10), then $(f(x), g(x)) \in P(\mathbb{R}[x])$. If $f(x) \; not \sim g(x)$, then (10) is equivalent to $(f(x), g(x)) \in P(\mathbb{R}[x])$.

Another useful formula $a_1^2 + b_1^2 = 4c_0 c_2$ can be derived from (9). That means c_0, c_2 have the same sign. It is well known that any quadratic polynomial has a discriminant $\Delta = a_1^2 - 4a_0 a_2$. So the following theorem holds.

Theorem 3.1.7. Let R be a UFD, $f(x), g(x), h(x) \in R[x]$ satisfy Pythagorean equation. If all common divisors of $f(x), g(x)$ are in R and $g(x), f(x) + h(x)$ are even elements, then $\Delta_h = (-1/2)(\Delta_f + \Delta_g)$.

3.2   The Application to PH Curves

Definition 3.2.1. A parametric polynomial curve $(f(x), g(x)) \in R[x]^2$ is called a PH curve, if $(f'(x), g'(x)) \in P(R[x])$. According to this definition, we have

Theorem 3.2.1. Let $(f(x), g(x)) = (a_0 + a_1 x + a_2 x^2 + a_3 x^3, b_0 + b_1 x + b_2 x^2 + b_3 x^3)$ is a degree 3 parametric polynomial curve on $\mathbb{R}^2$, if their coefficients satisfy

$$\begin{cases} a_2^2 - b_2^2 = 3(a_1 a_3 - b_1 b_3) \\ 2a_2 b_2 = 3(a_1 b_3 + a_3 b_1) \end{cases} \tag{12}$$

then $(f(x), g(x))$ is a PH curve.

A parametric polynomial curve might as well be considered on the complex plane, i.e. $a_0 + a_1 x + a_2 x^2 + a_3 x^3 \in \mathbb{C}[x]$. Then (12) takes a simpler expression $a_2^2 = 3a_1 a_3$.

In geometric modeling Bézier curve is expressed with the base of Bernstein polynomials. After transforming from power base $(1, x, x^2, x^3)$ to Bernstein base $((1-x)^3, 3x(1-x)^2, 3x^2(1-x), x^3)$ we get:

Theorem 3.2.2. If the coordinates of the control points of a degree 3 Bézier curve $(f(x), g(x)) = \sum_{i=0}^{3} (a_i, b_i) B_i^3(x)$ satisfy

$$\begin{cases} (a_2 - a_1)^2 - (b_2 - b_1)^2 = (a_1 - a_0)(a_3 - a_2) + (b_1 - b_0)(b_2 - b_3) \\ 2(b_2 - b_1)(a_2 - a_1) = (a_3 - a_2)(b_1 - b_0) + (a_1 - a_0)(b_2 - b_3) \end{cases} \tag{13}$$

Then the Bézier curve is PH curve.

Considered on complex plane, (13) can be written simply as $(a_2 - a_1)^2 = (a_1 - a_0)(a_3 - a_2)$.

Obviously this theorem has another form as follows.

Corollary 3.2.1. Except for the trivial case that $(f'(x), g'(x))$ is a line, $(f(x), g(x))$ is a PH curve if and only if $f_1(x) = \dfrac{a_1 - a_0}{2} + (a_2 - a_1)x + \dfrac{a_3 - a_2}{2}x^2$,
$g_1(x) = \dfrac{b_1 - b_0}{2} + (b_2 - b_1)x + \dfrac{b_3 - b_2}{2}x^2$ is a pair of Pythagorean polynomials.

The degree 3 C-Bézier curve is constructed with a mixed base of trigonometric functions and power functions [6]

$$(1, \frac{x+\sin x}{2}, \frac{1-\cos x}{2}, \frac{x-\sin x}{2}) \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1-c}{\alpha-s} & 0 & 0 \\ 0 & \frac{-2s}{\alpha-s} & \frac{-2s}{\alpha(1-c)-2s} & 0 \\ 0 & \frac{1+c}{\alpha-s} & \frac{2c+2}{\alpha(1+c)-2s} & \frac{2}{\alpha-s} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & -1 & 1 \end{bmatrix} \tag{14}$$

where $c = \cos\alpha, s = \sin\alpha, 0 < \alpha < \pi$.

The derivative of $(1, \frac{x+\sin x}{2}, \frac{1-\cos x}{2}, \frac{x-\sin x}{2})$ is $(0, \frac{1+\cos x}{2}, \frac{\sin x}{2}, \frac{1-\cos x}{2})$
$= \frac{1}{1+t^2}(0,1,t,t^2)$, where $t = \tan\frac{x}{2}$. Therefore, the coefficients of a degree 3 PH C-Bézier curve should satisfy the Pythagorean discriminant equation after the

transformation of the matrix in (14). In detail, the array

$$
\begin{bmatrix}
\dfrac{1-\cos\alpha}{\alpha-\sin\alpha} & 0 & 0 \\[2mm]
\dfrac{-2\sin\alpha}{\alpha-\sin\alpha} & \dfrac{-2\sin\alpha}{\alpha(1+\cos\alpha)-2\sin\alpha} & 0 \\[2mm]
\dfrac{1+\cos\alpha}{\alpha-\sin\alpha} & \dfrac{2\cos\alpha+2}{\alpha(1+\cos\alpha)-2\sin\alpha} & \dfrac{2}{\alpha-\sin\alpha}
\end{bmatrix}
\cdot
\begin{bmatrix}
a_1-a_0 & b_1-b_0 \\
a_2-a_1 & b_2-b_1 \\
a_3-a_2 & b_3-b_2
\end{bmatrix}
$$

satisfies (10).

4   Conclusions

Pythagorean equation in number theory is extended to general rings. Sets of easy to use polynomial coefficient based necessary and sufficient conditions are derived for Pythagorean polynomials on polynomial rings. The obtained results are applied to construct PH curves in geometric modeling. An old formula, a new application. However, this paper does not completely solve all problems about Pythagorean polynomials; for example, Pythagorean discriminant equation of the polynomials with arbitrary degree has not been got. Also multiple Pythagorean equation on ring and space PH curve need to be further studied.

References

1. Min, S., Yan, S.: Elementary Number Theory. Advanced Education Press, Peking (1982)
2. Zhang, H.: Foundations of Modern Algebra. Advanced Education Press, Peking (2006)
3. Rotman, J.J.: Advanced Modern Algebra. Mechanical Industry Press, Peking (2007)
4. Han, X., Ye, Z., Huang, X.: Pythagorean Bézier hodograph curve and its offsets. Mathematica Numerica Sinica 23, 27–36 (2001)
5. Tang, W., Liu, C.: Pythagorean hodograph curve and its application. Manufacturing Technology & Machine Tool 12, 64–67 (2005)
6. Cheng, W., Cao, J., Wang, G.: Pythagorean-hodograph C-curve. Journal of Computer Aided Design & Computer Graphics 7, 822–827 (2007)

The Bisector of a Point and a Plane Algebraic Curve

Huahao Shou[1], Tao Li[1], and Yongwei Miao[2]

[1] College of Science, Zhejiang University of Technology, Hangzhou, China
[2] College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China
{shh,ywmiao}@zjut.edu.cn

Abstract. A subdivision algorithm to compute the true bisector of a fixed point and a plane algebraic curve is presented. Quadtree data structure and interval analysis technique are used to accelerate the speed. Unlike the algorithm proposed in "The bisector of a point and a plane parametric curve" published on Computer Aided Geometric Design volume 11 page 117-151 in 1994 by R. T. Farouki and J. K. Johnstone our algorithm need not a trimming procedure which is usually complicated.

Keywords: Bisector, Voronoi diagram, algebraic curve.

1   Introduction

Point/curve bisectors arise in a variety of geometric "reasoning" and geometric decomposition problems (e.g., planning paths of maximum clearance in robotics, or computing Voronoi diagrams for areas with curvilinear boundaries) [1]. They play a key role in computing the medial axis transform or "skeleton" of planar shapes [2]. Yap discusses the bisectors of points, lines, and circles in the context of Voronoi diagrams [3]. Also in the context of Voronoi diagrams, Held treats the construction of bisectors in numerical control machining applications [4]. Yap and Alt analyze the complexity of the bisector computation for two algebraic curves, quoting an upper bound of $16m^6$ on the degree of the bisector for curves of degree m [5]. Nackman and Srinivasan discuss generic properties of the bisector of two linearly separable sets of arbitrary dimension, from the perspective of point set topology [6]. Elber and Kim presented a simple a robust method for computing the bisector of two planar rational curves [7]. Given a point and a rational space curve, in [8] Elber and Kim showed that the bisector surface is a rational ruled surface. Moreover, given two rational space curves, Elber and Kim showed that the bisector surface is rational except for the degenerate case in which the two curves are coplanar. In [9] Peternell studied algebraic and geometric properties of curve-curve, curve-surface, and surface-surface bisectors.

In [1] Farouki and Johnstone showed that the bisector of a point and a plane parametric curve may be regarded as a subset of a variable distance offset curve which has the attractive property, unlike fixed distance offsets, of being generically a rational curve. This untrimmed bisector usually exhibits irregular points and self-intersections similar in nature to those seen on fixed distance offsets. Therefore a trimming procedure, which identifies the parametric subsegments of this curve that constitute the true bisector, is needed afterward. However, to our best knowledge, due to

manipulation difficulty of algebraic curve there is no published work on the computation of the bisector of a point and a plane algebraic curve. In this paper a subdivision algorithm to compute the true bisector of a fixed point and a plane algebraic curve is presented. Quadtree data structure and interval analysis [10] technique are used to accelerate the speed. Unlike the algorithm proposed in [1] our algorithm need not a trimming procedure which is usually complicated.

The rest of this paper is organized as follows: In Section 2 we give the subdivision algorithm for computing the bisector of a point and a plane algebraic curve in detail. In Section 3 we present some examples to show that the proposed algorithm is reliable and efficient. Finally in Section 4 we give a conclusion.

2   Algorithm

Given a planar point $P(x_0, y_0)$ and a planar algebraic curve $f(x, y) = 0$ on a rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$, where $f(x, y)$ are polynomial in two variables. Suppose that the pixel size is ε. To find the bisector of the point $P(x_0, y_0)$ and the algebraic curve $f(x, y) = 0$ on the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ is equivalent to find all those pixels whose distances to the point $P(x_0, y_0)$ and to the algebraic curve $f(x, y) = 0$ are equal.

The first key step of the algorithm is to find the pixel set $A = \bigcup_{i=1}^{n} \left\{ [a_i, b_i] \times [c_i, d_i] \right\}$ of all those pixels where the algebraic curve $f(x, y) = 0$ passes though. By means of centered form interval arithmetic [11] we compute the value interval $\left[\underline{f}, \overline{f} \right]$ of $f(x, y)$ on rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$. If $0 \notin \left[\underline{f}, \overline{f} \right]$, the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ can not contain the algebraic curve $f(x, y) = 0$, we then simply discard the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$. Otherwise, if $0 \in \left[\underline{f}, \overline{f} \right]$, the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ may contain the algebraic curve $f(x, y) = 0$, we then subdivide the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ into four small rectangles at its midpoint. We repeat this process until the size of rectangle considered is equal to or smaller than the pixel size ε. If the rectangle whose size is equal to or smaller than the pixel size ε is still can not be discarded we then record this rectangle into the algebraic curve pixel set A.

The second key step of the algorithm is to find the pixel set B of all those pixels whose distances to the algebraic curve pixel set A and to the point $P(x_0, y_0)$ are equal. To this end, we first calculate the distance interval

$$\left[\underline{g_i}, \overline{g_i} \right] = \sqrt{\left([\underline{x}, \overline{x}] - [a_i, b_i] \right)^2 + \left([\underline{y}, \overline{y}] - [c_i, d_i] \right)^2}$$ between   the   rectangle

$[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ and the pixel $[a_i, b_i] \times [c_i, d_i]$ by means of ordinary interval arithmetic. Let $\underline{h} = \min\limits_{1 \le i \le n} \{\underline{g}_i\}$, $\overline{h} = \min\limits_{1 \le i \le n} \{\overline{g}_i\}$, then the interval $[\underline{h}, \overline{h}]$ is the distance interval between the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ and the algebraic curve pixel set $A = \bigcup\limits_{i=1}^{n} \{[a_i, b_i] \times [c_i, d_i]\}$. Note that x_0 and y_0 can be represented as interval forms $[x_0, x_0]$ and $[y_0, y_0]$, we then calculate the distance interval $\left[\underline{l}, \overline{l}\right] = \sqrt{\left([\underline{x}, \overline{x}] - x_0\right)^2 + \left([\underline{y}, \overline{y}] - y_0\right)^2}$ between the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ and the point $P(x_0, y_0)$ using the ordinary interval arithmetic. If $[\underline{h}, \overline{h}]$ and $\left[\underline{l}, \overline{l}\right]$ do not intersect, that means the distance from any point in the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ to the algebraic curve can not be equal to the distance from this point to the point $P(x_0, y_0)$, therefore the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ does not contain any bisector point, and can be safely discarded. Otherwise, if $[\underline{h}, \overline{h}]$ and $\left[\underline{l}, \overline{l}\right]$ intersect, the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ may contain bisector point and therefore can not be discarded, we then subdivide the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ into four small rectangles at its midpoint. We repeat this process until the size of rectangle considered is equal to or smaller than the pixel size ε. If the rectangle whose size is equal to or smaller than the pixel size ε is still can not be discarded we then record this rectangle into bisector pixel set B. Finally the bisector pixel set B contains all those pixels whose distances to the algebraic curve and to the given point are equal and is what we want to compute. What follows is the algorithm in detail:

(1) Input the polynomial in two variables $f(x, y)$ which represents the algebraic curve, the given point $P(x_0, y_0)$, the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ and the pixel size is ε.

(2) Compute the value interval $\left[\underline{f}, \overline{f}\right]$ of $f(x, y)$ on rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ by means of centered form interval arithmetic. If $0 \notin \left[\underline{f}, \overline{f}\right]$, the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ is discarded, otherwise the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ is subdivided into four small rectangles at its midpoint. Repeat this process until the size of rectangle considered is equal to or smaller than the pixel size ε. If the rectangle whose size is equal to or smaller than the pixel size ε is still can not be discarded the rectangle is recorded into the algebraic curve pixel set A. Finally we get $A = \bigcup\limits_{i=1}^{n} \{[a_i, b_i] \times [c_i, d_i]\}$.

(3) Calculate the distance interval $\left[\underline{g}_i, \overline{g}_i\right]$

$$= \sqrt{\left(\left[\underline{x}, \overline{x}\right] - \left[a_i, b_i\right]\right)^2 + \left(\left[\underline{y}, \overline{y}\right] - \left[c_i, d_i\right]\right)^2}$$ between the rectangle

$[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ and the pixel $[a_i, b_i] \times [c_i, d_i]$ using ordinary interval arithmetic.

Let $\left[\underline{h}, \overline{h}\right] = \left[\min_{1 \le i \le n}\{\underline{g}_i\}, \min_{1 \le i \le n}\{\overline{g}_i\}\right]$. Calculate the distance interval

$$\left[\underline{l}, \overline{l}\right] = \sqrt{\left(\left[\underline{x}, \overline{x}\right] - x_0\right)^2 + \left(\left[\underline{y}, \overline{y}\right] - y_0\right)^2}$$ between the rectangle

$[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ and the point $P(x_0, y_0)$ using the ordinary interval arithmetic. If

$[\underline{h}, \overline{h}]$ and $\left[\underline{l}, \overline{l}\right]$ do not intersect, the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ is discarded,

otherwise the rectangle $[\underline{x}, \overline{x}] \times [\underline{y}, \overline{y}]$ is subdivided into four small rectangles at its midpoint. For every small rectangle repeat step (3) until the size of rectangle considered is equal to or smaller than the pixel size ε. If the rectangle whose size is equal to or smaller than the pixel size ε is still can not be discarded the rectangle is recorded into the bisector pixel set B.

(4) Draw the pictures of the given point $P(x_0, y_0)$ and the algebraic curve pixel set A and the bisector pixel set B. The algorithm is completed.

3   Examples

We implemented the above algorithm using Mathematica 5.0. Several well chosen examples are tested on a personal computer with Intel® Core™2 CPU 6300 @ 1.86 GHz and 2GB RAM.

Example 1: The algebraic curve is $x^2 + y^2 - x - y + \dfrac{7}{16} = 0$ which represents a

circle with center at $(\dfrac{1}{2}, \dfrac{1}{2})$ and radius $\dfrac{1}{4}$, the given point is $(0.62, 0.62)$, the

rectangle is $[0,1] \times [0,1]$ and $\varepsilon = \dfrac{1}{256}$. The computed results are showed in Figure 1. The total CPU time used is 104.375 seconds, total number of subdivisions is 886, and total number of pixels (including the algebraic curve and the bisector) is 896.

Example 2: The algebraic curve is $4x^2 - 4x - y + \dfrac{9}{8} = 0$ which represents a

parabola, the given point is $(0.55, 0.25)$, the rectangle is $[0,1] \times [0,1]$ and

$\varepsilon = \dfrac{1}{256}$. The computed results are showed in Figure 2. The total CPU time used is

191.359 seconds, total number of subdivisions is 1182, and total number of pixels (including the algebraic curve and the bisector) is 1308.

Example 3: The algebraic curve is $x^2 + \dfrac{9}{4}y^2 - x - \dfrac{9}{4}y + \dfrac{43}{64} = 0$ which represents

an ellipse, the given point is $\left(\dfrac{3}{8}, \dfrac{5}{8}\right)$, the rectangle is $[0,1] \times [0,1]$ and $\varepsilon = \dfrac{1}{256}$.
The computed results are showed in Figure 3. The total CPU time used is 148.578 seconds, total number of subdivisions is 1054, and total number of pixels (including the algebraic curve and the bisector) is 1135.

Example 4: The algebraic curve is $256x^4 + 256x^2y^2 - 512x^3 - 256xy^2$
$+ 288x^2 + 112y^2 - 32x - 64y + 13 = 0$ which represents a bicorn, the given

point is $(0.5, 0.7)$, the rectangle is $[0,1] \times [0,1]$ and $\varepsilon = \dfrac{1}{256}$. The computed

results are showed in Figure 4. The total CPU time used is 63.125 seconds, total number of subdivisions is 836, and total number of pixels (including the algebraic curve and the bisector) is 664.

Example 5: The algebraic curve is $((x + \dfrac{1}{2})^2 + (y + \dfrac{1}{2})^2 - 1)^3 - (x + \dfrac{1}{2})^2$

$(y + \dfrac{1}{2})^3 = 0$ which represents a heart curve, the given point is $(0.24, 0.3)$, the

rectangle is $[-2,1] \times [-2,1]$ and $\varepsilon = \dfrac{1}{256}$. The computed results are showed in

Figure 5. The total CPU time used is 208.094 seconds, total number of subdivisions is 1441, and total number of pixels (including the algebraic curve and the bisector) is 1355.
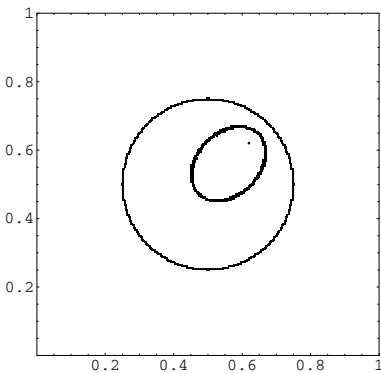
Fig. 1. Bisector of a point and a circle
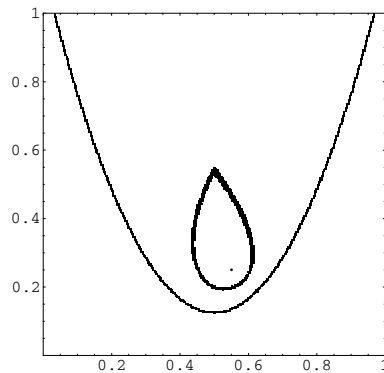
Fig. 2. Bisector of a point and a parabola
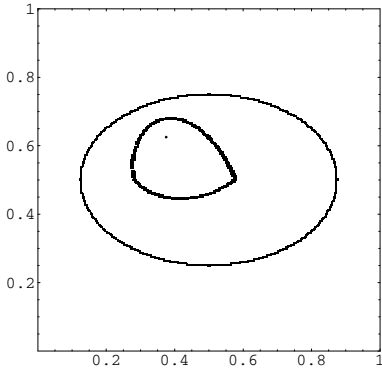
Fig. 3. Bisector of a point and an ellips
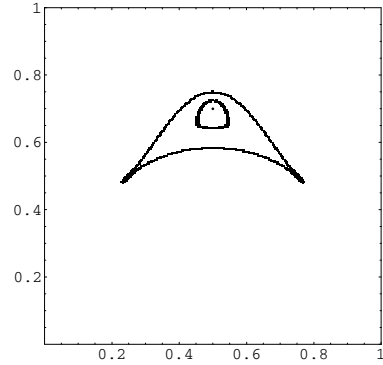
Fig. 4. Bisector of a point and a bicorn
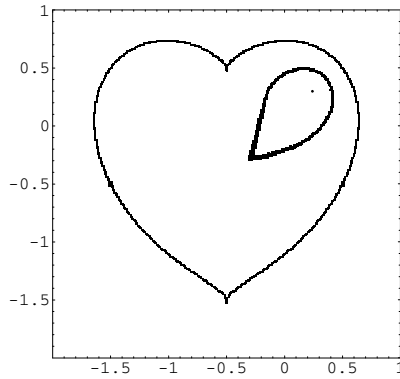
Fig. 5. Bisector of a point and a heart curve

4   Conclusion

From the above examples we can see that the proposed algorithm can find the bisector of a given point and a planar algebraic curve reliably and effectively. Unlike the algorithm proposed in "The bisector of a point and a plane parametric curve" published on Computer Aided Geometric Design volume 11 page 117-151 in 1994 by R. T. Farouki and J. K. Johnstone our algorithm need not a trimming procedure which is usually complicated. However, due to the conservativeness of the interval arithmetic, sometimes the computed bisector may looks fatter than it should be, this is because some pixels which is close to but not on bisector can not be discarded.

References

1. Farouki, R.T., Johnstone, J.K.: The bisector of a point and a plane parametric curve. Computer Aided Geometric Design 11, 117–151 (1994)
2. Lee, D.T.: Medial axis transformation of a planar shape. IEEE Transactions on Pattern Analysis and Machine Intelligence PAMI-4, 363–369 (1982)
3. Yap, C.K.: An O(n log n) algorithm for the Voronoi diagram of a set of simple curve segments. Discrete and Computational Geometry 2, 365–393 (1987)
4. Held, M.: On the Computational Geometry of Pocket Machining. Springer, Berlin (1991)
5. Yap, C.K., Alt, H.: Motion planning in the CL-environment. In: Dehne, F., Santoro, N., Sack, J.-R. (eds.) WADS 1989. LNCS, vol. 382, pp. 373–380. Springer, Heidelberg (1989)
6. Nackman, L.R., Srinivasan, V.: Bisectors of linearly separable sets. Discrete and Computational geometry 6, 263–275 (1991)
7. Elber, G., Kim, M.S.: Bisector curves of planar rational curves. Computer Aided Design 30, 1089–1096 (1998)
8. Elber, G., Kim, M.S.: The bisector surface of rational space curves. ACM Transactions on Graphics 17, 32–49 (1998)
9. Peternell, M.: Geometric properties of bisector surfaces. Graphical Models 62, 202–236 (2000)
10. Moore, R.E.: Interval Analysis. Prentice-Hall, Englewood Cliffs (1966)
11. Martin, R., Shou, H., Voiculescu, I., Bowyer, A., Wang, G.: Comparison of interval methods for plotting algebraic curves. Computer Aided Geometric Design 19, 553–587 (2002)

Biarc Approximation of Planar Algebraic Curve

Huahao Shou[1], Wen Shi[1], and Yongwei Miao[2]

[1] College of Science, Zhejiang University of Technology, Hangzhou, China
[2] College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China
{shh,ywmiao}@zjut.edu.cn

Abstract. A novel algorithm for approximating planar algebraic curve with biarcs is presented. With reasonable selection of split points the algebraic curve is segmented according to convexity and monotonicity. For every curve segment biarc is constructed based on tangents of two end points and careful selection of common tangent point of the biarc. The whole approximate biarc curve keeps some important geometric features of the original algebraic curve such as convexity, monotonicity and G^1 continuity and is easy to operate and achieve in NC machining. Numerical experiments show that the algorithm is reliable and efficient. The approximation error can be controlled by recursive call of the algorithm. As a direct application, we can apply the algorithm to calculate the offsets of planar algebraic curve.

Keywords: Algebraic curve, biarc curve, approximation algorithm, offset, normal direction error.

1 Introduction

Biarc curve, was firstly designed for shipbuilding industry in 1970 and provided the basic curve and hull surface definition for the widely-used BRITSHIPS system, and was introduced later to academia by Bolton [1]. It's also discussed in the book "Computational Geometry" by Su Buqing and Liu Dingyuan [2].

Arc spline is made up of circle arc and straight line and is easy to manipulate and calculate in shape simulation, as well as in describing the path of the NC machine tool. Compared with linear approximation, circle arc approximation has more advantage. Furthermore, the fairness of biarc approximation is better than single circle arc, it can interpolate end points and their tangent vectors at the same time, preserving some important geometric features of original curve. Approximation to data point set by G^1 biarc was investigated in literature [3-5], to parametric spline curve by biarc was investigated in literature [6-12]. It is necessary to investigate biarc approximation of algebraic curve, for there are more and more applications of algebraic curve and surface in computer aided design and computer graphics recently.

Generally, biarc can be divided into C-type biarc and S-type biarc. In this paper, only C-type biarc is needed. The rest of this paper is organized as follows: In Section 2, we briefly give the definition of biarc and the radiuses of two arcs, and then we can obtain the fairest joint and its calculation. In Section 3, algorithms for biarc and offset approximation of planar algebraic curve are developed. In Section 4, we discuss the

approximation error. In Section 5, an algebraic curve example is given for biarc and offset approximation. Finally in Section 6 we make a conclusion.

2   Definition and Property of Biarc

Definition 2. The two smoothly connected circular arc D_1, D_2 are said to form a biarc, represented by the given two distinct end points P_1, P_2 and unit tangent vectors t_1, t_2 (Fig.1), satisfy the following properties:

- The circular arc D_1 passes through P_1 and has the tangent vector at P_1 ,the circular arc D_2 passes through P_2 and has tangent vector at P_1 ;
- The two circular arcs must have a point of common tangency, the point P called joint and the tangent vector is t .

In order to form the biarc, there are six conditions to determine. The definition provides the five conditions. The sixth unknown condition is choosing the joint.

In this paper, we uniformly divide the original curve into the curve with no inflection for convenient. To insure this, we take $|\theta| < \min(|\alpha_1|, |\alpha_2|)$.

2.1   Biarc Radius

As showed in Fig.1, let
$$|P_1P_2| = L, \angle P_1OP = \theta, \angle P_2P_1P_t = \alpha_1, \angle P_1P_2P_t = \alpha_2, \angle P_2P_1P = \beta_1, \angle P_1P_2P = \beta_2.$$
We can obtain R_1, R_2
$$R_1 = \frac{L\sin((\alpha_2+\theta)/2)}{2\sin((\alpha_1+\alpha_2)/2)\sin((\alpha_1+\theta)/2)}, R_2 = \frac{L\sin((\alpha_1-\theta)/2)}{2\sin((\alpha_1+\alpha_2)/2)\sin((\alpha_2-\theta)/2)}. \quad (1)$$
Actually, formula (1) gives the biarc radius of relative curvature.
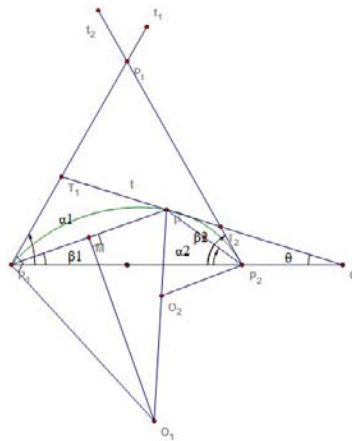
Fig. 1. Biarc radius

2.2   Choice of Joint P

The rule to choose biarc joint P is to make the connection as smoothly as possible, not just satisfy G^1 continuity. No matter what value of θ when $\alpha_1 = \alpha_2$, we have $R_1 = R_2$ by (1), thus the biarc is degenerated to a single circular. We suppose that $\alpha_1 \neq \alpha_2$ in this paper.

Connect P_1, P_2, take P_1 as the origin of the Cartesian orthogonal coordinate system and $P_1 P_2$ as the x-axis to establish a coordinate system. Then according to the relation of the global coordinate and local coordinate system, we can calculate that we need.

Let $H_1(\theta) = |R_1/R_2 - 1|$, then $H_1(\theta)$ takes the minimum value when $\theta = 0$. The change of biarc curvature reaches the minimum at this moment. Therefore $P_1 P$ and PP_2 are two angle bisectors of the triangle $\Delta P_1 P_t P_2$, P is the incenter of the triangle $\Delta P_1 P_t P_2$. So we can obtain the two centre of the biarc. The center coordinates obtained above are in the local coordinate system, so we need to transform them into the global coordinate system.

3   Biarc Approximation

3.1   Segmentation of Algebraic Curve and Determination of the Control Triangle

Firstly, divide the algebraic curve into segments at singular points, inflection points and extreme points [13]. Suppose the algebraic curve is $F(x, y) = 0$, let the start point of the algebraic curve segment is P_1, and the end point is P_2, and then the tangent equation t_1 which passes through P_1 is

$$F_x(x_1, y_1)(x - x_1) + F_y(x_1, y_1)(y - y_1) = 0$$

The tangent equation t_2 passes through P_2 can be determined similarly. Then the intersection point P_t between t_1 and t_2 is determined. Hence the triangle $\Delta P_1 P_t P_2$ is also determined. Also the length of the biarc radiuses, the position of the centers can be determined. An algorithm for approximation curve can be derived after calculating the central angle of each circle arc.

3.2   Offset Approximation of Algebraic Curve

Definition 2. *Since biarc curve can be represented in parametric form, therefore, offset* $D_r(t)$ *of biarc curve* $D(t)$ *can be defined by*

$$D_r(t) = D(t) + r \cdot N(t) \tag{2}$$

Where r is a constant radius, $N(t)$ is the unit normal of $D(t)$. After the biarc approximation curve $D(t)$ of the planar algebraic curve is obtained as previously described, the offset approximation curve of the algebraic curve can be obtained

straightforwardly by offsetting the biarc curve. Obviously the offset approximation error is the same with the biarc approximation error.

3.3 Algorithm for Biarc and Offset Approximation of Algebraic Curve

Input: An algebraic curve F and the tolerance δ.

Output: Biarc and offset approximation curves of the algebraic curve within error tolerance δ.

- Divide the original algebraic curve into segments at singular point, inflection point and extreme point;
- For every algebraic curve segment, compute tangents at the two end points and their intersection point to obtain the control triangle;
- Compute the incenter of the control triangle, that is the joint of the biarc;
- Compute the radius of the two circle arcs, the coordinates of the center and the central angel from the above formulas to obtain the biarc approximation of the algebraic curve segment;
- Check the approximation error, if the error $e_k < \delta$, then stop the process. Otherwise, separate the segment into two segments, recursively call the algorithm until the error within tolerance;
- Calculate the offset of biarc approximation, use it to approximate offsets of the original algebraic curve.

4   Error Discussion

To compute the distance between the approximation curve and the original curve is the most important thing to evaluate the algorithm. Theoretically Hausdoff distance is difficult to calculate. Usually a simpler method for error calculation is used instead.

Assuming that there is a planar algebraic curve $F(x, y) = 0$, and its biarc approximation is $D_i(t)$, $i = 0, 2 \cdots, n-1$.

Firstly, divide the algebraic curve segment between the nodes P_i and P_{i+1} into n parts, then calculate the coordinates of all points.

For general algebraic curves, divide the value of x-axis between the nodes P_i and P_{i+1} into n parts. For those algebraic curves which can be transformed into parametric form, divide the parameter t between the nodes P_i and P_{i+1} into n parts.

According to the joint of the corresponding biarc segment, P_{i_k} belongs to the first arc when $x_{i_k} < x_p$, otherwise it belong to the second.

Finally, calculate the normal direction error, that is,

$$e_{i_k} = \left| \sqrt{(x_{i_k} - x_{o_k})^2 - (y_{i_k} - y_{o_k})^2} - R_k \right| \tag{3}$$

Where $\left(x_{o_k}, y_{o_k} \right)$ is the center and R_k is the radius of the corresponding circular arc.

Let $e_i = \max_{k=1}^{l-1} \{e_{i_k}\}$ .If $e_i > \delta$,we divide this algebraic curve segment into two smaller segments at its mid point and recursively call the algorithm until the computed approximation error is equal to or smaller than tolerance δ .

5   Example

Give an algebraic curve $F : x^6 + y^6 + 3x^4y^2 + 3x^2y^4 + 2x^2y^2 - x^4 - y^4 = 0$ (Fig.2).

Due to symmetry property we only need to approximate its right quarter . The right quarter of the algebraic curve can be divided into four parts, the split points are: $(0,0), (\sqrt{30}/9, \sqrt{6}/9), (1,0), (\sqrt{30}/9, \sqrt{6}/9)$.

The corresponding expression of the biarc which approximate the right quarter of the algebraic curve are as follows:(The equation set (4) represents the biarc approximation for left upper part, (5) for the right upper part, (6) for the left lower part, and (7) for the right lower part.)

$$\begin{cases} x_1 = 1.0021\cos(\theta) + 0.7086 \\ y_1 = 1.0021\sin(\theta) - 0.7086 \end{cases}, \begin{cases} x_2 = 0.7571\cos(\theta) + 0.6086 \\ y_2 = 0.7571\sin(\theta) - 0.4849 \end{cases} \tag{4}$$

$$\begin{cases} x_3 = 0.5220\cos(\theta) + 0.6086 \\ y_3 = 0.5220\sin(\theta) - 0.2498 \end{cases}, \begin{cases} x_4 = 0.2177\cos(\theta) - 0.7823 \\ y_4 = 0.2177\sin(\theta) \end{cases} \tag{5}$$

$$\begin{cases} x_5 = 1.0021\cos(\theta) + 0.7086 \\ y_5 = -1.0021\sin(\theta) + 0.7086 \end{cases}, \begin{cases} x_6 = 0.7571\cos(\theta) + 0.6086 \\ y_6 = -0.7571\sin(\theta) + 0.4849 \end{cases} \tag{6}$$

$$\begin{cases} x_7 = 0.5220\cos(\theta) + 0.6086 \\ y_7 = -0.5220\sin(\theta) + 0.2498 \end{cases}, \begin{cases} x_8 = 0.2177\cos(\theta) - 0.7823 \\ y_8 = -0.2177\sin(\theta) \end{cases} \tag{7}$$

Fig. 3 shows the overall approximation effect of the right quarter algebraic curve, where the green dashed line represents the original curve, the blue and black solid lines represent the biarc approximation. The red solid line represents the polyline which connect the joints and the end points of the biarc.
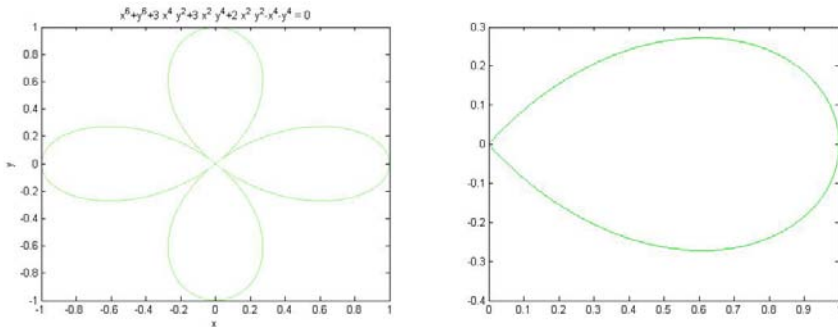
Fig. 2. An algebraic curve and its right quarter
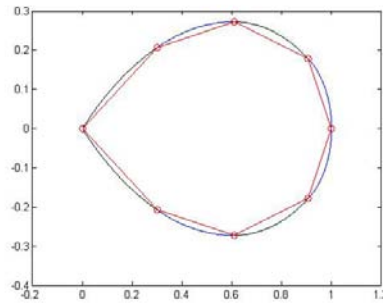
Fig. 3. Biarc approximation of the algebraic curve

Since the right quarter of the algebraic curve is also symmetrical to x axis, the left upper and the left lower part, the right upper and the right lower part all have the same approximation error. Fig.4 shows respectively the error functions of the left and the right part biarc approximation.
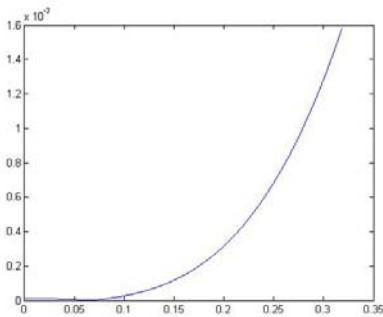
(a) First left upper (lower) part
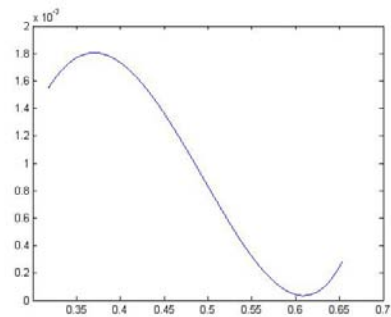
(b) Second left upper (lower) part
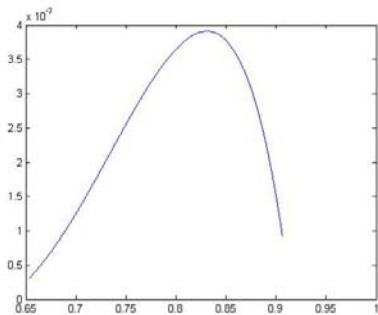
(c) First right upper (lower) part
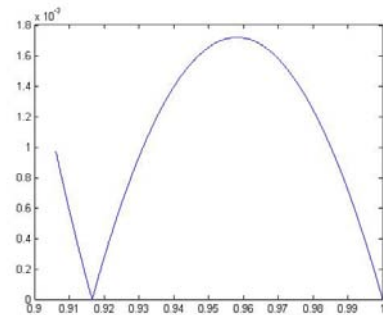
(d) Second right upper (lower) part

Fig. 4. Error function

As one can see from Fig.5(a) the outer offset is not closed, the inner offset has a self intersection point and redundant parts. Therefore some procedures need to be done afterwards. For the outer offset, we need to add a circular arc with center at the origin and radius r. For the inner offset, we calculate the self intersection point and remove redundant parts. Fig.5(b) shows the result after these processing.

Obviously the error function of offset approximation is the same as biarc approximation.

Calculated offset approximation of the algebraic curve is shown in Fig.5(a) where r takes 0.03.

(a) Before processing   (b) After processing
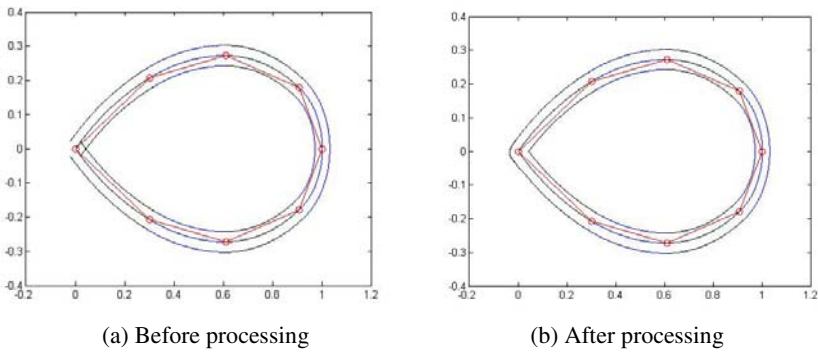
Fig. 5. Offset approximation of the algebraic curve

6   Conclusions

From above example we can see that the proposed algorithm for biarc approximation of planar algebraic curve is feasible and efficient. The whole approximate biarc curve keeps some important geometric features of the original algebraic curve such as convexity, monotonicity and G^1 continuity and can be applied to NC machining directly. The approximation error can be controlled within a certain given tolerance by recursive call of the algorithm. As a direct application, the biarc approximation algorithm is applied to calculate the offsets of planar algebraic curve.

References

1. Bolton, K.M.: Biarc curves. Computer Aided Design 7, 88–92 (1975)
2. Su, B., Liu, D.: Computational geometry. Shanghai Scientific & Technical Publishers, Shanghai (1982)
3. Meek, D.S., Walton, D.J.: Approximation of discrete data by arc splines. Computer Aided Design 24, 301–306 (1992)

4. Piegl, L.A., Tiller, W.: Data approximation using biarcs. Engineering with Computers 18, 59–65 (2002)
5. Schonherr, J.: Smooth biarc curves. Computer Aided Design 25, 365–370 (1993)
6. Dong, G., Liang, Y., He, Z.: Spline curve and its biarc approximation. Acta Mathematae Applagatae Sinica 1, 333–340 (1978)
7. Piegl, L.A., Tiller, W.: Biarc approximation of NURBS curves. Computer Aided Design 34, 807–814 (2002)
8. Piegl, L.A., Rajab, K., Smarodzinava, V., Valavanis, K.P.: Using a biarc filter to compute curvature extremes of NURBS Curves. Engineering with Computers 24, 379–387 (2009)
9. Meek, D.S., Walton, D.J.: Approximating quadratic NURBS curves by arc splines. Computer Aided Design 25, 371–376 (1993)
10. Meek, D.S., Walton, D.J.: Approximating smooth planar curves by arc splines. Journal of Computer and Applied Mathematics 59, 221–231 (1995)
11. Walton, D.J., Meek, D.S.: Approximation of quadratic Bezier curves by arc splines. Journal of Computer and Applied Mathematics 54, 107–120 (1994)
12. Wang, G., Sun, J.: The biarc approximation of planar NURBS curve and its offset. Journal of Software 11, 1368–1374 (2000)
13. Shou, H., Shen, J., Yoon, D.: Numerical computation of singular and inflection points on planar algebraic curves. In: Proceedings of 2007 International Conference on Computer Graphics & Virtual Reality, pp. 133–138. CSREA Press, Las Vegas (2007)
14. Elber, G., Lee, I.K., Kim, M.S.: Comparing offset curve approximation methods. Computer Graphics and Applications 5-6, 66–71 (1997)

On Self-complementary of Circulant Graphs

Houqing Zhou

Department of Mathematics, Shaoyang University, Hunan, China 422000

Abstract. a graph G is self-complementary if it is isomorphic to its complement $\overline{G}$. If G is a regular self-complementary graph, then G is connected and has $n = 4k + 1$ vertices and degree $r = 2k$, where n, k are positive integers. In this paper, we investigate the existence condition for self-complementary of circulant graphs with order $n = 4k + 1$. Moreover, we proved that the circulant graphs of order 17 exist self-complementary strongly regular graphs.

Keywords: strongly regular, self-complementary, circulant graphs.

1   Introduction

In this paper we consider only simple graphs. We use $V(G)$ and $E(G)$ to denote the vertex set and the edge set of G, respectively. If $v_i \in V(G)$, denote its set of neighbors by $N_G(v_i)$, i.e., $N_G(v_i) = \{v_j \in V(G) : v_i v_j \in E(G)\}$. Given a graph G, the complement of G, denoted by $\overline{G}$, the complement $\overline{G}$ has the same vertices such that two vertices of $\overline{G}$ are adjacent if and only if they are not adjacent in G.

Definition 1.1. A self-complementary graph is a graph which is isomorphic to its complement.

Let G be a self-complementary graph, σ is an isomorphic mapping going from G to $\overline{G}$, then σ is called a complementing permutation of G. A self-complementary graph will be of order $4k$ or $4k + 1$ for some natural number k and of diameter 2 or 3. The simplest self-complementary graphs are the 4-vertex path graph and the 5-vertex cycle graph.

Definition 1.2. Let $G = (V, E)$ be a regular graph with n vertices and degree r. G is said to be strongly regular if there are also integers, λ and μ such that: Every two adjacent vertices have λ common neighbors. Every two non-adjacent vertices have μ common neighbors.

A graph of this kind is sometimes said to be an $srg(n, r, \lambda, \mu)$. Obviously, the 5-vertex cycle is a self-complementary strongly regular graph.

Now we define circulant graphs.

Definition 1.3. A circulant graph $C(n, S)$ is a Cayley graph on Z_n. That is, it is a graph whose vertices are labelled $\{0,1,2,\ldots,n-1\}$, with two vertices labelled i and j adjacent iff $(i-j)(\mathrm{mod}\ n) \in S$, where $S \subset Z_n$ has $S = -S$ and $0 \notin S$. For a circulant digraph, the condition that $S = -S$ is removed. Self-complementary graphs have been studied by several authors (see[1], [2], [3], [4], [5]). In[1] and [3], a property conjectured by Kotzig is investigated which would imply that a self-complementary graph is strongly regular. In [2] Boolean techniques are used to enumerate regular and strongly regular self-complementary graphs. The corresponding sets of quadratic equations are solved for $n = 4k+1, k = 2,3,4$, under the assumption that σ consists of a fixed point and a single cycle, yielding only Paley type solutions. [4] proved that if $G = (V, E)$ is a self-complementary graph and σ is a complementing permutation of G. Then:

  i $|V| \equiv 0,1(\mathrm{mod}\ 4)$;

  ii σ has at most one fixed point and the length of every other cycle of σ is a multiple of 4 .

In[5], a self-complementary graph is strongly regular if and only if it is strongly edge triangle regular have been proved. Kotzig put forward a question on strongly regular self-complementary graphs(see [6]). That is, for any positive integers k, whether there exists a strongly regular self-complementary graph whose order is $4k+1$, where $4k+1 = x^2 + y^2$, x and y are positive integers. In this paper, we shall investigate the existential condition for strongly regular self-complementary circulant graphs with order $n = 4k+1$. In Section 2, we shall introduce notation of self-complementary graphs, strongly regular graphs. In Section 3, we quote some lemmas and also summarize properties of Paley graphs. In Section 4, we obtain some results of circulant self-complementary graphs.

2   Some Basic Preliminaries

We begin by defining terminology and introducing notation. Throughout this discussion, all matrices will be real and symmetric.

   A graph G is said to be r-regular if every vertex $v \in V(G)$ is incident with exactly r edges of G. The complement of regular graph is regular, the complement of strongly regular graph is also strongly regular, a connected strongly regular graph has diameter 2 (see [7]). A vertex u in a self-complementary graph is called a fixed vertex if $\sigma(u) = u$ for some complementing permutation σ. The set of all complementing permutations of G is denoted $\Gamma(G)$. Sachs ([8]) proved the existence of exactly one fixed vertex associated with each $\sigma \in \Gamma(G)$ when G is

of odd order and non-existence otherwise. For a self-complementary graph G, there exists isomorphism $\sigma : G \to \overline{G}$, i.e., if there exists a permutations σ of the vertex set $V(G)$ which maps every edge (non-edge) to a non-edge (edge).

The parameters of strongly regular graphs satisfy a number of restrictions, some of the more important are to ignore here. Paley graphs are self-complementary strongly regular graphs and Hamiltonian, the complement of any Paley graph is isomorphic to itself, i.e., via the mapping that takes a vertex x to $xk \mod q$, where k is any non-residue mod q. The eigenvalues of Paley graphs are $\dfrac{q-1}{2}$ (with multiplicity 1) and $\dfrac{-1 \pm \sqrt{q}}{2}$ (both with multiplicity $\dfrac{q-1}{2}$).

When q is prime, its Paley graph is a Hamiltonian circulant graph. Paley graphs are quasi-random: the number of times each possible constant-order graph occurs as a subgraph of a Paley graph is (in the limit for large q) the same as for random graphs, and large sets of vertices have approximately the same number of edges as they would in random graphs(see[9]).

In what follows, we consider 3-circulant graphs and 4-circulant graphs.

Since circulant graphs are vertex-transitive, then we only consider the neighbors of one vertex, and give the first row of its adjacent matrix.

3 Some Lemmas

The number of triangles in G containing a vertex v is called the triangle number of v in G, denoted by $t(v)$, and $\overline{t}(v)$ denote the triangle number of v in $\overline{G}$. Triangle number $t(e)$ of an edge e is also defined in similar terms. A graph G is vertex triangle regular if its vertices have the same triangle number and is strongly vertex triangle regular if it is regular also. Edge triangle regular and strongly edge triangle regular is defined similarly([5]). A graph G is vertex triangle regular if all of its vertices have the same triangle number and is strongly vertex triangle regular (s, v, t, r) if it is regular also. A graph G is edge triangle regular if all of its edges have the same triangle number and is strongly edge triangle regular (s, e, t, r) if it is regular also. We require the following basic properties of self-complementary graphs.

Lemma 3.1([5]). A graph G is strongly regular if and only if both G and $\overline{G}$ are strongly edge triangle regular.

Lemma 3.2([5]). Every strongly edge triangle regular graph is strongly vertex triangle.

Lemma 3.3 ([7]). A regular connected graph G is strongly regular if and only if it has exactly three distinct eigenvalues.

4   Main Results

Now, we turn our attention to a subset of the class of circulant graphs: 3- and 4-circulant graphs. We begin with 3-circulant graphs. All 3-circulant graphs are 3-regular. Since the sum of the degrees of the vertices must be two times the number of edges, then 3-circulant graphs must have an even number of vertices. Therefore, in what follows we shall assume that n is even, since 3-circulant graphs are 3-regular, and according to the complementary graph of a strongly regular graph must be strongly regular(the complete and null graphs are vacuously strongly regular, often these trivial cases are excluded). Then we deduce the complementary of 3-circulant graphs be $n-4$ regular, note that n is even, obviously, $n-4 \neq 3$, hence, 3-circulant graphs and their complementary are non-isomorphic. Yielding immediately, we have the following theorem.

Theorem 4.1. All 3-circulant graphs are not self-complementary graphs.

Next, we consider the 4-circulant graphs. A 4-circulant graph is 4-regular and has n vertices and $2n$ edges. For example, circulants $C(9,\{a,b\}),1 \leq a < b \leq 4$, it have six form, i.e., $C(9,\{1,2\})$, $C(9,\{1,3\})$, $C(9,\{1,4\})$, $C(9,\{2,3\})$, $C(9,\{2,4\})$, $C(9,\{3,4\})$. Via a straightforward calculation, their eigenvalues of the corresponding form are given in the following $Table$ 1, respectively. It shows that $C(9,\{a,b\})$ have more than three distinct eigenvalues.

Table 1. The Spectrum of 4-circulant graph: $C(9,\{a,b\})$

Form	Spectrum
$C(9,\{1,2\})$	$4,-2^2,\left[2\cos\dfrac{\pi}{9}\right]^2,\left[-2\cos\dfrac{2\pi}{9}\right]^2,\left[-2\cos\dfrac{4\pi}{9}\right]^2$
$C(9,\{1,3\})$	$4,1^2,\left[-1+2\cos\dfrac{2\pi}{9}\right]^2,\left[-1+2\cos\dfrac{4\pi}{9}\right]^2,\left[-1-2\cos\dfrac{\pi}{9}\right]^2$
$C(9,\{1,4\})$	$4,-2^2,\left[2\cos\dfrac{\pi}{9}\right]^2,\left[-2\cos\dfrac{2\pi}{9}\right]^2,\left[-2\cos\dfrac{4\pi}{9}\right]^2$
$C(9,\{2,3\})$	$\left[-1+2\cos\dfrac{2\pi}{9}\right]^2,\left[-1+2\cos\dfrac{4\pi}{9}\right]^2,\left[-1-2\cos\dfrac{\pi}{9}\right]^2,4,1^2,$
$C(9,\{2,4\})$	$\left[2\cos\dfrac{\pi}{9}\right]^2,\left[-2\cos\dfrac{2\pi}{9}\right]^2,\left[-2\cos\dfrac{4\pi}{9}\right]^2,4,-2^2,$
$C(9,\{3,4\})$	$\left[-1+2\cos\dfrac{2\pi}{9}\right]^2,\left[-1+2\cos\dfrac{4\pi}{9}\right]^2,\left[-1-2\cos\dfrac{\pi}{9}\right]^2,4,1^2$

The *Table* 1 shows that $C(9,\{1,2\})$, $C(9,\{1,4\})$, $C(9,\{2,4\})$ are isomorphic, but they are not self-complementary. Similarly, $C(9,\{1,3\})$, $C(9,\{2,3\})$, $C(9,\{3,4\})$ are isomorphic but not self-complementary. According to the Table 1 above and Lemma 3.3, we have the following proposition.

Table 2. The spectrum of 6-circulant graph : $C(13,\{a,b,c\})$

Form	Spectrum
$C(13,\{1,2,3\})$	6, -2.41002^2, -1.66799^2, -1.51496^2, -0.43532^2, -0.11982^2, 3.14811^2
$C(13,\{1,2,4\})$	6, -1.0701^2, 0.0701^2, -1.96516^2, 0.96516^2, -3.19783^2, 2.19783^2
$C(13,\{1,2,5\})$	6, -4.14811^2, -0.880181^2, -0.564681^2, 0.514964^2, 0.667993^2, 1.41002^2
$C(13,\{1,2,6\})$	6, -1.0701^2, 0.0701^2, -1.96516^2, 0.96516^2, -3.19783^2, 2.19783^2
$C(13,\{1,3,4\})$	6, $\left[\dfrac{-1-\sqrt{13}}{2}\right]^6$, $\left[\dfrac{-1+\sqrt{13}}{2}\right]^6$
$C(13,\{1,3,5\})$	6, -4.14811^2, -0.880181^2, -0.564681^2, 0.514964^2, 0.667993^2, 1.41002^2
$C(13,\{1,3,6\})$	6, -1.0701^2, 0.0701^2, -1.96516^2, 0.96516^2, -3.19783^2, 2.19783^2
$C(13,\{1,4,5\})$	6, -2.41002^2, -1.66799^2, -1.51496^2, -0.43532^2, -0.11982^2, 3.14811^2
$C(13,\{1,4,6\})$	6, -4.14811^2, -0.880181^2, -0.564681^2, 0.514964^2, 0.667993^2, 1.41002^2
$C(13,\{1,5,6\})$	6, -2.41002^2, -1.66799^2, -1.51496^2, -0.43532^2, -0.11982^2, 3.14811^2
$C(13,\{2,3,4\})$	6, -4.14811^2, -0.880181^2, -0.564681^2, 0.514964^2, 0.667993^2, 1.41002^2
$C(13,\{2,3,5\})$	6, -2.41002^2, -1.66799^2, -1.51496^2, -0.43532^2, -0.11982^2, 3.14811^2
$C(13,\{2,3,6\})$	6, -4.14811^2, -0.880181^2, -0.564681^2, 0.514964^2, 0.667993^2, 1.41002^2
$C(13,\{2,4,5\})$	6, -1.0701^2, 0.0701^2, -1.96516^2, 0.96516^2, -3.19783^2, 2.19783^2
$C(13,\{2,4,6\})$	6, -2.41002^2, -1.66799^2, -1.51496^2, -0.43532^2, -0.11982^2, 3.14811^2
$C(13,\{2,5,6\})$	6, $\left[\dfrac{-1-\sqrt{13}}{2}\right]^6$, $\left[\dfrac{-1+\sqrt{13}}{2}\right]^6$
$C(13,\{3,4,5\})$	6, -1.0701^2, 0.0701^2, -1.96516^2, 0.96516^2, -3.19783^2, 2.19783^2
$C(13,\{3,4,6\})$	6, -2.41002^2, -1.66799^2, -1.51496^2, -0.43532^2, -0.11982^2, 3.14811^2
$C(13,\{3,5,6\})$	6, -1.0701^2, 0.0701^2, -1.96516^2, 0.96516^2, -3.19783^2, 2.19783^2
$C(13,\{4,5,6\})$	6, -4.14811^2, -0.880181^2, -0.564681^2, 0.514964^2, 0.667993^2, 1.41002^2

Proposition 4.2. All 4-circulant graphs must not be strongly regular self-complementary graphs.

We shall start with the question: How can it be decided by means of its vertices whether or not exists self-complementary. First of all,let's look at an example. Consider circulant graphs with 13 vertices $C(13,\{a,b,c\}), a,b,c \in \{1,2,3,4,5,6\}$, it contains 20 cases, let's compute the spectra of $C(13,\{a,b,c\})$. As a consequence of this computing, we have the following *Table* 2 .

From the *Table* 2 above, we obverse that exists regular self-complementary, moreover, there exists strongly regular self-complementary. Perhaps the most important thing to take this Table 2 is that thevertices of $C(13,\{a,b,c\})$ is a prime. Why will appear this kind case?

Assume that $n = 4k +1$ is a prime number such that $\frac{n-1}{2}$ is the smallest positive integer r such that $2^r \equiv 1 \pmod{n}$, where we say 2 is the quasi-primitive root of n . We construct a circulant graph G with vertex set $\{0,1,2,\ldots,n-1\}$. Let $N_G(0) = \{1,2,2^2,\cdots,2^{(2k-1)}\}$, where the subscripts are under module n . In this paper, we obtain the following results.

Theorem 4.3. The circulant graphs G of degree $r = 2k$ with $n = 4k+1, k \geq 3$ (n is a prime) vertices must exist strongly regular self-complementary graphs.

Proof. First we prove the graph G is a self-complementary graph. To this purpose, we only give a one to one correspondence from $V(G)$ to $V(G)$ such that two vertices adjacent in G if and only if that there are non-adjacent under the mapping. Without loss of generality, we may assume that

$$\theta : j \to 2^{2k} \cdot j, 0 \leq j \leq (n-1),$$

where the subscriptsare under module $n.$

It is easy to verify that the mapping θ is a one to one correspondence of the vertex set of G . If the vertex 0 is adjacent to j , then by the definition of G , $\theta(0) = 0$ is non-adjacent to $\theta(j) = 2^{2k} \cdot j$. It could be proved vice verse similarly. In general, if the vertex m is adjacent to the vertex l , then by the definition of circulant graphs, the vertex 0 is adjacent to the vertex $(m-l)$, thus we get the vertex 0 is non-adjacent to the vertex $2^{2k} \cdot (m-l)$, that is, the vertex $2^{2k} \cdot l$ is non-adjacent with the vertex $2^{2k} \cdot m$,therefore, the vertex $\theta(l)$ is non-adjacent to the vertex $\theta(m)$. It also could be proved vice verse, then the graph G is a self-complementary graph.

Now we shall prove the graph G is a regular graph. By Lemma3.1, 3.2, and the graph G is self-complementary, we only need to prove the graph G is strongly edge triangle regular. Since the circulant graphs are vertex transitive, then we only

need to prove the edges incident at 0 are strongly edge triangle regular. In fact, it is easy to see that the induced subgraph $\Gamma\left(1,2,2^2,\ldots,2^{2k-1}\right)$ is a regular graph, then we get the edges incident at 0 are strongly edge triangle regular.

According to the foregoing Lemma 3.3, we only need to prove that the adjacent matrix of G has exactly three distinct eigenvalues. We suppose the first row of the adjacent matrix is $(c_1,c_2,\ldots,c_n)$, where $c_i=1$, there exists some integer $0\le j\le(2k-1)$ such that $i=2^j$, otherwise, $c_i=0$.

We also suppose that the first row of the circulant matrix C with n vertices is $(0,1,0,\ldots,0)$. $1,\omega,\omega^2,\ldots,\omega^{n-1}$ are the eigenvalues of C, where $\omega=e^{\frac{2\pi i}{n}}$. Hence the eigenvalues of G can be expressed in the following form

$$\lambda_l=\sum_{j=1}^{n}c_j\omega^{(j-1)l},l=0,1,2,\ldots,n-1.$$

Thus we get

$$\lambda_0=2k,\quad \lambda_1=\lambda_2=\cdots=\lambda_{2^{2k-1}}=\omega+\omega^2+\cdots+\omega^{2^{2k-1}},$$

$$\lambda_{2^{2k}}=\lambda_{2^{2k+1}}=\cdots=\lambda_{2^{4k-1}}=\omega^{2^{2k}}+\omega^{2^{2k+1}}+\cdots+\omega^{2^{4k-1}}.$$

Then the graph G has at most three distinct eigenvalues. By lemma 3.3, the girth of G is no less than 3, thus G has exactly three distinct eigenvalues. Then we proved the result above. Here's an example, let $C(17,S)$ denote circulant graphs of degree 8, via computing its spectra, we obtain the spectra of $C(17,\{1,2,4,8\})$ and

$C(17,\{3,5,6,7\})$, i.e., $\left\{8,\left[\dfrac{-1-\sqrt{17}}{2}\right]^8,\left[\dfrac{-1+\sqrt{17}}{2}\right]^8\right\}$. We vcan find

$C(17,\{1,2,4,8\})$ and $C(17,\{3,5,6,7\})$ are isomorphic strongly regular self-complementary graphs.

According to Theorem 4.3 above, we arrive at the following

Corollary 4.4. Let G be a circulant graph with 17 vertices, then G is a strongly regular self-complementary if and only if G and $C(17,\{1,2,4,8\})$ are isomorphic.

Corollary 4.5. Let G be circulant graphs with n vertices, if there exist at least two non-isomorphic strongly regular self-complementary graphs with the same number of vertices, then the smallest order n of G must satisfy $n\ge 21$.

In fact, as we above said, according to Ref [1], $n=4k+1$ must satisfy condition $n=x^2+y^2,x,y$ are integers. However, $21=x^2+y^2$, $x,y\in \mathbb{N}$ can not hold. Thus, we can deduce Corollary 4.5.

References

1. Ruiz, S.: On strongly regular self-complementary graphs. J. Graph Theory 5, 213–215 (1981)
2. Rosenberg, I.G.: Regular and strongly regular selfcomplementary graphs. Discrete Mathematics 12, 223–238 (1982)
3. Rao, S.B.: On regular and strongly-regular self-complementary graphs. Discrete Mathematics 54, 73–82 (1985)
4. Mathon, R.: On self-complementary strongly regular graphs. Discrete Mathematics 69, 263–281 (1988)
5. Nair, B.R., Vijayakumar, A.: Strongly edge triangle regular graphs and a conjecture of Kotzig. Discrete Mathematics 158, 201–209 (1996)
6. Kotzig, A.: Selected Open Problems in Graph Theory. In: Bondy, J.A., Murty, U.S.R. (eds.) Graph Theory and Releated Topics. Academic Press, New York (1979)
7. Cvetcovic, D.M., Doob, M., Sachs, H.: Spectra of Graphs: Theory and Applications, 3rd edn. Johann Ambrosius Barth Verlag, Heidelberg (1995)
8. Sachs, H.: Uber Selbstkomplementare Graphen. Publ. Math. Debrecen 9, 270–288 (1962)
9. Godsil, C., Royle, G.: Algebraic Graph Theory. Springer, New York (2001)

Transmissivity Simulation of Carbon Dioxide Using Narrow-Band K-Distribution with Different K-Discrete Schemes

XiJuan Zhu, Eriqitai, and Qiang Wang

School of Jet Propulsion, Beihang University, Beijing, 100191, China
zxj811129@163.com

Abstract. The narrow-band average transmissivity data of CO2 for the 2.0μm, 2.7μm and 4.3μm bands was calculated by narrow-band k-distribution based on the line-by-line (LBL) data. A uniform-discrete scheme and four discrete schemes of the absorption coefficients were employed to compute the k-distribution function, and the reference solutions are provided by LBL calculations. Finally, the comparisons of error for four proposed schemes were discussed. The results of the case show that all the proposed schemes can significantly improve the efficiency, they make the number of discrete k values decrease sharply with the same accuracy; The increase of scheme power make the effects more obviously in major bands but the opposite effects exist in some other bands. Thus, there may be a most proper scheme for the calculation. The comparisons of error indicate that the cubic scheme on account of its balance in the calculating band performs better than others.

Keywords: narrow band k-distributions, Line by Line calculation, gas radiation property, discrete schemes of the absorption coefficients.

1   Introduction

Accurate and compact gas radiation property models are highly desirable in many applications like fires and combustion systems. Gases differ from most solids, the absorptivity and the emissivity fluctuate sharply with frequency. In practice, CO_2 is one of the most important radiation gases for its high concentrations in high temperature regions. As is well-known, Line-by-line (LBL) approach is the most accurate method. However, the long calculation time and the large computer resource requirement make LBL approach impractical for engineering applications [1]. The statistic narrow band (SNB) model is often considered as the relatively more accurate non-grey gas radiation model in the absence of LBL results [2], However, it is difficult to be applied to nonhomogeneous gases and multi-dimensions problem and limited to scattering media [3].

The narrow-band k-distributions has the greatly improved efficiency and is as accurate as LBL in the spectral integration computation [4-6]. Obviously, the absorption coefficient distribution function is the most important part in narrow-band

k-distributions, which can be found by two ways: one is calculated by incorporating LBL data into the k-distribution function (LBL k-distributions) [1] and the other is calculated by the inverse Laplace transform of statistic narrow band transmissivity data (SNB k-distributions) [2-3].The former method is considered in the present study. Proper discretization of the absorption coefficient is the key to success with this method. The objective of this study is to find a more appropriate discrete scheme to obtain accurate results with fewer numbers of discrete k values. The transmissivities of CO_2 for 4.3μm bands were calculated which are taken from the previously work [7].

2   Mathematical Formulation

The narrow band average of transmissivity $\bar{\tau}_\eta$ can be rewritten in terms of a k-distribution function $f(k)$ as follows

$$\bar{\tau}_\eta(L) = \frac{1}{\Delta\eta} \int_{\Delta\eta} e^{-k_\eta L} d\eta = \int_0^\infty e^{-kL} f(k) dk \tag{1}$$

Fig.1 depicts the absorption coefficient data of CO_2 in 2325-2330cm-1 band. As shown in Fig.1, the absorption coefficient goes through a series of minima and maxima; between any two of these the integral maybe rewritten as

$$\int e^{-k_\eta L} d\eta = \int_{k_{\eta,min}}^{k_{\eta,max}} e^{-k_\eta X} \left|\frac{d\eta}{dk_\eta}\right| dk_\eta \tag{2}$$

The absolute value sign denotes that, where $d\eta/dk_\eta < 0$, the direction of integration has been changed. Therefore, integration over the entire range $\Delta\eta$ gives $f(k)$ as a weighted sum of the number of point where $k_\eta = k$.

$$f(k) = \frac{1}{\Delta\eta} \sum_i \left|\frac{d\eta_i}{dk_\eta}\right| \tag{3}$$

In actual reordering schemes values of k are grouped over small ranges $k_j \le k < k_j + \delta k_j$ as depicted in Fig.1, thus[4]

$$f(k_j) \approx \frac{1}{\Delta\eta} \sum_i \left|\frac{\delta\eta_i}{\delta k_j}\right| \left[H(k_j + \delta k_j - k_{\eta_i}) - H(k_j - k_\eta)\right] \tag{4}$$

Where $H(k)$ is Heaviside's unit step function

$$H(x) = \begin{cases} 0, & x < 0 \\ 1, & x > 0 \end{cases} \tag{5}$$

Here, the absorption coefficient is calculated by LBL with HITEMP database [8], and then the k distribution function can be easily computed from equation (4).
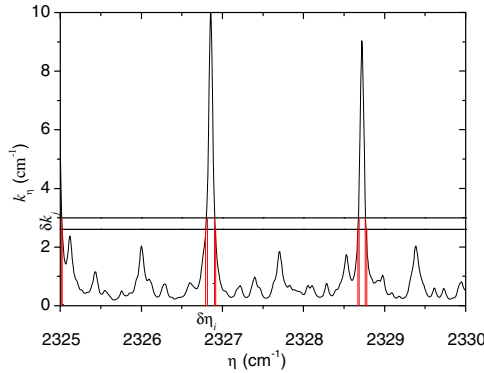
Fig. 1. Spectral absorption coefficient distributions across a small portion of CO_2 4.3μm band

Finally, to simplify the integration, the equation (1) can be rewritten as [4]

$$\bar{\tau}_\eta(L) = \int_0^1 e^{-k(g)L}dg \; ; \quad g(k) = \int_0^k f(k)dk \qquad (6)$$

Where $g(k)$ is the cumulative k distribution, $k(g)$ is the inverse function of $g(k)$.

As seen in Fig.1, if the absorption coefficient is uniformly divided to be used in equation (4), when the number of discrete k values (N) is small, in other words, δk is too large for the lower k values to capture the detailed information. On the other hand, when N is large, it would be rather wasteful for the larger k values. Therefore, an excellent scheme is the one that can make δk has the same variation characteristics of k. Here, the schemes are proposed to be used as follows.

$$\delta k_j = \frac{j^n}{\sum_1^N j^n} (k_{\eta,max} - k_{\eta,min}) \qquad (7)$$

n value of scheme1-4 is 1-4, respectively. Then 7-point Gauss-Labatto quadrature was used for calculating the narrow band transmissivities.

3   Results and Discussions

The narrow band transmissivities were calculated for the 4.3μm bands of CO_2, T=1000K, pressure ratio XCO_2=0.05 and path length L= 40cm. Fig.2 shows the LBL spectral absorption coefficients with a resolution of 0.01 cm^{-1}. This figure indicates the spectral k distribution data vary wildly across the band.

Fig.3 shows the narrow band average of transmissivity $\bar{\tau}_\eta$. Fig.3a compares the k-distributions results using the uniform-discrete scheme with the LBL ones. The k-distribution results were calculated for seven N values. As depicted in the figure, the k-distributions results show more and more agreement with LBL ones with the N increasing. Results are satisfactory when N=10000, however, when N is less than

1000, the accuracies of results are not acceptable, especially in the 2000-2180 cm-1 and 2400-2500 cm-1 bands in which the absorption coefficients are relatively low (as shown in Fig.2). Fig.3b-e show the comparisons of results calculated by LBL calculations and LBL k-distributions using the scheme-1, 2, 3 and 4, respectively. The accuracies of results in Fig.3b for N=50 are almost as same as those in Fig.3a for N=1000. Results in Fig.3c-e for N=50 are very close to LBL ones. To sum up, Fig.3 indicates that four proposed scheme can remarkably improve the efficiency, and the effects are more obviously in the 2000-2180 cm-1 and 2400-2500cm-1 bands with the scheme power increasing.
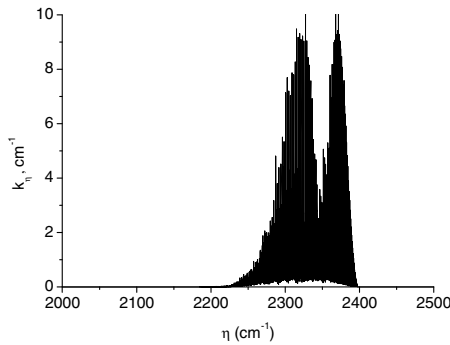
Fig. 2. LBL spectral absorption coefficients with a resolution of 0.01 cm-1

Fig.4 presents the absolute values of the transmissivity result absolute errors of the four proposed schemes, and the error can be expressed by the formula

$$\varepsilon_{abs} = |\tau_{LBL} - \tau_k| \tag{8}$$

Fig.4a shows ε_{abs} comparisons of four proposed schemes for N=20. As depicted in this figure, ε_{abs} values of scheme-1, 2, 3 and 4 are less and less in the 2000-2180 cm-1 and 2400-2500cm-1 bands, interestingly, the trend is contrary to the previous one in the 2180-2250 cm-1 band. ε_{abs} comparisons of the proposed schemes for N=50 are shown in Fig.4b. It is apparent that the errors for N=50 are much lower than N=20, and the trend is similar with N=20. Fig.4b presents that the errors of scheme-2, 3 and 4 are very low across entire band in which the maximum is less than 0.05; ε_{abs} results of scheme-3 are lower than in the 2180-2250 cm-1 and 2370-2400 cm-1 bands and are nearly as accurate as scheme-4 in the other bands. In a word, Fig.4 shows that the increase of scheme power can raise accuracy in most bands, whereas the opposite conclusion can be drawn in some other bands. Moreover, there is another trouble for the higher power scheme that Overflow will occur while calculating denominator of δk when N is not very large. Thus, if the power of scheme continuously increases, it would be extremely hard for practical applications. That is to say, there may be a most proper scheme for the calculation. Finally, by above comparisons, Scheme-3 is suggested as the most proper one.
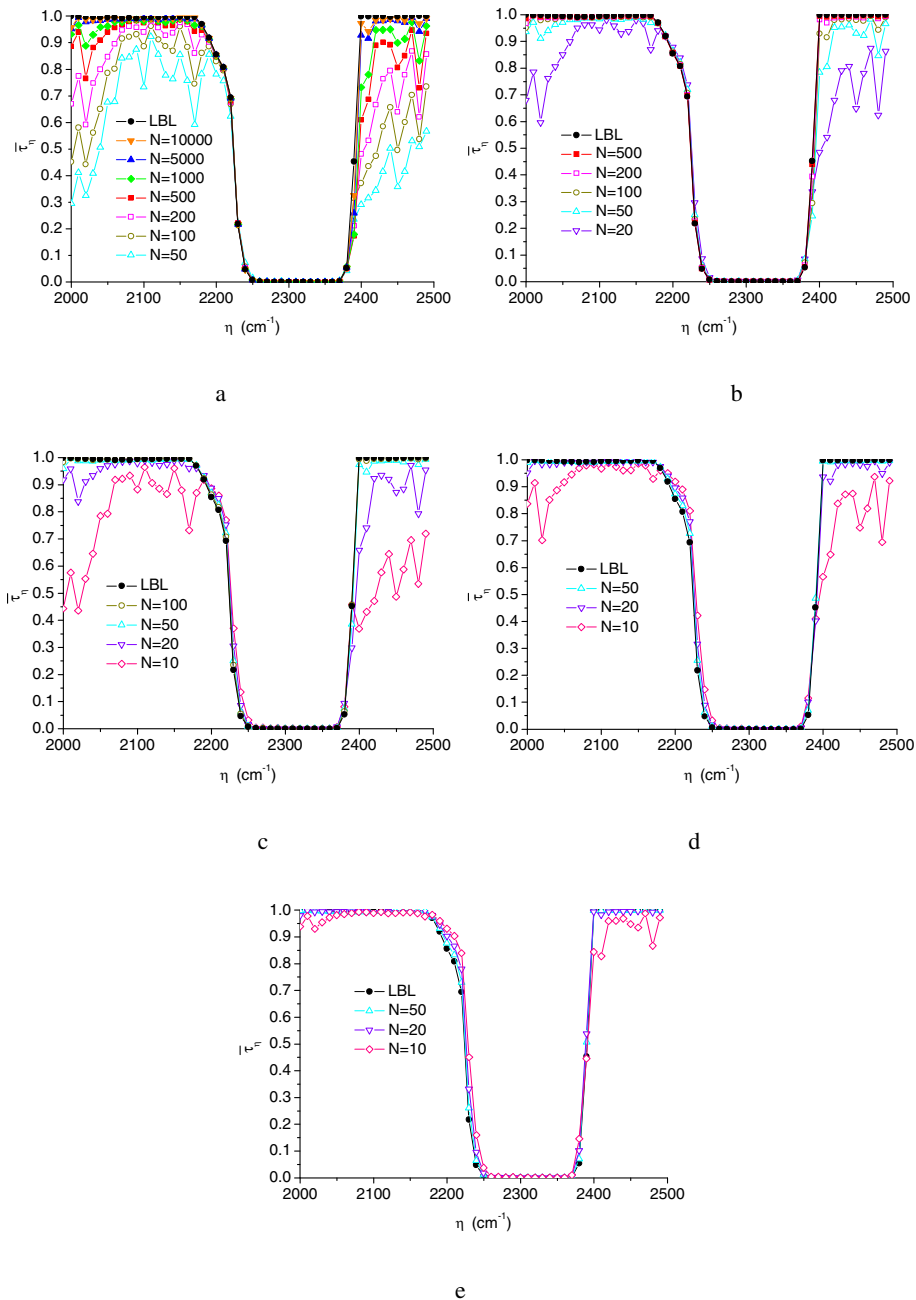
Fig. 3. Narrow band average transmissivity data using LBL calculations and LBL k-distributions based on different k discrete schemes; (a) uniform-discrete scheme, (b) scheme-1,(c) scheme-2,(d) scheme-3,(e) scheme-4

4   Conclusions

Proper discretization of the absorption coefficient is the key to success with LBL k-distributions. The number of discrete k values deeply affects the calculation efficiency. The case for CO_2 indicates that all proposed schemes can greatly improve the efficiency. The increase of scheme power for same N value can raise accuracy in most bands, whereas the opposite conclusion can be drawn in some other bands, thus, there may be a most proper scheme for the calculation. Through the comparisons of the four proposed schemes, the cubic scheme due to its balance in the calculating band performs better than others.

References

1. Wang, A., Modest, M.F.: High-accuracy, compact database of narrow-band k-distributions for water vapor and carbon dioxide. JQSRT 93, 245–261 (2005)
2. Liu, F., Smallwood, G.J., Gülder, Ö.L.: Application of the statistical narrow-band correlated-k method to low-resolution spectral intensity and radiative heat transfer calculations–effects of the quadrature scheme. International Journal of Heat and Mass Transfer 43, 3119–3135 (2000)
3. Liu, F.: Three-dimensional non-grey gas radiative transfer analyses using the statistical narrow-band model. Revue Générale de Thermique 37(9), 759–768 (1998)
4. Modest, M.F.: Radiative heat transfer, 2nd edn. Academic Press, New York (2003)
5. Goody, R. M., Yung, Y.L.: Atmospheric radiation–theoretical basis, 2nd edn. Oxford University Press, New York (1989)
6. Tang, K.C., Brewster, M.Q.: K-distribution analysis of gas radiation with nongray, Emitting, Absorbing, and Anisotropic Scattering particles. Journal of heat transfer 116(4), 980–985 (1994)
7. Bharadwaj, S.P., Modest, M.F.: Medium resolution transmission measurements of CO2 at high temperature–an update. JQSRT 103, 146–155 (2007)
8. Rothman, L.S., Camy-Peyret, C., Flaud, J.-M., Gamache, R.R., Goldman, A., Goorvitch, D., Hawkins, R.L., Schroeder, J., Selby, J.E.A., Wattson, R.B.: HITEMP, the high- temperature molecular spectroscopic database (2000), `http://www.hitran.com`

The Research of Temperature Fields during Hot Rolling for the Strip

Junwei Cheng, Xianzhang Feng, Liangji Chen, and Zhiqiang Jiang

School of Mechatronics Engineering, Zhengzhou Institute of Aeronautical Industry Management, Zhengzhou, Henan, China, 450015
Phdfxz@163.com

Abstract. The hot rolling strip plays an important role in the domestic economy, and its products are widely used in industry, agriculture, national defenses and civil areas, etc. It can not only be directly used as slab and sheet, but also as raw and processed materials of cold rolling, welding tube, and cold banding beam. The rough rolling process was analyzing using the means of FE technology, with consider of the deformation behavior of metal, studying the effect of environmental temperature, rolling piece initial temperature, and rollers surface temperature on the temperature fields distribution of the rolling piece. The results have important significance to improvement of mechanical properties of hot rolling strip and the quality of production.

Keywords: hot rolling strip, temperature field, rolling piece, plastic deformation, FE model.

1 Introduction

The hot rolling strip can be directly used as plate, sheet and various kinds of section steel, also can be as raw materials for welding bending special-section profile, welded tube, and cold stripe rolling. The hot rolling steel is developing very fast in china in recently year, and application of new technique to tandem mills of the hot rolling strip industry. So, to a certain degree, the level of production can reflects the level of a country's iron and steel industry. [1-5]

It's about a century years of product of hot rolling strip, an can divide in to three stages: the first tandem mills, the rolling speed is below 12m/s, the slab unit weight is small, the annual output is between the 80 to 180 tons, its the level of product is still low compared with the advanced technology before the 50 years of the 20th century. The second stage: the rolling maximum speed is up to 21.5m/s, in which has the process computer system, the product of tandem mills is higher in Japan an USA, slab unit weight is up to 40 tons, the annual output is between the 100 to 350 tons in the 60 years of the 20th century. The third stage: The generation of hot strip mill will be looking for large-scale, high-speed, continuous and automated from 60 time end of the 20th century. [6-9]

2   Finite Element Theory and Its Application in Engineering

Finite element method is the discrete method, in which is consist of finite element by continuous deformation of the solid dispersion, there is joined by a hinge in the nodal places among the elements. It can build the algebraic equations of contact node displacement and load nodes by variation principle or other methods. It can solution the unknown nodal displacement, eventually obtained all of the other physical through these equations. In general, the finite element problem-solving process can be divided into the following six steps: [10-15]

A: Discretization of the continuity of the structure: the continuity of the structure can be divided into lots, in which constitute a connected among the elements, the new element aggregation replace the original continuous deformation body to complete analysis of the process of deformation. It can be obtained each unit of physical quantity, after the solved the parameters of each element node. Finally the solutions of whole continuum body are realized.

B: Selection the mode of displacement: In order to obtain the mechanical properties of a typical unit after the continuum discretization. It is important assumption of the displacement distribution for displacement, strain and stress of the element unit the can be represented by the nodal displacement or speed.

C: The stiffness matrix: It can build the displacements relation between the nodes, in which act on the element nodes on the force by the principle of virtual work.

D: Calculate equivalent nodal force.

E: Assembly of element stiffness matrix to the global stiffness matrix.

F: Calculated nodal forces: The linear finite element method is a new numerical method based on the linear elastic finite element technology, it is similar the solving process with the elastic problem. [16-19]

3   The Rolling Process of Strip

Pressure processing is the large deformation elastic-plastic process of the metal deformation for rolling, forging, stamping, etc, also is nonlinear problems. There is existence the geometrical and material nonlinearity at the same time, and are also non-linear boundary conditions. In generally, for the complex problem, it can use the method of experimental study and numerical simulation to combining plastic deformation of metals.

Virtual work equation is a deformation of the weak form of equilibrium, every moment it must satisfy the equilibrium relationship, that satisfy the principle of virtual work during deforming for the deformation body. For the coordinates of the initial state is the base for the $g_i (i = 1,2,3)$ using a rectangular cartesian coordinate system. Set coordinate a_i, set coordinate-based G_i for the change shape, set coordinate x_i, And make u_i to represent the displacement components. The rate of change expressed by the equation of virtual work will be obtained.

$$\int_V \sigma_i \delta \dot{e}_{ij} dV = \int_{S_0} p \delta u_i dS + \int_V F_i \delta v_i dV \tag{1}$$

Where σ_{ij} is the Euler stress tensor components, δv_i is the virtual objects within the particle velocity component, $\delta \ddot{e}_{ij}$ is virtual strain rate, e_{ij} is Almansi strain tensor, V is the volume of deformable objects, p_i is the surface force on the part of the surface of objects, F_i is body force per unit volume, S_0 is p_i to act on the reference configuration of the surface area.

For two objects a and b consisting of contact problems and for analytical convenience, it separates them into two separate objects. Then their respective basic equation of the finite element is as follows:

$$\begin{cases} [K_a][u_a] = \{R_a\} + \{P_a\} \\ [K_b][u_b] = \{R_b\} + \{P_b\} \end{cases} \tag{2}$$

Where $[K_a]$ is stiffness matrix of object a, $[K_b]$ is stiffness matrix of object b, $\{u_a\}$ is node displacement vector of object a, $\{u_b\}$ is node displacement vector of object b, $\{R_a\}$ is contact force vector of object a, $\{R_b\}$ is contact force vector of object b, $\{P_a\}$ is external force vector of object a, $\{P_b\}$ is external force vector of object b.

In the large deformation elastic-plastic finite element, the establishment of virtual work equation is not the only way, but no matter how the form of virtual work equation, which itself reflects the strain energy density must be objective. However, as reflected by its own strain energy density must be objective.

For the long time, for the restrictions on the production process, it can only obtain the workpiece surface temperature measurement, but not get the internal temperature. For the many affecting factors, such as surface iron oxide, thermal deformation during rolling, applied high pressure water revamping before each rolling pass, in order to remove the rolling surface of the iron oxide processing of rolling process. But the surface temperature is actually not representative of the true temperature rolling, in the hot rolling process, it is often accompanied by temperature changes in the same time, in order to accurately analyze the process of metal deformation problem, it must consider the impact of temperature on the deformation. In addition to the affect of temperature variation on the rolling deformation and material properties, and in the same time, the rolling deformation will in turn change the thermal boundary conditions, thereby affecting the temperature change. It is the strong correlation mutual coupling between the temperature field and displacement field. In general, and so deformation on the reaction temperature in the following areas:

   A: Effect of geometric parameters
   B: Plastic work heat

Taking temperature 1200°C for rolling piece model, the length 1000 mm, thickness 250mm. To reduce the computation time, according to symmetry, taking the establishment of a model, ignore the temperature difference along the horizontal rolling, building the two-dimensional finite element model to analyze, the geometric model created as shown in Figure 1.
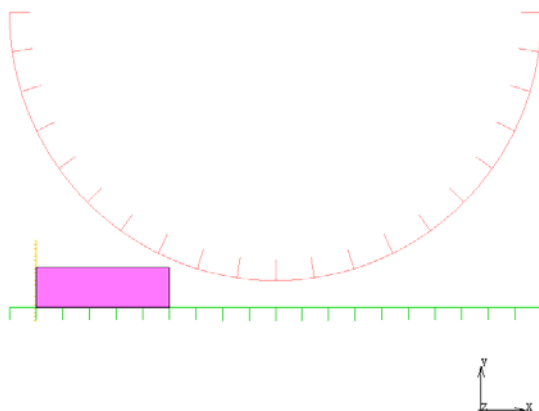
Fig. 1. The FE model of hot rolling strip

Because of the little elastic for the rollers during rolling strip, the rollers can be considered rigid body, but the rolling piece can be considered elastic-plastic. In order to realize the process of bite, the piece is pushed by a rigid body along the rolling direction, but its speed is smaller than the rollers, they can immediately separate after biting for the rolling piece. The assuming is not the influencing in rolling process for strip.

The temperature boundary conditions of the model as shown in Figure 2.
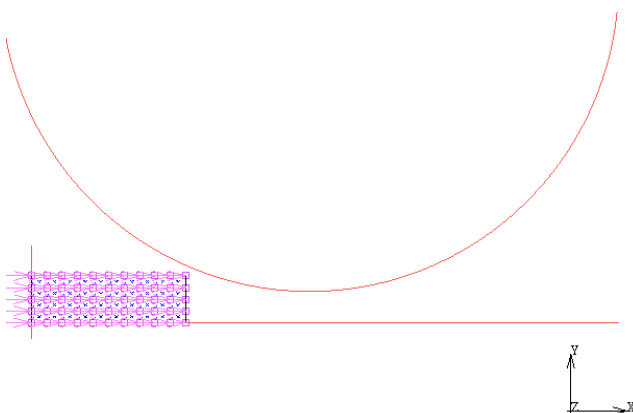
Fig. 2. The temperature boundary condition for the FE model

Form the Figure 2, the study object is belong to the plane-strain problems.

As the rolling temperature changed greatly in the hot rolling process, so these parameters that include the thermal expansion coefficient, specific heat, thermal conductivity, physical parameters of materials such as deformation resistance variation with temperature change dramatically.

The initial conditions of hot rolling strip as shown in the Table 1.

Table 1. The initial conditions of hot rolling strip

Item	Symbol	Value	Unit
Environmental temperature	T_v	25	℃
Rolling piece initial temperature	T_W	1200	℃
Rollers surface temperature	T_t	100	℃

The parameters of hot rolling sheet as shown in the Table 2

Table 2. The parameters of hot rolling sheet

Reference place/mm	Velocity m/s	Roller diameter /mm
230	2	1550

To simulate the temperature distribution contours in the process of rolling, it's the contour line as shown in Figure 3.
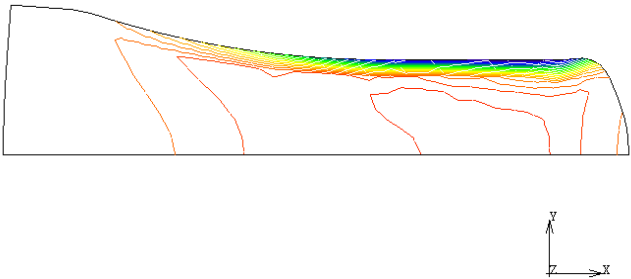
Fig. 3. Contour line of the temperatures

Form the Figure 3 shows, as plastic work heat in the process of plastic deformation, it can cause temperature rising internal nodes in the model, otherwise temperature dropping in the surface of rolling pieces.

In order to more clearly describe the changes, at a time, along the length of the rolling pieces, the curve of the temperature distribution in the surface at a time as shown in Figure 4.
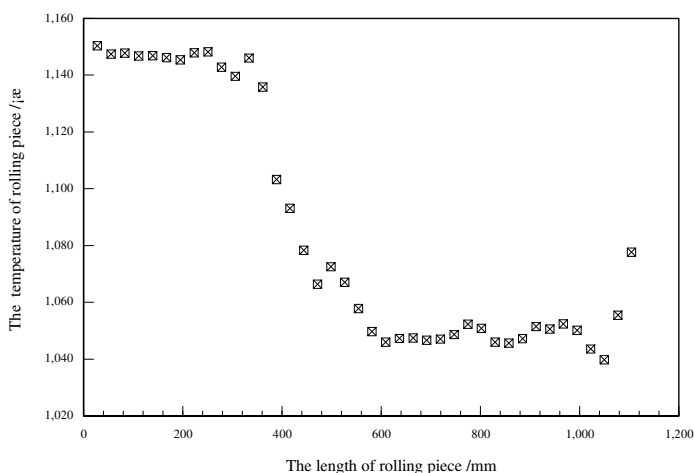
Fig. 4. Temperature distribution in the surface at a time

Form the Figure 4 shows, There is two distinct stages of temperature reduction for the surface node, the temperature reduction is very significantly in the first stage, the reason is the high-pressure water to spray the rollers surface, in the same time, the temperature reduction is very obvious in the second stage, the reason is small change of temperature of the rollers in the contact area.

Get a node of rolling piece surface as a reference point, the temperature curve during the rolling shown in Figure 5
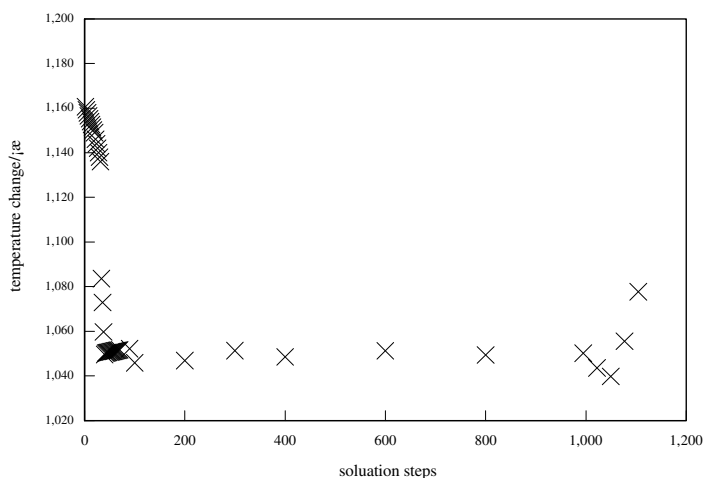
Fig. 5. Temperature change of the node with the time

Form the Figure 5 shows, only slightly change of the temperature in the course of the stage of air phase, but larger the magnitude of temperature decrease in high-pressure water and contact area for all nodes. And lower the temperature change happened to the two stages for nodes. After rolling piece and rollers have separated, temperature curve began to rise, the temperature starts to rise.

4   Conclusion

The coupled thermal model was established by the finite element technique for hot-rolled strip. Considering the factors of the ambient temperature, cooling water, etc. It can get the rules of the temperature variation of surface nodes and internal nodes in the rolling piece in the course of hot rolling, by means of the analyzing the strip temperature distribution in process of the hot rolling. The studing results that it is important significance to improvement of mechanical properties of hot rolling strip and the quality of production.

References

1. Meyer, C.J., Kroger, D.G.: Air-cooled heat exchanger inlet flow losses. Applied Thermal Engineering 21(7), 771–786 (2001)
2. Munsi, A.S.M.Y., Waddell, A.J., Walker, C.A.: Vibratory stress relief-an investigation of the torsional stress effect in welded shafts. Journal of Strain Analysis 36(5) (2001)
3. Meyer, C.J., Kroger, D.G.: Numerical investigation of the effect of fan performance on forced draught air-cooled heat exchanger plenum chamber aerodynamic behavior. Applied Thermal Engineering 24(2-3), 359–371 (2004)
4. Chaohong, L., Kuo, H.: Study on mosaic-type solid lubricating materials for friction lining board in slab-strip steel coilers. Heavy Machinery 3, 3–4 (2007)
5. Kawasaki, H., Major, D.J.: Estimation of Friction Levels between Tire and road. SAE Paper 2002-01-1198
6. Yong, L., Jianrong, Z., Weifeng, T.: Analysis of Damping Material and Structure for Viscoelastic Suspensions Using Nonlinear FEM. Transactions of the Chinese Society of Agricultural Engineering 1, 1–3 (2005)
7. Shyu, S.C., Chang, T.Y.P., Saleeb, A.F.: Friction Contact Analysis Using a Mixed Finite Element Method. Computer&Structures 32(1), 223–242 (1989)
8. Lijun, Y., Xiaoze, D., Yongping, Y., Lining, W.: Operation Performance Analysis of Axial Flow Fan Cluster in Direct Air-cooled System. Proceedings of the CSEE 29(20), 1–5 (2009)
9. Tianmin, G., Dongsheng, Z., Lei, L.: Method of force bearing analysis and finite element analysis on contacting state of tooth surface for new typed FA planetary transmission of cycloidal needle-wheel. Journal of Machine Design 3, 8–10 (2005)

10. Hac, A., Simpson, M.D.: Estimation of Vehicle Side Slip Angle and Yaw Rate. SAE Paper 2000-01-0696
11. Litvin, F.L., Lian, Q.M.: Asymmetric modified gear drives:Reduction of noise, localization of contact, simulation of meshing and stress analysis. Comput. Methods Appl. Mech. Engrg 188, 363–390 (2000)
12. Bredell, J.R., Kroger, D.G., Thiart, G.D.: Numerical investigation of fan performance in a forced draft air-cooled steam condenser. Applied Thermal Engineering 26(8-9), 846–852 (2006)
13. Zihua, P.A.N.: Comprehensive technical measures for prolonging the life of the hot press roll forging die. Forging & Stamping Technology 31(6), 85–86 (2006)
14. Xiaolin, W.: The status of dry cooling technology of thermal power plants in China. International Electric Power for China 9(1), 15–18 (2005)
15. Vishal, S., Suresh, V.G.: A novel valveless micropump with electro-hydrodynamic enhancement for high heat flux cooling. IEEE Trans. (2005)
16. Feng, X., Liu, C., Jiang, G., et al.: Dynamics Analyse for SP Rolling Mill's Side Framing of Baosteel. Heavy Machinery 254(2), 34–37 (2004)
17. Seong, H.K., Chul, H.P., Hyun, C.P., et al.: Vibration control of an arc type shell using active constrained layer damping. Smart Materials and Structures 13(2), 350–354 (2004)
18. Pattinson, E., Dugdale, D.S.: A literature survey on the stability and significance of residual stresses during fatigue. Fatigue & Fracture of Engineering Materials and Structures 30, 173 (2007)
19. Yajun, L., Zhuoru, Y., Zhenping, W., Yong, T., Wei, W.: Ploughing-extrusion Machining Mechanism of the Integral-fin of Stainless Steel Surface. Journal of South China University of Technology (Natural Science Edition) 32(4), 61–65 (2004)

Using Bees Algorithm to Solve the Resource Constrained Project Scheduling Problem in PSPLIB

Amir Sadeghi[1,*], Abolfazl Kalanaki[2], Azadeh Noktehdan[3],
Azamdokht Safi Samghabadi[1,**], and Farnaz Barzinpour [4,***]

[1] Dept. of Industrial Engineering, Tehran Payame Noor University, Tehran, Iran
[2] Faculty of Management, University Of Tehran, Tehran, Iran
[3] Dept. of Industrial Engineering, Amirkabir University of Technology, Tehran, Iran
[4] Dept. of Industrial Engineering, Iran University of Science and Technology, Tehran, Iran
Amir_Sadeghi_IE@yahoo.com

Abstract. Today, trade globalization caused optimum use of resources to become a vital factor for surviving in the global arena. The same need led to the introduction of concepts such as project, project control and resource constrained project scheduling. In the field of operations research and project management, project scheduling with resource constraints is of great importance. Most of the contributions made to this field can be attributed to two main factors. First, based on different conditions for objective function, characteristics of activities, resources and priority rules, the form of the problem tends to vary too much. Second, this kind of problem is of Np-Hard nature for which researchers are always trying to find new solutions. In this paper, Bees Algorithm is proposed as an approach to solve this kind of problem. Results obtained from deploying this algorithm are compared to those of other algorithms, and it is shown that Bees algorithm is a suitable one to solve RCPSP.

Keywords: Bees Algorithm, Project Scheduling, Resource Constraint, RCPSP.

1 Introduction

As an Np-Hard problem, project scheduling with resource constraints is an important area of interest for researchers in the field of operations research and project management [1].

In such problems, every project includes a number of activities. And related to these are a number of resources, each defined to have a limited capacity to serve in every period of time. Depending on the Decision Maker's goals, a variety of objectives could be set, while "finding minimum makespan" is the most common.

Exact methods available for solving this problem mainly consist of a large number of variables and constraints. Therefore their efficiency dramatically decreases as the dimensions of practical problems increases. Two groups of methods for solving this

---

* Corresponding author.
** Assistant Professor .Ph.D, Payame Noor University, Iran.
*** Assistant Professor .Ph.D, University of Science and Technology, Iran.

problem can be identified: 1) methods in which activities are organized based on some priority rules, and then selected each time. The main weakness of these methods is their lack of demonstrating a general rule for organizing activities. However, desirability of solution is related to network of project activities. In other words, if there exists an optimal solution for a given rule in a specific problem, then its success may not last forever. 2)Metaheuristic methods that start from several solutions.

Many heuristic or priority-rule based approaches have been proposed for this problem [2, 3].In multi-priority rule methods a different priority rule is used at each iteration [4.5]. Sampling methods are used by Drexl [5], Schirmer [6]. Genetic algorithms have been applied in Leon and Rama- moorthy [7], Hartmann [8], Alcaraz and Maroto [9], Valls et al. [10].Bouleimen and Lecocq [11] have applied simulated annealing. Tabu search based metaheuristics are proposed by Pinson et al. [12], Nonobe and Ibaraki [13] proposed an ant-colony approach to the RCPSP. Colak et al. [14] proposed a neural-network based technique. For instance, we can point to Stoylar and Kotchetov [15] which a tabu search with variable neighborhood is formed to solve this problem Lecocq and Bouleiem [16] used simulated annealing algorithm and Debleses et al [17] used scatter search. Genetic algorithm is also used by Alcaraz et al and Hartmann [8, 18].

In this paper we propose Bees algorithm (BA) to tackle the RCPSP with makespan minimization as the objective function. When applied to other combinatorial problems, BA has shown inspiring results so far, [19] and since RCPSP is an important problem, we employ the idea of this algorithm and incorporate it in a metaheuristic framework and then applying it to such problems. The main prospected contribution of our work is proposing a new algorithm with [new] operators integrated into it which lead us to develop an appropriate metaheuristic algorithm to solve RCPSP.The rest of this paper is organized as follows: The Bees algorithm is described in Section 2. The RCPSP is explained in Section 3 and the proposed algorithm is described in Section 4. Computational experiments are presented in Section 5. Section 6 includes the overall conclusions.

2   Bees Algorithm

Bees are social insects that are capable of solving complex problems. The best evidence for this argument is the process of producing nectar which is an advanced organized process. Rather than finding a new flower, every bee prefers to follow the path in which a pervious bee associated to the same hive has already traveled [20].

Lucic and Teodorovic [21] were the first persons to use simple and basic method for solving combination problems. They introduce bees system (BS) and use it for known issue of Traveling Salesman Problem (TSP).

The Bees Algorithm is based on algorithm of quest that was developed in 2005 [19]. This algorithm is an optimization algorithm inspired by the natural foraging behavior of honey bees to find the optimal solution. In early version of this algorithm, it did a kind of local search that was combined with random search and so it could be used for combined optimization where we want to optimize several variables or perform functional optimization. In order to exploit food resources, a colony of bees

can spread in different directions. Floral parts with plenty of nectar and pollen may be selected. It is visited by plenty of bees. The less the nectar of a land part, the fewer the number of bees attracted to it will be.

The foraging process begins in a colony by scout bees being sent to search for promising flower patches. Scout bees move randomly from one patch to another. During the harvesting season, a colony continues its exploration, keeping a percentage of the population as scout bees. When they return to the hive, those scout bees that found a patch which is rated above a certain quality threshold deposit their nectar or pollen and go to the "dance floor" to perform a dance known as the "waggle dance". This mysterious dance is essential for colony communication, and contains three pieces of information regarding a flower patch: the direction in which it will be found, its distance from the hive and its quality rating. This information helps the colony to send its bees to flower patches precisely, without using guides or maps. Each individual's knowledge of the outside environment is gleaned solely from the waggle dance. After waggle dancing on the dance floor, the dancer goes back to the flower patch with follower bees that were waiting inside the hive. More follower bees are sent to more promising patches. This allows the colony to gather food quickly and efficiently. While harvesting from a patch, the bees monitor its food level. This is necessary to decide upon the next waggle dance when they return to the hive. If the patch is still good enough as a food source, then it will be advertised in the waggle dance and more bees will be recruited to that source [19].The algorithm requires a number of parameters to be set, namely:

m = number of sites selected out of n visited sites	n = number of scout bees
e = number of best sites out of m selected sites	nsp = selected sites
nep = number of bees recruited for best e sites	ngh = initial size of patches
m-e = number of bees recruited for the other	

In step 1, the algorithm starts with n scout bees randomly distributed in the search space. The fitness of the sites visited by the scout bees are evaluated in step 2.

The algorithm includes site and its neighborhood and stopping criterion. The algorithm starts with the n scout bees being placed randomly in the search space. The fitnesses of the sites visited by the scout bees are evaluated in step 2.

In step 4, bees that have the highest fitnesses are chosen as "selected bees" and sites visited by them are chosen for neighborhood search. Then, in steps 5 and 6, the algorithm conducts searches in the neighborhood of the selected sites, assigning more bees to search near to the best e sites. Alternatively, the fitness values are used to determine the probability of the bees being selected. Searches in the neighborhood of the best e sites which represent more promising solutions are made more detailed by recruiting more bees to follow them than the other selected bees. Together with scouting, this differential recruitment is a key operation of the Bees Algorithm. However, in step 6, for each patch only the bee with the highest fitness will be selected to form the next bee population. In nature, there is no such a restriction. This restriction is introduced here to reduce the number of points to be explored. In step 7, the remaining bees in the population are assigned randomly around the search space

scouting for new potential solutions. These steps are repeated until a stopping criterion is met. At the end of each iteration, the colony will have two parts to its new population - representatives from each selected patch and other scout bees assigned to conduct random searches [19].

3   The Resource Constrained Project Scheduling (RCPSP)

Suppose that a project is defined based on AON network as G (V, E) where V is a collection of whole nodes that represent activities. E is the arc set that specifies priority rule as FS (finish to start).

   N is the number of activities in the project, I = (1,…,N) is the collection of all activities, and Π is the collection of all defined permutations on I. Every permutation of $\pi \, \varepsilon \, \Pi$ is defined as an array of N vectors; $\pi(1), \pi(2), ..., \pi(N)$. The **1st** and **Nth** activities are dummy start and end activities of the project with zero duration. The activities should be non preemptive in basic model of RCPSP. Duration, time of start and time of end of each activity are denoted by d_i (1<i<N), S_i, and F_i, respectively. We need to assume renewable resources in the same number of K. (1<i<N, 1<k<K). R_{ik} is constant rate by which activity **i** requires resource **K**. a_k is constant availability rate for resource **K**. RCPSP can be stated as follows:

$$Min \ f_n \qquad\qquad (1)$$

$$st: \qquad f_1 = 0 \qquad\qquad (2)$$

$$f_j - d_j \geq f_i \, , \forall \, (i, j) \in H \qquad\qquad (3)$$

$$\sum_{i \in s_i} r_{ik} \leq a_k \ , \ t = 1, 2, ..., f_n ; \ k = 1, 2, ..., K \qquad (4)$$

H is the collection of paired activities that conform to priority rule. S_t is the collection of activities that are placed in the range of [t-1, t],so that $s_t = \{f_i - d_i \prec t\}$. Permutation Π is called a "feasibility scheme", if all the activities in it conform to the priority rule of the project, i.e. activities can only be accomplished as determined in the specified order. Hence, every permutation cannot newcessarily be a possible sequence. Suppose F is collection of all possible permutations on Π. In this state can determined the project based on determined possible order and observance of scheduled resources limitation and total project time (Cmax).

4   Suggested Bees Algorithm for Solving RCPSP

Stage 1: First, Scout bees are randomly placed in the solution space, and produce an early solution, that in fact is a list of activities with observance limitations. Numbers of Scout Bees are shown in the table below.

Table 1. Numbers of Scout Bees for PSPLIB

Problem	Number of Scout Bees
J30	15
J60	20
J120	20

Stage 2: Bees start to dance considering produced solution that is stated in terms of project end time. Dance rate for each bee is determined by considering the following relations. It is clear that if the ratio of the quality of the solution found by one scout bee to whole solutions found by other bees is equal to 1.15, then that bee will return to hive with probability of 10%, and new bees will mobilize to search in the neighborhood of that solution to obtain better solutions. Time of dancing is denoted by d_i :

$$Pf_{colony} = \frac{1}{n}\sum_{j=1}^{n}\frac{1}{C_{max}^i} \quad , \quad Pf_i = \frac{1}{C_{max}^i} \quad \rightarrow \quad d_i = \frac{Pf_i}{Pf_{colony}} \qquad (5)$$

Table 2. Probability of returning to hive and dancing scout bees

Rate	r_i
$Pf_i \leq 0.9\,Pf_{colony}$	0.6
$0.9\,Pf_{colony} \leq Pf_i \leq 0.95\,Pf_{colony}$	0.2
$0.95\,Pf_{colony} \leq Pf_i \leq 1.15\,Pf_{colony}$	0.02
$Pf_i \geq 1.15\,Pf_{colony}$	0.00

Stage 3: The number of bees that would be selected to research the neighborhood is related to the quality of answer, namely it is related to the dancing rate of

Scout bees that are calculated by the following formula: $n_{dance}^i = [d_i.nDance\,0]$

nDance() is constant factor, d_i is time of dancing of its scout bees that is calculated above and n_{dance}^i is number of new bees that are specialized for searching neighborhood.

Stage 4: The obtained solution is compared to that of the scout bee. If their answer is better, those new bees will be placed and become scout bees.

Stage 5: Repeat Stage 4, until the stop criterion is satisfied.

5   Computational Results

This section, results obtained from solving basic RCPSP will be surveyed by examining ratio of results of Bees Algorithm to those of others. A library of project scheduling problems (PSPLIB), available on the Internet, is used to provide a basis

for comparison. In this library, there are some problems with 30, 60, 90 and 120 activities. Number of problems used in j30, j60 and j90 is 480 while in j120 some 600 problems are used. To code the model, we used MATLAB Ver. 2010 and a computer with Windows XP operating system running on a 2.1GHz CPU.

The problems were repeated 1000, 5000 and 50000 times. Results are shown in terms of percent of deviation from mean. Other algorithms that were used to solve the problems are shown in following tables. The results are shown in the following table:

Table 3. Comparison with well-reported algorithms (J30)

Algorithm	Reference	Iteration		
		1000	5000	50000
Bees algorithm	**This paper**	**0.15**	**0.09**	**0**
GA, TS-path relinking	[15]	0.10	0.04	0
GAPS	[22]	0.06	0.02	0.01
ACOSS	[23]	0.14	0.06	0.01
ANGEL	[24]	0.22	0.09	-
Scatter search- FBI	[25]	0.27	0.11	0.01
GA-DBH	[26]	0.15	0.04	0.02
GA-hybrid FBI	[27]	0.27	0.06	0.02
GA-FBI	[28]	0.34	0.20	0.02
Sampling-LFT,FBI	[29]	0.25	0.13	0.05
TS-activity list	[30]	0.46	0.16	0.05

Table 4. Comparison with well-reported algorithms (J60)

Algorithm	Reference	Iteration		
		1000	5000	50000
GAPS	[22]	11.72	11.04	10.67
ACOSS	[23]	11.75	10.98	10.67
GA-DBH	[26]	11.45	10.95	10.68
Scatter search-FBI	[25]	11.73	11.10	10.71
GA-hybrid FBI	[27]	11.56	11.10	10.73
Bees algorithm	**This Paper**	**11.93**	**11.48**	**10.74**
GA,TS-path relinking	[15]	11.71	11.17	10.74
ANGEL	[24]	11.94	11.27	-
GA-FBI	[28]	12.21	11.27	10.74
Sampling-LFT,FBI	[29]	11.88	11.62	11.36
GA-activity list	[31]	12.68	11.89	11.23

The methods are sorted with respect to the results for 50,000 schedules for problems in J30 that optimal solutions are obtained, low values for comparison of algorithms are considered as the reason of optimal solutions. For j60, j90 and j120 solutions obtained are studied through the critical path (CPM), because, as mentioned above, since optimal solutions cannot be obtained for these problems, the best criteria would be the critical path. For J30 problem set, optimal solutions are found and Bees algorithm, with

generation of 50000 solutions as the stopping criterion, provides the optimal solutions for one hundred percent of 480 instances in the set. As in the above table, for problem J30 the deviation from the optimal solution for 1000, 5000 and 50000 iterations equals to 0.15%, 0.10% and 0% respectively, that is considered a satisfactory result.

For J60 and J120 sets, critical-path based lower bound is employed. For J60 and J120 problem sets, having 50,000 generated solutions as the stopping criterion. For j60 and j120 problem sets, the results are shown in tables 3 and 4.

The above table shows that deviation from mean of solution in 1000, 5000 and 50000 iterations equals to 11.93%, 11.48% and 10.74 % respectively.

Table 5. Comparison with well reported algorithms (J120)

Algorithm	Reference	Iteration		
		1000	5000	50000
ACOSS	[23]	35.19	32.48	30.56
GA-DBH	[26]	34.19	32.34	30.82
GA-hybrid FBI	[27]	34.07	32.54	31.24
GAPS	[22]	35.87	33.03	31.44
Bees algorithm	**This Paper**	**35.80**	**33.33**	**31.55**
Scatter search-FBI	[25]	35.22	33.10	31.57
GA-FBI	[28]	35.39	33.24	31.58
GA, TS-path relinking	[15]	34.74	33.36	32.06
ANGEL	[24]	36.69	34.49	-
Sampling-LFT,FBI	[29]	35.01	34.41	33.71

6   Conclusions

In this study, Bees algorithm is developed to solve project scheduling problems with resource constraints. This algorithm is used for solving problems in Project Scheduling Problem Library (PSPLIB). Results show that this algorithm is successful. In next studies, this algorithm can be used for solving other problems of RCPSP such as MRCPSP, RCPSP/max,…

The multiple projects scheduling with resource limitation and different multi modes can be pointed out as another field to deploy our algorithm.

References

1. Blazewicz, J., Lenstra, J.K., Kan, A.H.G.R.: Scheduling subject to resource constraints– classification and complexity. Discret. Appl. Math. 5, 11–24 (1983)
2. Davis, E.W., Patterson, J.H.: A comparison of heuristic and optimum solutions in resource-constrained project scheduling. Management Science 21(81), 944–955 (1975)

3. Alvares-Valdes, R., Tamarit, J. M.: Heuristic algorithms for resource-constrained project scheduling: a review and an empirical analysis. In: Slowinski, R., Weglarz, J. (eds.) Advances in Project Scheduling, pp. 113–134. Elsevier, Amsterdam (1989)

4. Boctor, F.F.: Some efficient multi-heuristic procedures for resource-constrained project scheduling. European Journal of Operational Research 49, 3–13 (1990)

5. Drexl, A.: Scheduling of project networks. Management Science 37, 1590–1602 (1991)

6. Schirmer, A.: Case-based reasoning and improved adaptive search for project scheduling. Naval Research Logistics 47, 201–222 (2000)

7. Leon, V.J., Ramamoorthy, B.: Strength and adaptability of problem-space based neighborhoods for resource-constrained scheduling. OR Spektrum 17, 173–182 (1995)

8. Hartmann, S.: A self-adapting genetic algorithm for project scheduling under resource constraints. Naval Research Logistics 49, 433–448 (2002)

9. Alcaraz, J., Maroto, C.A.: robust genetic algorithm for resource allocation in project scheduling. Annals of Operations Research 102, 83–109 (2001)

10. Valls, V., Ballestin, F., Quintanilla, M.S.: A hybrid genetic algorithm for the resource constrained project scheduling. European Journal of Operational Research 185, 495–508 (2008)

11. Bouleimen, K., Lecocq, H.: A new efficient simulated annealing algorithm for RCPSP. Journal of Operational Research 149, 268–281 (2003)

12. Pinson, E., Prins, C., Rullier, F.: Using tabu search for solving the resource- constrained project scheduling problem. Project Management and Scheduling, 102–106 (1994)

13. Nonobe, K., Ibaraki, T.: Formulation and tabu search algorithm for the resource constrained project scheduling problem. In: Ribeiro, C.C., Hansen, P. (eds.) Essays and surveys in metaheuristics, pp. 557–588. Kluwer Academic Publishers, Dordrecht (2002)

14. Colak, S., Agarwal, A., Erenguc, S.S.: Resource-constrained project scheduling problem: a hybrid neural approach. Perspectives in Modern Project Scheduling, 297–318 (2006)

15. Kochetov, Y., Stolyar, A.: Evolutionary local search with variable neighborhood for the resource constrained project scheduling problem. In: Proceeding of the 3rd International Workshop of Computer Science and Information Technologies (2003)

16. Bouleimen, K., Lecocq, H.: A new efficient simulated annealing algorithm for the resource-constrained project scheduling problem. Eur. J. Oper. Res. 149, 268–281 (2003)

17. Debels, D., De Reyck, B., Vanhoucke, M.: A hybrid scatter search/electromagnetism meta-heuristic for project scheduling. Eur. J. Oper. Res. 169, 638–653 (2006)

18. Alcaraz, J., Maroto, C., Ruiz, R.: Improving the performance of genetic algorithms for the RCPS problem. In: Proceedings of the Workshop on Project Management, pp. 40–43 (2004)

19. Pham, D.T., Ghanbarzadeh, A., Koc, E., Otri, S., Rahim, S., Zaidi, M.: The Bees Algorithm. Technical Note. Manufacturing Engineering Centre, Cardiff University, UK (2005)

20. Pham, D.T., Ghanbarzadeh, A., Koc, E., Otri, S., Zaidi, M.: The Bees Algorithm -A Novel Tool for Complex Optimisation Problems. In: Proceedings of IPROMS, pp. 454–461 (2006)

21. Lucic, P., Teodorovic, D.: Bee system: Modeling combinatorial optimization transportation engineering problems by Swarm Intelligence. TRISTAN IV Azores (2001)

22. Mendes, J.J.M., Goncalves, J.F.: A random key based genetic algorithm for the resource constrained project scheduling problem. Computers & Operations Research 36, 92–109 (2009)

23. Chen, W., Shi, Y.-j., Teng, H.-f., Hu, L.-c.: An efficient hybrid algorithm for resource-constrained project scheduling. Information 180, 1031–1039 (2010)

24. Tseng, L.-Y., Chen, S.-C.: A hybrid metaheuristic for the resource-constrained project scheduling problem. European Journal of Operational Research 175, 707–721 (2006)

25. Debels, D., De Reyck, B., Leus, R., Vanhoucke, M.: A hybrid scatter search meta-heuristic for project scheduling. European Journal of Operational Research 169, 638–653 (2006)
26. Debels, D., Vanhoucke, M.: A decomposition-based genetic algorithm for the resource-constrained project-scheduling problem. Operations Research 55, 457–469 (2007)
27. Valls, V., Ballestin, F., Quintanilla, M.S.: A hybrid genetic algorithm for the RCPSP. Department of Statistics and Operations Research. University of Valencia (2003)
28. Valls, V., Ballestín, F., Quintanilla, S.: Justification and RCPSP: a technique that pays. European Journal of Operational Research 165, 375–386 (2005)
29. Tormos, P., Lova, A.: Integrating heuristics for resource constrained project scheduling: one step forward. Technical Report. Department of Statistics and Operations Research. Universidad Politecnica de Valencia (2003)
30. Nonobe, K., Ibaraki, T.: Formulation and tabu search algorithm for the resource constrained project scheduling problem. In: Hansen, P. (ed.) Essays and Surveys in Metaheuristics, pp. 557–588. Kluwer Academic Publishers, Dordrecht (2001)
31. Hartmann, S.: A competitive genetic algorithm for resource-constrained project scheduling. Naval Research Logistics 45, 733–750 (1998)

The Industry Cluster Manufacturing Service of Cooperative Payment System on Lace

Wuling Ren[*] and Jun Yu[**]

Zhejiang Gongshang University, Hangzhou, Zhejiang, China 310018
rwl@zjgsu.edu.cn, yuj@pop.zjgsu.edu.cn

Abstract. In modern manufacture service, the key basis of technology are collaborative and integration. And collaborative design is one of the main support technology on lace project. This paper will apply lace collaborative design platform to research collaborative payment system, for achieving lace product business cooperation techniques better. Meanwhile, lace collaborative payment system can help payment company, seller, buyer, bank, logistics enterprise and relevant society departments to share information, realize real-time interactive of information, coordinate payment work of lace product, and synchronization reflect and process the problems appeared of payment in time, for reducing sale cost maximum, improving payment efficiency of lace products, also benefiting all parties who are in the chain of lace products.

Keywords: collaborative, integration, payment system, lace product.

1   Introduction

Lace, a kind of crafts products, closely related with textile arts. Because of its highly artistic aesthetic and artistic value is being constantly explored, it is being warmly welcomed by people from all walks of life. But lacking of product innovation ability, highly transaction cost, and long transaction process has limited its further development. So we have to do some improvement to solve these problems.

Collaborative commerce will be good to overcome it, which integrate the partners together who have a common commercial interests, and it's mainly to share with the information in the whole business cycle, realize and fulfill the increasing requirements of customers.

Lace collaborative payment system is based on collaborative commerce, which provides payment activities integration, information sharing, collaborative work, and other functions for pay enterprise and its partners through the integration of the lacy collaborative platform. Based on the competitive advantage of the partners of integration, to cooperate and obtain the best commercial value and to provide more profits.

---

[*] Associate Professor, Master Instructor, the main research areas: modern integrated manufacturing system, the computer network project, e-commerce.

[**] Graduate Student, the main research directions: the computer network project, e-commerce.

2   Electronic Payment Theoretical Basis

With the development of e-commerce, networking business models have severely impact the traditional payment models. Electronic payment not only can cut transaction cycles, save time and office cost, but also can reduce bank cost and accelerate business processing speed as a financial services development innovation. Also electronic payment is beneficial to expand banking and increase intermediary business income.

Electronic payment refers to the trading parties, who use safe and online payment methods through money paid or cash flow by networking. In e-commerce typical payment has electronic cash, electronic card and electronic check. When you make transaction and payment on internet, security is very important, it mainly includes:

(1) Integrity, refers to the information which has not been amended, damaged and lost when stored or transmitted for ensuring legitimate users can receive and use real information;

(2) Identity authenticity, when transferred with trade information, we must provide reliable Logo to enable them correctly identify each other and prove themselves, and thereby prevent cheating online effectively;

(3) Undeniably, in order to ensure the transaction run availably, we must prevent trading parties to deny sending or receiving some information;

3   Electronic Payment System Model

Electronic payment system, based on the Internet payment services system, is the most important part in electronic commerce system, it mainly completes to transmit payment information safely between contracting parties and the bank, also supports electronic cash, credit card, e-check and another new or advanced payment tools to implement payment online. It is a system that comprehensive the buyers, sellers, banks, credit agency, certification bodies, payment tool and security technology. The pattern, as figure 1:
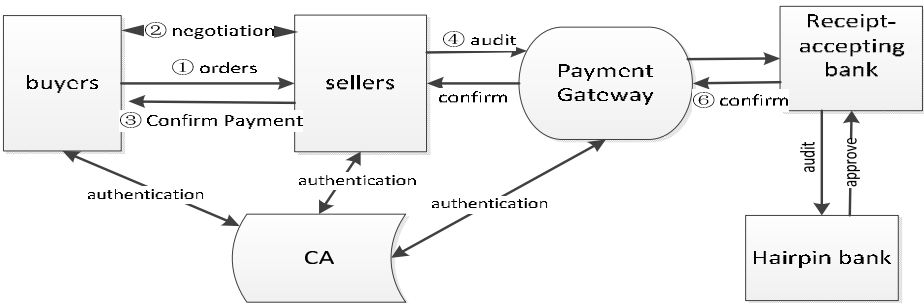
Fig. 1. Electronic payment system

In the electronic payment system, buyer is the one who buy goods or services through Internet and need to pay for seller, who do pay by its own payment tool (such as debit CARDS, electronic purse, etc), which is the reason and start in payment system;

Seller is the one who own creditor's rights with commodity trading, who may request payment to consumer bank or issue according to payment orders launched by buyer;

Buyer's bank or issuer refers to the bank customers own account in it; The receipt-accepting bank is the bank seller open account in it;

Payment gateway is the interface between Internet and financial private network, payment information can't enter bank payment system unless pass payment gateway, then completes the authorization and access of payment. Payment gateway plays a safety protection role for bank's payment systems and payment information; Financial private network is the communication between bank internal and among them, with higher safety;

CA is the one who send digital certificate for participants (including buyer, seller, bank and payment gateway) to confirm their identity, and ensure the safety of payment online.

4   Collaborative Payment Theory

From the above discussion, we can see the development of e-commerce, with the computer and modern communication network and other advanced tools and technologies, electronic payment remove the limit of time and space as traditional payment, so it is welcomed and applicated by more sellers and buyers.

However, with its widespread and application deeply, its disadvantages and limitations were explored too. For instance each enterprise use electronic payment in every field, but relationship can't be increased closely, every enterprise also is a information island, it is contradicted with high-efficient and cooperated goal the enterprise emphasized nowadays.

Collaborative payment theory provides the relevant payment activities integration, information sharing, collaborative work and other functions through integrated payment platform for payment enterprise and its partners. Collaborative payment theory derived from outspread by collaborative e-commerce, cooperation commerce theory, it can realize information collaborative, pay enterprise internal and external collaborative, and gather downstream of the relationship enterprise and customer of payment enterprise, inspire the partners in the chain of common value to fulfill the growing customer demand to enhance profit, and forge a efficient pay value chain.

5   Lace Collaborative Design Technology

Collaborative design, guided by regarding concurrent engineering, and designed development mode by new simulation tools, according to the thoughts oriented design to construct system framework, integrated analysis model in all areas, demanders amend design results continuous and real-time when designing for realizing unify

parallel collaborative design in many fields, and make systematic thought obtain specific applications and reflect in complex products design, so that improve product performance, shorten the design cycle, reduce development costs effectively.

Lace enterprise can put preliminary design results and orders on Internet directly, with hoping to complete design by orders, also by network, designers, manufacturers, material suppliers, and products buyers can communicated directly together, then complete innovative design, thus get rid of time limiting in traditional design, can fully exert design personnel's imagination and creativity to turned conception into final product quickly, also has the incomparable running speed, flexibility and powerful features.

6   Lace Collaborative Design Mode

Cooperation is omni-directional in collaborative design, according to different angles and collaboration granularity, it should satisfy organizations and resources collaborative, design process collaborative, information collaborative and application demand collaborative.

① Collaboration of the organizations and resources

The subjects of products collaborative is come from various organizers, various equipments and software resources, therefore, collaboration of organizational structure and resource model is the prerequisite of product collaborative design. Resource shows the hardware and software resources, resource model is the organization form of material, while organization model is organization form of people, they build relationships by associating.

Collaboration of the design process
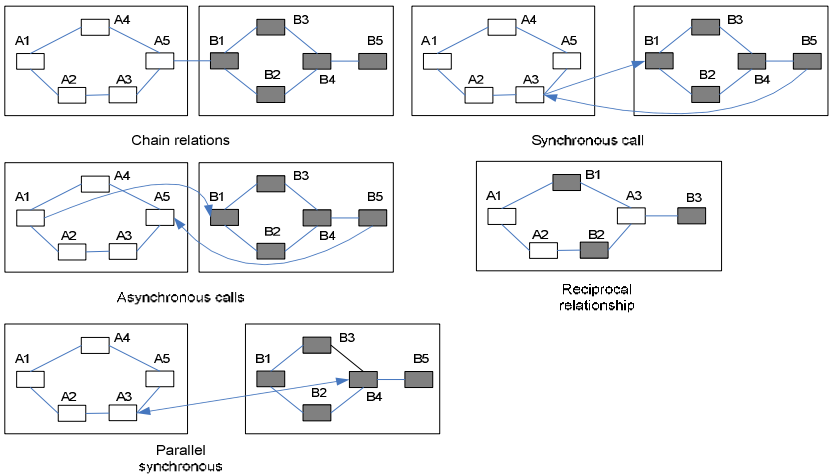
Fig. 2. Five basic forms of design process collaborative

The process of product collaborative design is very complex, which need many designers, communication between design groups, the process of coordination and control, system design should meet the basic five forms of cooperation, namely: chain relations, synchronous calls, asynchronous calls, reciprocal relationship and parallel synchronization, as figure 2.

Collaboration of the Information

Sharing and exchange product information is the form of information collaborative. Products produce a large number of data in the process of design, and it contains product design, production, wisdom and experience in management, so it's the enterprise's precious wealth.

Designer or design groups need to share and exchange information with others in collaborative design, but they also hope to keep a certain degree of autonomy and sketched and decide granularity of sharing information with others independently. Information collaborative should consider the information format, storage methods, safety control and interoperability problems fully to provide smooth data exchange and shared bus for collaborative design.

Collaboration of the application

Collaboration of the application refers to the collaboration among application software which attended the collaborative design of product, that is a operation process use the application tool with collaborative function to complete specific product development, it is a important part in product collaborative design.

According to the coupling degree in product's collaborative development, it can be divided into synchronous collaboration and asynchronous collaboration and collaborative work flow .

In this project, it uses the synchronous collaborative mechanism to process the complex collaborative design task in lace product's collaborative design.

7   Lace Collaborative Payment System Model

In process of lace collaboration design, cooperation is entirely, such as customer's demands, supply, manufacturing, sourcing and the cooperation technology during trading. Therefore it don't need each department to build relationship alone in lace collaborative payment model. In the past, just only produce information flow between the department which produce trade information directly in payment chain, so it is easy to form information island, if there are some connection among departments, we must to establish contact platform again, thus it cause higher cost and lower efficiency. However, with lace collaborative platform, it will connect with each department together, so that all information flow will be produced on it. And provide payment activities integration, information sharing, collaborative work and other functions for payment enterprise and its partners by integrated cooperative platform. Lace collaborative payment systems as figure 2:

Lace collaborative payment system integrate payment work in the technical level to provide a set of system which can help each related department to profit and

operate, that is to say, when the data was transferred in real-time, system will coordinate payment platform, demander, supplier and bank sector to cooperative work together closely, and synchronization reflect and processing relevant matters in time.
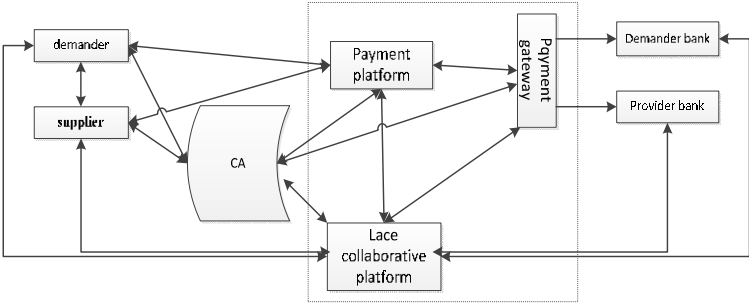
Fig. 3. Lace collaborative payment system

8   Conclusions

Enterprise use electronic payment in every field, but relationship can't be increased closely, there also is an information island among enterprises, it is contradicted with high-efficient and cooperated goal the enterprise emphasized nowadays. So through researching collaborative payment system, it can solve various safety problems in electronic payment systems for enterprise. Meanwhile lace collaborative payment system can ensure decision accuracy and operation efficiency for each enterprise, one of the necessary conditions is that they can share information and link relevant work automatically, also enterprises possess the function of utilization resources effectively. Resources are the basis of enterprise ability, meanwhile, enterprise ability is the main source of enterprise competitive advantage.

References

1. Jin, G., Huo, Y., Sun, X.: Electronic trading and payment, vol. 9. China power press (2004)
2. Han, B., et al.: E-commerce Security and Payment. People's wiley&sons press (2001)
3. Satyam partners with Adexa to implement collaborative commerce solutions. World IT Report, London (April 8, 2003)
4. Du, J.: Collaborative e-commerce: The 21st century's commerce model. Jiangxi Social Science 9 (2002)
5. Schmidt, D.: Credit's role in collaborative commerce. Business Credit NewYork (June 2002)

Floatation Froth Image Segmentation Algorithm Based on Mathematical Morphology and Wavelet

Fen-Ling Lang and Da-Ling Jiang

Beijing University of Technology
100124 Beijing, China
Lfl191@163.com

Abstract. The features of floatation froth: no background, the bubbles are adhesive and the weak verges between them. This paper presents segmentation algorithm for floatation froth based on watershed and wavelet, at the same time, application of opening and closing operations, morphological gradient method based on mathematical morphology. The algorithm solved the problems of over segmentation and under segmentation and reduced the complexity of the computation. At last, get each froth's area. Experiments show that the proposed method can ensure both calculated efficiency and segmentation accuracy.

Keywords: floatation froth, image segmentation, mathematical morphology, wavelet transform.

1 Introduction

Mineral flotation is a kind of mineral processing methods. During the process, flotation reagents are added to the pulp and air is filled in the slot. Then they are mixed to bring a great deal of air bubbles. Finally ore grade is improved by retrieving froth containing minerals to meet smelting requirements. Usually, froth is large quantity, adherence, hybrid and irregular shape. Flotation process of metal mines in China is usually operated by experienced workers through observing froth surface [1]. As a result, it is hard to work in optimized running state and mineral recovery ratio is low. The rapid progress in computer technology has made the use of machine vision in the control of industrial flotation operations possible. In the last ten years, a number of researchers have studied this topic. Moolman[2] train a neural network to classify image characteristics. However, they recognize that the complexity of the froth makes it extremely difficult to relate the visual parameters to individual processes or mechanisms which occur in the froth or to build up the large data bank which would be required to be able to have confidence in the capacity of the neural network to correctly diagnose faults. The use of textural analysis for extracting image information has been proposed [3]. It is found to be difficult to attach physical meaning to these numbers, although they qualitatively indicate features such as fineness, homogeneity and coarseness. So this paper presents segmentation algorithm for floatation froth. Accurately measurement of the bubble size distribution on the surface of the froth is required. The method can ensure both calculated efficiency and

segmentation accuracy. Resolve the primary problem of automatic control system in flotation process.

2   Floatation Froth Image Segmentation Algorithm Based on Mathematical Morphology and Wavelet

2.1   Theory of Image Processing

2.1.1   Wavelet Transform

Wavelet transform has the ability to examine a signal at different scales. Matllat[4] proposed the relationship between multi-resolution analysis and wavelet transform. Any multi-resolution subspace V_m can be decomposed to rough approximation of a low-frequency V_{m-1} and details of a high frequency W_{m-1} through one step of Multi-resolution., Low frequency and high frequency part should meet:

$$V_m \bigcap W_m = \{0\}, m \in Z \tag{1}$$

$$V_m = V_{m-1} \bigcap W_{m-1}, m \in Z \tag{2}$$

Here m the series of multi-resolution analysis.

Extended the one-dimensional wavelet transform to two-dimensional, two-dimensional signal such as the image can be wavelet decomposition. All wavelet transform coefficients can be expressed as:

$$\{W_A^J\} \bigcup \{W_H^j, W_V^j, W_D^j\}_{j=1,2...J} \tag{3}$$

Here J the series of wavelet transformation, W_A^J the J layer of low-frequency wavelet coefficients. W_H^j the j layer of horizontal low-frequency and vertical high-frequency wavelet coefficients, W_V^j means the j layer of horizontal high-frequency and vertical low-frequency wavelet coefficients, W_D^j means the j layer of horizontal and vertical high-frequency wavelet coefficients.

Any image can be decomposed into two parts: low frequency (subject information) and high-frequency (detail information) used low pass and high pass filter provided by wavelet filter. Each image can be decomposed into horizontal and vertical high-frequency low-frequency image (HL), horizontal and vertical high-frequency low-frequency image (LH), high frequency in both directions (HH) image, low-frequency in both directions (LL) image. The size of each image is a quarter of the original image.

2.1.2   Mathematical Morphology

(1) Filter and morphological gradient

This paper use morphological opening and closing filter to low noise. The definition of gray closed filter is [5]:

$$close(A, B) = (A \oplus B)\Theta B \qquad (4)$$

Here $\oplus$ erosion, Θ denote, B is structure elements, A is image.

Gray open filter is the gray closed filter's dual operation. The definition of gray open filter:

$$open(A, B) = (A\Theta B) \oplus B \qquad (5)$$

The dilation and erosion are used to compute the morphological gradient of image f, denoted by B:

$$grad(f) = (f \oplus B) - (f\Theta B) \qquad (6)$$

(2) Watershed algorithm

Watershed algorithm is proposed by Vincent and Soille [6] in 1991, it is a method based on mathematical morphology. Watershed algorithm is widely-used method in image segmentation and image edge detection. Generally, it is used to process the gray gradient image. Its basic thought is that the image is regarded as topology geomorphology in geodesy and each pixel value in the image is taken as the altitude above sea level. There are basin, ridges, the hills between ridges and basins. The algorithm simulates process of flooded terrain from bottom to up. First the water is constantly pouring from the lowest point of terrain namely basin bottom, Then the terrain will gradually be submerged. When two water basins will be convergence, establish a dam in the confluence. Until the entire terrain were submerged, so get the various dams (watershed) and the basin (target objects) be separated by dams.

Watershed algorithm is sensitive to noise, the result of segmentation have under segmentation and over segmentation. To solve the problem have two methods. The one is a post-processing: region merging by certain criteria, the other is generating accurate water basins.

2.2 The Process of Algorithm

This paper algorithm mainly includes four steps: (1) wavelet transform (2) gradient image (3) seeds extraction (4) watershed segmentation. The process of algorithm is showed below:
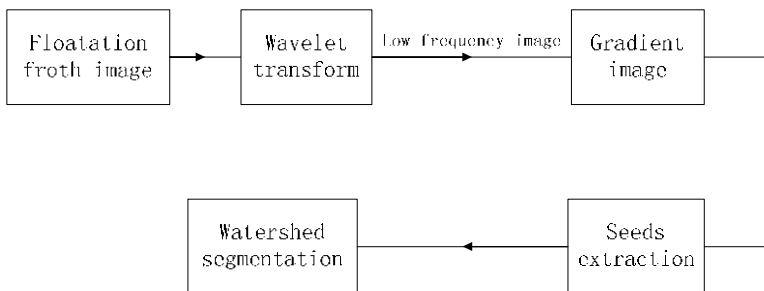
Fig. 1. The process of algorithm

2.2.1   Wavelet Transform

Wavelet transform is seen as low-pass filter, filtering image noise and small water basins. The image is decomposed by one series wavelet transform. low-frequency image (LL) maintains the image low-frequency information, reduce the noise, over-segmentation, the computational complexity. The result of one series wavelet transform is showed in below:

a. floatation froth image   b. image after wavelet transform
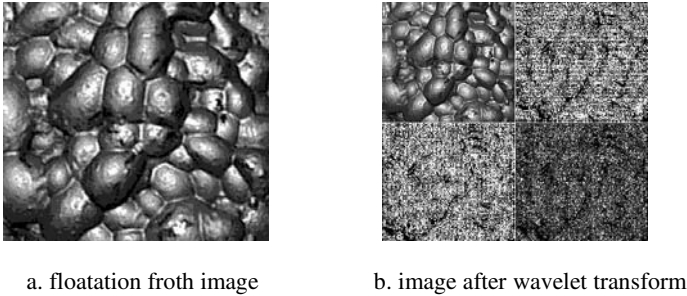
Fig. 2. One series wavelet transform

2.2.2   Gradient Image Processing

Gradient image can provide better performance in the trend of the image, and the watershed algorithm results show a larger relationship with the gradient image. The morphological gradient is less sensitive to noise. The result of gradient image processing is showed below:

a. floatation froth image   b. gradient image
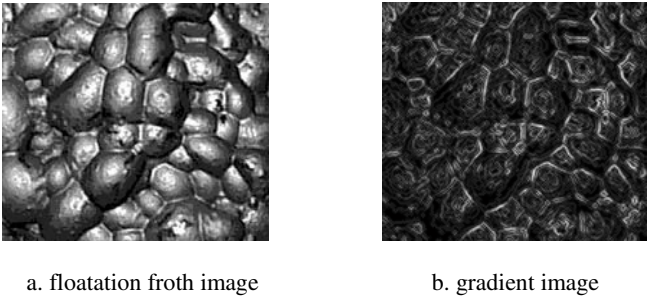
Fig. 3. Gradient image

2.2.3   Extraction of Seeds

At the top of froth film hydration becomes thin, is high light reflection coefficient. So there is a bright spot in the top of the froth named seed point. The key step is to mark seed points, before application the watershed algorithm. When the froth contains some seeds, froth is divided into several smaller froths, resulting in over-segmentation. When the bubble boundary is very weak, a few seeds into a seed point, several froth into a bubble, resulting in a less divided. The accuracy of seed points determines segmentation good or bad.

The gray histogram of froth image has single peak, selection the threshold is more difficult. This algorithm uses OTSU method, choose a reasonable threshold to extract the binary image, select accurate seed points applying the morphological opening and closing operation.

The processing steps of the image with gray value 0-255 by OTSU are as follows:

(1) Calculate the probability function $p(i)$ of the image gray level is i

$$p(i) = \frac{\text{the number of pixels gray value of } i}{\text{the total number of pixels in the image}} \quad i = (0,1...255) \quad (7)$$

(2) The mean gray A, mean of class $A(k)$, sum of histogram class $W(k)$:

$$A = \sum_{i=0}^{255} (i-1)P(i) \quad (8)$$

$$A(k) = \sum_{i=0}^{k} (i+1)P(i) \quad (9)$$

$$W(k) = \sum_{i=1}^{k} P(i) \quad (10)$$

(3) Divergence guideline of class $Q(k)$:

$$Q(k) = \frac{[A \bullet W(k) - A(k)]^2}{W(k)[1 - W(k)]} \quad (11)$$

(4) Find the Q when k is largest, determined T is the optimal threshold:

$$T = k - 1 \quad (12)$$
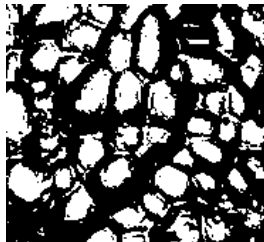
a. floatation froth image   b. image after binary   c. image after opening and closing operation
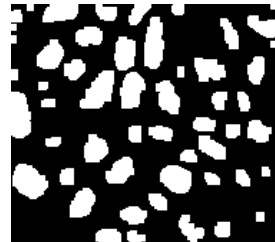
Fig. 4. Extraction of seeds

The image is binary according the best threshold T, Separated the seed points from the picture. After binary transformation, there has been the phenomenon of adhesion

and fracture. The different goals of the large area separate by morphological opening and closing operations. opening operation can remove small isolated points, burrs and bridges, closing operation can fill holes, bridge small cracks. The result is showed below:

2.2.4   Watershed Algorithm

Watershed algorithm combines the advantages of edge detection and region growing, and can quickly get a single wide, connected, closed, exact location of the outline. Because of the influence by noise and texture detail, there are a lot of pseudo-local minimum, resulting in the corresponding pseudo-water basin, eventually leading to over-segmentation. The paper combine the wavelet transform and watershed algorithm, Wavelet transform is considered as low-pass filter, have a good filtration image noise and small water basins, the calculation time is reduce by 1/4 and the result is showed below:

| a. algorithm in the paper | b. result without wavelet transform | c. result with traditional watershed |
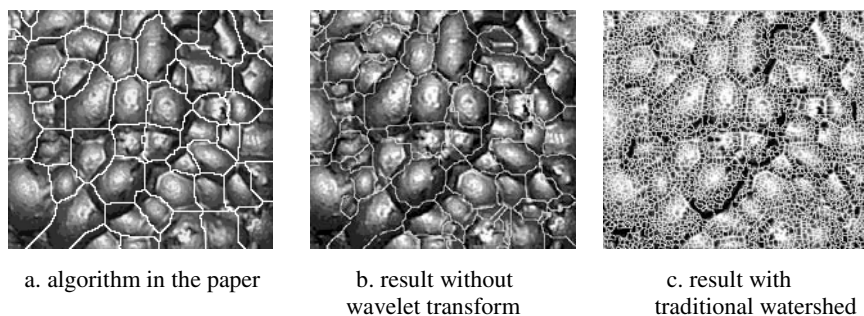
Fig. 5. Watershed segmentation

2.3   Feature Extraction and Analysis of Floatation Froth

Properties of froth surface such as the number, size, color, shape can reflect the mineral content, are important basis to complement automatic control of flotation process. The shape and size of the bubble reflects the quality of production .froth size reflecting the flotation agent or inflated is appropriate or not.

After the flotation froth image segmentation, get the number and size of froth by connected component labeling. Divide into large, medium and small froth according to the bubble size. A lot of large froth means high gas content, a lot of small bubbles mean that foaming process is inhibited, a large number of middle-foam flotation means that the flotation state is good.

3   Conclusion

This paper presents segmentation algorithm for floatation froth based on multi-resolution analysis and watershed. Experiments show that the proposed method can ensure both calculated efficiency and segmentation accuracy. Finally, calculate the size and number of the froth. The system can give operating mode information and

operation suggestion to the worker. Furthermore, labor productivity is increased and operation aimlessness is avoided, which provided the foundation for optimal control of flotation process.

References

1. Wang, W., Bergholm, F., Yang, B.: Froth delineation based on image classification. Minerals Engineering 16(1), 1183–1192 (2003)
2. Moolman, D.W., Eksteen, J.J., Aldrich, C., et al.: The significance of floatation froth appearance for machine vision control. International Journal of Mineral Processing 48, 135–158 (1996)
3. Wang, Y., Yang, G.-x., Lu, M.-x., Gao, S.-h.: The gray run length and its statistical texture features of coal flotation froth image. Journal of China Coal Society 31(1), 94–98 (2006)
4. Mallat, S.G.: A Theory for Multiresolution Signal Decomposition: The Wavelet Representation. IEEE Trans. on Pattern Analysis and Machine Intelligence 11(7), 674–693 (1989)
5. Rafael, C., Gonzalez Richard, E., Woods Steven, L., et al.: Digital Image Processing Using Matla. Publishing House of Electronics Industry 9, 285–320 (2005)
6. Vincent, L., Soille, P.: Watershed in digital spaces: an efficient algorithm based on immersion simulations. IEEE Trans. Pattern Analysis and Machine Intelligence 13(6), 583–598 (1991)

Image Enhancement Using the Multi-scale Filter: Application of the Bilateral Filtering Scheme and PSO Algorithm

Wei-Sheng Yang[1], Chih-Hsien Kung[2], and Chih-Ming Kung[3]

[1] Dept. of Information Management, Chang Jung Christian University,
Tainan, Taiwan
[2] Dept. of Engineering & Management of Advanced Technology
Chang Jung Christian University, Tainan, Taiwan
`kung@mail.cjcu.edu.tw`
[3] Dept. of Information Technology and Communication
Shih Chien University Kaohsiung Campus, Kaohsiung, Taiwan
`alex@mail.kh.usc.edu.tw`

Abstract. As technology advances, the image display technology and industry have been evolved as well. In the research field of color images, image quality analysis and enhancement are increasingly important. Therefore, we focus on image enhancement in this research. For this reason, we propose a new opinion about image enhancement by multi-scale image filter. The multi-scale image filter apply the bilateral filtering scheme and PSO algorithm to improve the image quality. This study expects to improve the image quality by multi-scale image filter.

Keywords: Image Enhancement, Particle Swarm Optimization, Bilateral Filter.

1 Introduction

As technology advances, the image display technology and industry have been evolved as well. The resolution of monitor continue to be improved and the size of monitor also continue to become larger. However, the hardware technology of panel industry has become increasingly, but the image processing technology has not kept pace with hardware. For example in LCD display, it maybe appear block effect sometimes, because its image processing is not well. In this case, some manufactures propose the technology of High Dynamic Image and Mode Selection to apply the LCD panels, but this method can't not do real time and adaptive processing. For this reason, we propose a new opinion about image enhancement by multi-scale image filter. Therefore, we focus on image enhancement in this research.

We enhance the image by bilateral filter and use PSO algorithm to adjust the parameter of the bilateral filter. And we use the SSIM index to do image quality assessment. The image quality will be improved.

2   Image Enhancement

As digital archives are popularity, the tone of image is very important. In 2001, Agaian et al. proposed the new method about new type signal and image enhancement which is based on frequency. These algorithms are applied to image detection and object of the visual image, which is based on Fourier, Hartly, cosine, Hadamard transforms and the new enhanced operator. The goal of image enhancement is improving the visual identification, and provides the automatic image processing procedure in the future (e.g. analyze, detection, division, and identify). Most methods are proposed about image enhancement. [1-3], these methods mostly modify the value of histogram, the other methods is analyzing the edge and adjusting contrast or transforming the global entropy.

2.1   Bilateral Filter

Bilateral filter is a technology to smooth images. It is a non-linear filter. It is proposed for smoothing the noise and preserving edges in the image processing. It starts with standard Gaussian filtering in both spatial and intensity domains.

It has been used in various contexts such as denoising, texture editing and relighting, tone management, demosaicking, stylization, and optical-flow estimation. The bilateral filter has several qualities that explain its success:

1.   Its formulation is simple: each pixel is replaced by a weighted average of its neighbors. This aspect is important because it makes it easy to acquire intuition about its behavior, to adapt it to application-specific requirements, and to implement it.
2.   It depends only on two parameters that indicate the size and contrast of the features to preserve.
3.   It can be used in a non-iterative manner. This makes the parameters easy to set since their effect is not cumulative over several iterations.

Fig.1 is the bilateral filter deal with the High dynamic range image. The output image of the bilateral filter is become very well, the edge is obviously.

(a) the high dynamic range image   (b) output of the bilateral filter

Fig. 1. Image processing use the bilateral filter

The bilateral filtering is defined as follows:

$$g(x,y) = \frac{\sum_{i=-a}^{a}\sum_{j=-b}^{b}W(i,j)f(x+i,y+i)}{\sum_{i=-a}^{a}\sum_{j=-b}^{b}W(i,j)} \qquad (1)$$

Where $f(x, y)$ is the original signal, $g(x, y)$ is the smoothed signal by the bilateral filtering, $(2a+1)\times(2b+1)$ is the length of bilateral filter. $W(i, j)$ is the kernel of bilateral filter:

$$W(i,j) = W_s(i,j) \times W_I(i,j) \qquad (2)$$

W_s is the Gaussian filter on the spatial domains, is defined by :

$$W_s(i,j) = G\left(\sqrt{i^2+j^2},\sigma_s\right) = \frac{1}{2\pi\sigma_s^2}\exp\left(-\frac{\sqrt{i^2+j^2}^2}{2\sigma_s^2}\right) \qquad (3)$$

W_I is the Gaussian filter on the intensity domains, is defined by ::

$$W_I(i,j) = G(f(x+i,y-i)-f(x,y),\sigma_i)$$
$$= \frac{1}{2\pi\sigma_i^2}\exp\left(-\frac{[f(x+i,y-i)-f(x,y)]^2}{2\sigma_i^2}\right) \qquad (4)$$

2.2   Particle Swarm Optimization

In 1995, PSO is proposed by the Eberhart and Kennedy [4-5], which is a kind of Evolutionary Computation. Every bird can be as a particle. Each particle keeps track of its coordinates in hyperspace which are associated with the best solution (fitness). The value of that fitness is also stored. This value is called pbest. Another "best" value is also tracked. The "global" version of the particle swarm optimizer keeps track of the overall best value, and its location, obtained thus far by any particle in the population; this is called gbest. The particle swarm optimization concept consists of, at each time step, changing the velocity each particle toward its pbest and gbest (global version). Acceleration is weighted by a random term, with separate random numbers being generated for acceleration toward pbest and gbest.
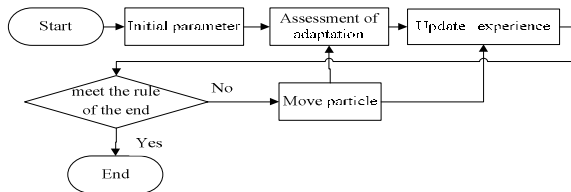
Fig. 2. PSO diagram

PSO is a population-based algorithm for searching global optimum. The original idea of PSO is to simulate a simplified social behavior. It ties to artificial life, like bird flocking or fish schooling, and has some common features of evolutionary computation such as fitness evaluation. For example, PSO is like a GA in that the population is initialized with random solutions. The adjustment toward the best individual experience (PBEST) and the best social experience (GBEST) is conceptually similar to the crossover operation of the GA. However, it is unlike a GA in that each potential solution, called particle, is "flying" through hyperspace with a velocity. Moreover, the particles and the swarm have memory, which does not exist in the population of the GA.

Let $x_{j,d}(t)$ and $v_{j,d}(t)$ denote the dth dimensional value of the vector of position and velocity of jth particle in the swarm, respectively, at time t. The PSO model can be expressed as

$$v_{j,d}(t) = v_{j,d}(t-1) + c_1 \cdot \varphi_1 \cdot (x_{j,d}^* - x_{j,d}(t-1)) + c_2 \cdot \varphi_2 \cdot (x_d^{\#} - x_{j,d}(t-1)) \qquad (5)$$

$$x_{j,d}(t) = x_{j,d}(t-1) + v_{j,d}(t) \qquad (6)$$

where x_j^* (PBEST) denotes the best position of jth particle up to time t-1 and $x^{\#}$ (GBEST) denotes the best position of the whole swarm up to time t-1, φ_1 and φ_2 are random numbers, and $c1$ and $c2$ represent the individuality and sociality coefficients, respectively.

The population size is first determined, and the position and velocity of each particle are initialized. Each particle moves according to (5) and (6), and the fitness is then calculated. Meanwhile, the best positions of each particle and the swarm are recorded. Finally, as the stopping criterion is satisfied, the best position of the swarm is the final solution. The block diagram of PSO is displayed in Fig. 3 and the main steps are given as follows:

1. Set the swarm size. Initialize the position and the velocity of each particle randomly.
2. For each j, evaluate the fitness value of x_j and update the individual best position x_j^* if better fitness is found.
3. Find the new best position of the whole swarm. Update the swarm best position $x^{\#}$ if the fitness of the new best position is better than that of the previous swarm.
4. If the stopping criterion is satisfied, then stop.
5. For each particle, update the velocity and the position according (5) and (6). Go to step 2.

3   Experimental Methods

The study focuses on the image enhancement by Bilateral filter with Particle Swarm Optimization Alogrithm. And we use the SSIM index [6-15]to assess the image quailty. According to the quailty, the image process will finish or again.

In this study, we use this two parts to set a system to achive the image enhancement about adaptive video enhancement filters. The system diagram is given in Fig. 9.
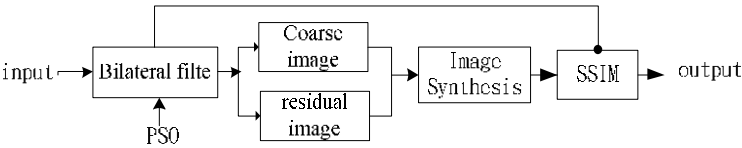
Fig. 3. The system diagram

3.1   Bilateral Filter with PSO

As discussed in Section 2, we know the bilateral filter is a neighborhood filter by Gaussian filter. The bilateral filter has three parameters: $|N_x|$ is the neighborhood size, σ_s is the distance variance of Gaussian distribution function, σ_i is the gray value difference of Gaussian distribution function.

We encode the particle as $x_j = (|N_x|, \sigma_s, \sigma_i)$, which is the position of the domain block. The steps of encoding a range block using PSO are summarized as follows:

1. Initialize the parameters of PSO.
2. For each particle $x_j = (|N_x|, \sigma_s, \sigma_i)$, fetch the domain block at $x_j = (|N_x|, \sigma_s, \sigma_i)$ in the image. Sub-sample the block and denote it.
3. Find the new best position of the whole swarm. Update the swarm best position $x^\#$ if the fitness of the new best position is better than that of the previous swarm.
4. If the stopping criterion is satisfied, then stop.
5. For each particle, update the velocity and the position according (5) and (6). Go to step 2.

Table 1. The result of the image enhancement

	IMAGE A	IMAGE B	IMAGE C	IMAGE D
ORIGNAL IMAGE				
PSNR	13.9827	18.4834	15.1862	18.4487
SSIM	0.6987	0.6866	0.6219	0.5480
IMANG ENHANCEMENT				

4   Experimental Results

In this study, we use the bilateral filter to enhancement the image, especially in the High dynamic range image is very significant. To set the best parameter of bilateral filter, we use the PSO to find the best value of parameter. And using the SSIM to assessment the image quality after enhancement. If the image quality is not well, the image will enhance again. Table II is the result of the image enhancement by Bilateral filter and PSO, and use the SSIM and PSNR to assessment the image quality.

As the Table 2, bilateral filter is helpful for the High dynamic range images. The image detail can be improved by bilateral filter. We can see experiment results as the Table 2, the original images qualities aren't very well. After bilateral filtering, the images become very well.

5   Conclusion

According to the experimental results, the quality of the image has increased by image enhancement. Because the bilteral filters can save the detail of the image and increase the luminance. Therefore, the image enhancement filter can help for adjusting the High dynamic range images and make the image suit for human vision.

References

1. Rosenfeld, Kak, A.C.: Digital Picture Processing, vol. 1. Academic, New York (1982)
2. Jain: Fundamentals of Digital Image Processing. Prentice-Hall, Englewood Cliffs (1989)
3. Ji, T.L., Sundareshan, M.K., Roefrig, H.: Adaptive image contrast enhancement based on human visual properties. IEEE Trans. Med. Img. 13, 573–586 (1994)
4. Kennedy, J., Eberhart, R.C.: Particle swarm optimization. In: Proc. IEEE Int. Conf, on Neural Networks, vol. 4, pp. 1942–1948 (1995)
5. Eberhart, R.C., Kennedy, J.: A new optimizer using particle swarm theory. In: Proc. IEEE Int. Symposium on Micro Machine and Human Science, Nagoya, Japan, pp. 39–43 (1995)
6. McCulloch, W.S., Pitts, W.: A logical calculus of ideas immanent in nervo-Us activity. Bulletin of Mayhematical Biophysics 5, 115–133 (1943)
7. Hebb, D.O.: The Organization of Behavior: A Neuropsychological Theory. Wiley, New York (1949)
8. Rosenblatt, F.: The perceptron: A probabilistic model for information Storage and organization in the brain. Psychological Review 65, 386–408 (1958)
9. Wang, Z., Bovik, A.C., Sheikh, H.R., Simoncelli, E.P.: Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing 13(4), 600–612 (2004)
10. Wang, Z., Li, Q.: Video quality assessment using a statistical model of human visual speed perception. Journal of the Optical Society of America A (December 2007)
11. Wang, Z., Shang, X.: Spatial pooling strategies for perceptual image quality assessment. In: IEEE International Conference on Image Processing, Atlanta, GA (October 8-11, 2006)

12. Wang, Z., Simoncelli, E.P.: Translation insensitive image similarity in complex wavelet domain. In: IEEE International Conference on Acoustics, Speech and Signal Processing, Philadelphia, PA, vol. II, pp. 573–576 (March 2005)
13. Wang, Z., Lu, L., Bovik, A.C.: Video quality assessment based on structural distortion measurement. Signal Processing: Image Communication, special issue on "Objective video quality metrics" 19(2), 121–132 (2004)
14. Wang, Z., Simoncelli, E.P., Bovik, A.C.: Multi-scale structural similarity for image quality assessment. In: Invited Paper, IEEE Asilomar Conference on Signals, Systems and Computers (November 2003)
15. Kung, C.-H., Yang, W.-S., Huang, C.-Y., Kung, C.-M.: Investigation of the Image Quality Assessment using Neural Networks and Structure Similarty. In: The Third International Symposium Computer Science and Computational Technology (ISCSCT 2010), Jiaozuo, China, pp. 219–222 (August 14-15, 2010)

The Impact of LUCC on Ecosystem Service Values in HaDaQi Industrial Corridor

Xiaodong Na, Shuying Zang, Nannan Zhang, and Hang Liu

Key Laboratory of Remote Sensing Monitoring of Geographic Environment,
College of Heilongjiang Province, Harbin Normal University,
Harbin, Heilongjiang, P.R. China 150025

Abstract. Taking HaDaQi industrial corridor, Heilongjiang Province, China as a case study area, this paper examined the trend of land use changes during 1990-2005 used three LANDSAT TM and/or ETM data sets, and quantified their influences on natural ecosystem service values. During the whole period of study, Land Use/Cover Type changed immensely in the study area, the development of land is increasing continuously. The total value of ecosystem services in HaDaQi Industrial Corridor declined by 18.23 billion yuan. We also found that the contribution of construction, reclamation and water shortage increased during the 15-year time period. We conclude that future land-use policy formulation should give precedence to the conservation of these ecosystems over uncontrolled construction, reclamation, and water consumption and that further land development should be based on rigorous environmental impact analyses.

Keywords: Ecosystem Service Values; LUCC; HaDaQi Industrial Corridor; remote sensing images.

1 Introduction

Change in land use/cover (LUCC) is one of the most profound human-induced alterations of the Earth's system [1]. During this process of land conversion, economic development and quality of life improvement are considered as major goals, and their influences on ecological systems have often been neglected.

The degradation of natural ecological systems due to land use change, however, has become severe, and may require immediate attentions from urban planners and local governments [2]. Since 1990 numerous studies have been conducted to estimate the values of various ecosystem services, including the economic valuation of different biological resources, protected areas and endangered species management [3-6]. Especially, Constanza attempted to estimate the global biospheric value of 17 ecosystem services provided by 16 dominant global biomes [7]. When applied in China, Xie et al. (2001) argued that the valuation method proposed by Costanza et al. underestimates the service value of agricultural lands, and overestimates other biomes, such as wetlands and forest [8]. Consequently, Xie et al. (2003) calculated valuation coefficients for ecosystems in China through a contingent valuation analysis based on a survey of 213 ecologists [9]. The purpose of this paper, therefore, is to

evaluate the impact of LUCC on natural ecosystem service values in HaDaQi Industrial Corridor based on the valuation method provided by Xie et al., and make some preliminary policy recommendations to ensure the sustainable use of these industrializations area.

2   Materials

2.1   Study Area

Ha-Da-Qi Industrial Corridor is located in the west of Heilongjiang Province, which covers an area of 21 180 km^2 between 122°48' and 127°15'E, 45°31' and 47°51'N. It is an economic region including three major cities (Harbin, Daqing, and Qiqihar) and four counties (Zhaodong, Anda, Dumeng, and Tailai). Located in the eastern part of HaDaQi Industrial Corridor, Harbin is the capital city of Heilongjiang Province, with a geographical area of 53,100 km^2 (see Fig 1).
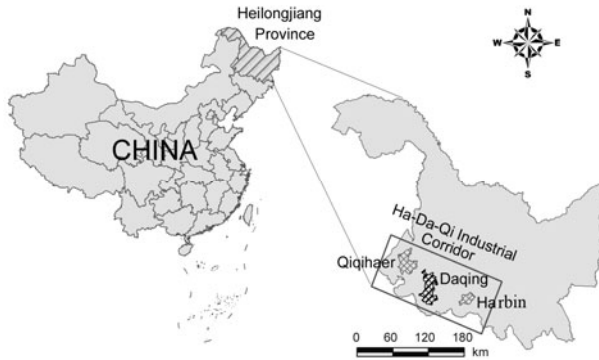
Fig. 1. Location Map of the HaDaQi Industrial Corridor

2.2   Data Description

Land use was studied on the basis of digital data of Landsat-5 TM band 1 to 5 and band 7 (1990, 2000, and 2005) covered HaDaQi Industrial Corridor. Each image comprises six bands with 30m spatial resolution (bands 1 to 5 and band 7). In addition to the remote sensing imagery, socio-economic data, such as the gross domestic products (GDP) and market prices of agricultural produce, were also obtained from Heilongjiang Statistics Yearbooks.

3   Methodology

3.1   Geometric Rectification and Land Cover Classification

The geometric errors of these remote sensing images were evaluated and corrected using ground control points (GCPs). All images were registered to the Albers

projection using ERDAS Imagine 8.7software. Between 55 and 66 Ground Control Points (GCPs) were used for each image. This registration procedure achieved an accuracy of less than 0.5 pixel root mean squares error (RMSE).Then land use types is classified into cultivated land, forestland, meadow, unused land, residential area, saline-alkali, and open water. For testing of the land cover classification, field survey was conducted in August 2005 to collect real time ground truth reference data, aided by a global positioning system (GPS) unit. The accuracy of the resultant landscape maps was assessed with these testing samples in the study area. The producer's accuracy, user's accuracy, overall accuracy, and Kappa coefficient were derived for accuracy assessment.

3.2   Ecosystem Service Valuation Method

In order to obtain ecosystem services values for each of the six land-cover categories used to classify the LANDSAT datasets, Xie et al. (2003) developed a contingent valuation method based on the survey of more than 200 Chinese ecologists. With the ecosystem service coefficients for each land use/land cover type, the total ecosystem service values in HaDaQi industrial corridor in 1990, 2000, and 2005 were calculated as follows. Firstly, Calculating the food production service value for agricultural lands, which is one-seventh of the market price of agricultural produce; Secondly, with the food production service value of agricultural lands as the unit, estimating the ratio between service values of all other ecosystem functions to the food production service value of agricultural lands using surveying techniques; Thirdly, deriving the service values for each function of each ecosystem through multiplying the agricultural land service value with the corresponding ratio; lastly, generating a final ecosystem service value (ESV) for each land use type through summing the values for each function, and multiplying by the its respective geographical area.

4   Result

4.1   Land Use Change Analysis

Land use land cover maps in 1990, 2000, and 2005 derived from Landsat TM imagery were illustrated in figure 2, and the results are summarized in Table 1.Analysis of the results suggests that, during these 15 years, human-dominated land uses (i.e. cultivated land and residential area) have expanded rapidly at the cost of natural lands (forest, grassland and open water). In particular, as can be distinguished from Table 1, the area of cultivated land uses increased from 9842.55 km^2 in 1990 to 11685.1 km^2 in 2005, with a total increment of 18%. Similarly, the geographic areas of residential area and unused lands have increased 304.3 km^2. Conversely, natural lands, including forest, grassland, and open water, have diminished substantially. The geographical area of wetlands and water, in particular, has decreased from 1242.9 in 1990 to 975.31 in 2005, with an overall area change of 31.0%. Similarly, meadow area also diminished significantly (about 40.3%). These results suggest that human-disturbed land uses have expanded significantly, with the costs of natural lands.

Table 1. Land use changes in Ha-Da-Qi Industrial Corridor at various stages during 1990-2005

Land cover types	1990		2000		2005	
	area (km^2)	% Change	area (km^2)	% Change	area (km^2)	% Change
Cultivated land	9842.55	50.92	11229.91	58.1	11685.1	60.46
Forestland	124	0.64	282.54	1.46	190.58	0.99
Meadow	3768.09	19.5	2185.94	11.31	2247.85	11.63
Open water	1242.9	6.43	1172.01	6.06	975.31	5.05
Residential area	1056.8	5.47	1255.8	6.5	1361.1	7.04
Unused land	3293.77	17.04	3201.89	16.56	2868.16	14.84

4.2   Estimation of Changes in Ecosystem Service

Using the dynamic change in the size of each land-cover category together with the ecosystem service value coefficients reported by Xie et al., we found that land-use changes in the our study area resulted in net decline of ¥18.23 billion in ecosystem services between 1990 and 2005 (Table 2). For individual land use types, the ESV decrement for wetlands and water (¥17.03 billion) is higher than that that estimated from forestland (¥2.48 billion) and meadow (¥0.07 billion). For cultivated land, however, the increment of the ESV (¥1.33 billion) is significant. The result emphasizes the importance of this land type in the provision of ecosystems services, and underscores the substantial reduction in annual ecosystem services as a result of the extensive loss of wetlands. However, the result of our sensitivity analysis also emphasizes the importance of obtaining accurate value coefficients for dominant land types in order to quantify accurately the ecological economic effect of LUCC.

Table 2. ESVs in 1990, 2000, and 2005, and their changes from 1990 to 2005

Land use type	1990 (10^9¥)	2000 (10^9¥)	2005 (10^9¥)	1990-2005		
				change (10^9¥)	% Change	% per year
Cultivated land	415.87	426.41	429.12	13.25	3.19	0.21
Forestland	159.06	150.56	134.30	-24.76	-15.57	-1.04
Meadow	34.22	31.10	33.5	-0.72	-2.10	-0.14
Open water	548.58	493.00	378.3	-170.28	-31.04	-2.07
Residential area	0.00	0.00	0.00	0	0	0
Unused land	1.73	1.80	1.96	0.23	13.29	0.89
Total	1159.46	1102.87	977.18	-182.28	-15.72	-1.05

4.3   The Impact of LUCC on Ecosystem Service Value

In order to understand the relationship between the LUCC and ecosystem service value, we compare the construction of LUCC and ecosystem service value (see Table 3 and Figure 2). The Table 3 showed that the percentage of cultivated land area is the largest in HaDaQi Industrial Corridor (above 60%). However, the percentage of

ecosystem service value provided by cultivated land is much lower than its area (35%-45%). Especially, the ecosystem service value contributed from cultivated land increased ¥ 0.27 billion at the cost of the large-area reclamation (439.59 km2) from 2000 to 2005. The area percentage of open water is lower than 12%, while its percentage of ecosystem service value is between 39.2% and 47.6% during the past 15 years. Therefore, the decreasing area of open water leads to the declining of ecosystem service value in the study area.

Table 3. The construction comparison of LUCC and EVC

Land use type	1990年		2000		2005	
	area %	ESV%	area %	ESV%	area %	ESV%
Cultivated land	66.78	36.12	68.48	38.96	68.91	44.47
Forestland	8.08	13.81	7.65	13.76	6.82	13.92
Meadow	5.25	2.97	4.77	2.84	5.13	3.47
Open water	11.20	47.65	10.07	45.04	7.73	39.2
Residential area	4.13	-0.7	4.30	-0.77	6.23	-1.26
Unused land	4.56	0.15	4.75	0.16	5.18	0.2

5   Discussion and Conclusion

Through analyzing the land use land cover maps in 1990, 2000, and 2005 derived from Landsat TM imagery, we argued that the direct reason which leads to the decline of ecological service values is the land use and land cover change. The reasonability of the LUCC trend confined the total amount of the ecological services value. As a whole, the response of ecological services value to LUCC is passive. With the rapid economics development of the HaDaQi industrial corridor, more land resources are emergency needed. These lands would be changed from open water, forestland and grassland. Though the comparison of ecological services value in various land cover types, we could recognize the environmental importance of these open water, forestland and grassland. We argue that, in future land-use policy formulation, conservation of the open water and their resource rich ecosystems should take precedence over the uncontrolled reclamation of these areas for economic purposes. While it may not be feasible to stop all reclamation activities in this area, it is imperative that future land reclamation projects be controlled and based on rigorous environmental impact analyses.

References

1. Guo, Z., Xiao, X., Gan, Y., Zheng, Y.: Ecosystem functions, services and their values—a case study in Xingshan County of China. Ecological Economics 38, 141–154 (2001)
2. Zang, S.Y., Wu, C.S., Liu, Wu, C.S., Liu, H., Na, X.D.: Impact of urbanization on natural ecosystem service values: a comparative study. Environmental Monitoring and Assessment (2011), doi:10.1007/s10661-010-1764-1

3. Pearce, D., Moran, D.: The Economic Value of Biodiversity. IUCN, Cambridge (1994)
4. Zhao, B., Kreuter, U., Li, B., Ma, Z.J., Chen, J.K., Nakagoshi, N.: An ecosystem service value assessment of land-use change on Chongming Island, China. Land Use Policy 21, 139–148 (2004)
5. Munasinghe, M.: Economic and policy issues in natural habitats and protected areas. In: Munasinghe, M., Mc-Neely, J. (eds.) Protected Area Economics and Policy, IUCN, Cambridge (1994)
6. Molly, W.I., Shonda, G.F., Gilliland, F.: The value of ecosystem services provided by the U.S. National Wildlife Refuge System in the contiguous U.S. Ecological Economics 67, 608–618 (2008)
7. Costanza, R., d'Arge, R., de Groot, R., Farber, S., Grasso, M., Hannon, B., Limburg, K., Naeem, S., O'Neill, R.V., Paruelo, J., Raskin, R.G., Sutton, P., van den Belt, M.: The value of the world's ecosystem services and natural capital. Nature 387, 253–260 (1997)
8. Xie, G., Lu, C., Cheng, S.: Progress in evaluating the global ecosystem services. Resource Science 23(6), 5–9 (2001)
9. Xie, G., Lu, C., Leng, Y., Zheng, D., Li, S.: Ecological assets valuation of the Tibetan Plateau. Journal of Natural Resources 18(2), 189–196 (2003)

SecuRights

Ferhat Khenak

Pôle Technologies de l'Information et de la Communication pour l'Enseignement
Centre de Recherche sur l'Information Scientifique et Technique
Ben Aknoun, Algiers, Algeria
khenak@cerist.dz

Abstract. The technicality is no longer an obstacle; the issue of any environment of E-Learning (before) or V-Learning (now) is the production then the protection (in terms of security and confidentiality) of the content flowing through it. As part of our national policy of Visual Informatics For Education (VIFE), specifically for our Algerian V-Learning Network (AVN), which is a device of distributed interactive learning spread over all our vast territory according to a new concept based on the principle of the Online Video Learning via Internet and/or by Satellite; we have developed an encryption method enabling a certain security of copyrights. This paper discusses this method and presents its SecuRights system based on a distributed random algorithm.

Keywords: Visual Informatics, V-Learning, InterTvNet, SecuRights, VdoStat.

1 Introduction

Infrastructural, the Internet has become a world map of servers (cities), of cables (roads), of wireless (bridges), and of accessories (viabilities including parking). Systemically, it became a chain of information stations (new nuclear centrals, the nerves of the war) and of big motors (or giant gears of harvest, storage, processing and exploitation of information) that run 24/24 to irrigate the living things on earth (visible) and other (invisible) in the meaning of life from good to better, in principle...

What are these big machines actually do? In our humble understanding, is that everyone tries to take information from another without his consent (legally considered as a rape of privacy) and if possible to conceal hers. In other words, they are racing towards the quantitative and qualitative information [6] from each other and the best man win. It remains to know the rules that govern this race (if such rules exist), who creates and controls them. I know that nothing is sustainable in this world!

The question is: can we prevent someone from using our informational base today? The demonstrative answer which flowing from sense, has just been delivered to us last week (beginning March 2011) by this large-scale cyber attack to obtain information concerning the preparation of the G20, currently chaired by France, which has been squarely victim the French Foreign Affairs Ministry, which has suffered significant damage[7]. And whose spokesman considers just know that the origin of the attack is somewhere in China. This demonstrates the difficulty of the future to prevent a general war if unfortunately Internet goes mad as it was the English cow. I hope to be alive just to remind!

For our part, today even less than tomorrow, we are not able to shield the ports of our computers nor able to make the security keys of our systems inviolable. However, we have some ideas on how to plant the intruders who would be attracted by tourism in our systems. We have developed tools to make their task seriously tedious in terms of ratio: effort/result of the hacking. Indeed, we have created an info scholarship to measure (to estimate for now) the ratio of cost of (our) information hacked and efforts provided to resolve the difficulties to obtain it.

So, knowing that information published in its entirety on the Internet is quickly falsified (in 15 minutes), our encryption method is to segment and disperse information on several sites running randomly and dynamically to sow our prosecutors at least the medium term. The goal is to discourage many malicious intruders by making them run after a miniscule part of a mobile target. Based on this encryption method, the **SecuRight** system we will introduce in this paper is an example of our tools of security and confidentiality, implemented within our **Algerian V-Learning Network (AVN)** device.

2   Algerian V-Learning Network

The Algerian V-Learning Network (AVN) [4] operating principle is exactly the same as a national company that employs 500 permanents (direct) and 500 participants (indirect) with its very costly infrastructure and its qualified management five teams: 1- Technical: regulating, recording, assemblage, accommodation, broadcasting and streaming (T), 2- Pedagogical: restitution, accompaniment, self-government and self-evaluating (P), 3- Management: programming, inscription, monitoring and certification (G), 4- Marketing: promotion, awareness and adaptation (M), 5- Scientific-Validation: evaluation, innovation and normalization (V).

In many emergent countries, the distance between requirements and reality of quality assurance of higher education remains important [5]. In Algeria, although the policies are now well enough developed, practices still introduce serious insufficiency particularly in various regions of the vast Algerian territory. The AVN was conceived with a view to reduce this distance within reason. Its centralized organization allows distributing the content in an efficient and economic manner. In our Central Node, located at CERIST in Algiers, the infrastructure of the figure 1 below is the main focus (the server) of our InterTvNet of 77 endpoints [3].
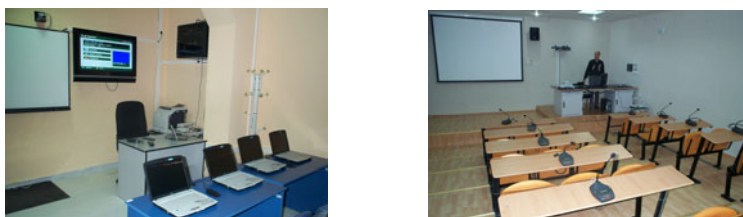
Fig. 1. Building of the QG, POLYCOM Cyber room, TANDBERG Cyber room [8]

The figure 2 next, shows our TV Studio, which is used for scientific debates, for preparing of teachers, and for content productions. On the second photo, we observe

the Governed of television for video editing. The third photo of this figure shows the multimedia station of assemblage.

Fig. 2. Studio of TV recording, Tray, State control, station of assemblage

3   SecuRights

The **SecuRights** system is a distributed random algorithm. Being an important module of our V-Learning concept (the third component of our national device of Tele-education) [2], its role is to maintain, as part of Algerian V-Learning Network (AVN), a certain level of vigilance in terms of security and confidentiality of data, information and knowledge of people [10], containers (hard) and content (software) [6], well knowing that computer security is completely random. Mr. Julian Paul Assange of Wikileaks knows something!

Thus, we are well aware that our SecuRights contributes only to mitigate online attacks just to plant the potential pursuers [11]. Therefore, our Strategy consists to develop original and private algorithms which should not be commercialized on a medium term. To secure the delivery of such contents, the idea is to fragment these contents with these algorithms before sending them, then to reconstruct them with these same algorithms after receiving them.

Develop methods to hide the random spread not only of the content but also and especially of the algorithm of security and confidentiality, is felt as an economic idea. SecuRights seeks to be a soft procedure of security used to protect the content [12] of our Algerian V-Learning Network device. Knowing in general, the natural recordings of courses that we produce in a V-Learning environment are not sustainable [1].

In support of our discussion, we provide an example of a simple algorithm called **Zsoft** and based on CTRL + Z command of Word we use to send distorted text [13] online. Taking the following: "**The rules for such occasions are simple: to be effective, they must be applied rigorously and methodically**". After 15 random modifications of deletion, addition and permutation, we get the distorted text as follows: "**hit rules for such occasions are suplet: to be effective, he must bit applied rigorously tand tehodicall**". Sent like this, it is not easy to guess the initial text. To rebuild it, simply open it with Word and apply 15 times the function equivalent to the CTRL + Z. The text is well reconstructed by one who knows. In practice, several hints are combined to make the task even more difficult for hackers.

The figures 3, 4, 5 below show the findings of the first 100% video-on-line program [9] for university courses, pedagogical exercises and self-evaluations of the AVN, which has been tested with success over the two past academic years.

Fig. 4. Examination from France Jury HEC (Paris) – Student (CERIST, Algiers)

Fig. 3. Doctoral School University (Béjaïa) – CERIST (Algiers)
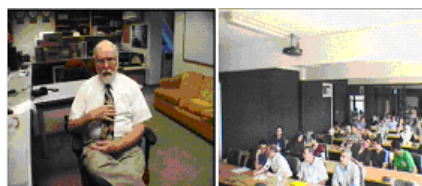
Fig. 5. Conference between Nasa (USA) – Béjaïa University (Algeria)

4   Conclusion

Gifted of a network 'InterTvNet', of a global scheme of order 'WhoDoWhat' and of a system 'SecuRights', this triptych concept is very economic for an education of mass (for more of pedagogic places), for a mutualisation of the quality teachers (for a better quality of education and tutoring), for a fairness between universities (for an equal opportunities) and for an openness to the world (for a better integration in world society of Information and Communication).

In spite of its high investment, the operation is not profitable for now, although the possibility to offer a complete training package via V-Learning concept by Internet and/or by satellite is a real need.

Unfortunately, the Economic Intelligence requires now more and more gray matter distributed according to a reliable, faithful and effective model of man-machine networking. That is to say, a model that fulfills its missions and tasks on safely and confidentially. Higher education and scientific research can not afford to escape to this obvious. But it is also undeniable that today the security and confidentiality of computer networks have not yet reached stability. Therefore, investment in the production of online content in education and training, particularly in underdeveloped countries including Algeria, now appears unprofitable and will have to wait!

In fact, for some, the theft on the Internet is considered as intelligence or as a contribution to the improvement of the Internet and any legal action against it is frowned upon and is not economical.

References

1. Khenak, F.: VDOSTAT. PACIIA2010: The 3rd International Conference on Computational Intelligence and Industrial Application, Wuhan (China), (December 4-5 (2010), http://www.paciia2010.org
2. Khenak, F.: V-Learning. CISIM2010: International Conference on Computer Information Systems and Industrial Management Applications, Cracow (Poland), October 8-10 (2010), http://www.mirlabs.org/cisim10/
3. Khenak, F.: InteTvNet. ITSIM2010: International Symposium on Information Technology, Kuala Lumpur (Malaysia), June 15-17 (2010), http://www.itsim.org/program.htm
4. Khenak, F.: Algerian V-Learning Network. ICT2010: The 17th International Conference on Telecommunications, Doha (Qatar), April 4-7 (2010), http://www.ict2010.org/docs/ICT2010-Detailed-Final-Program.pdf
5. Khenak, F.: REV Algérien. ICT2009: 2nd AFRA Conference on the Role of Information and Communication Technologies in Nuclear Science and Technology Training, Cape Town (South Africa), November 16-17 (2009), http://www.capegateway.gov.za/other/2009/9/invitation_08-09.pdf
6. Khenak, F.: Teaching by an Intermedia medium, towards a pocket school. In: M2E2 1998: IEEE International Conference on Multi-Media Engineering and Education, Hong Kong (China), July 7-9 (1998)
7. Tourancheau, P.: Attaque informatique. Info Libé: l'Elysée et le Quai d'Orsay également piratés... tout l'appareil d'Etat français en relation avec le G20 qui a été hacké. Une opération probablement menée par un pays asiatique, Paris (France), March 7 (2011), http://www.liberation.fr/economie/01012324191-attaque-informatique-l-elysee-et-le-quaid-orsay-egalement-pirates
8. Polycom and Tandberg Stations in our Central Node, located at CERIST in Algiers: the infrastructure of our InterTvNet of 77 endpoints, Algiers (Algeria), December 15 (2008), http://www.polycom.com, http://www.polycom.com
9. Dillenbourg P.: La fin du e-Learning ? Visioconférence : 4ème édition du forum des TIC sur le thème Convergence et éthique : de nouveaux enjeux pour les environnements numériques de travail, Charleroi (Belgique), June 6 (2009), http://www.educnet.education.fr/dossier/eformation/e-formation-e-learning/la-fin-du-e-learning
10. Ferraiolo, H., Newton, E.: Personal Identity Verification Program. Cyber Maryland Summit, held at the National Institute of Standards and Technology, Gaithersburg (Maryland), January 11 (2010), http://csrc.nist.gov/cyber-md-summit/
11. Contribution of Wikipedia: Information Security. Wikipedia: Free Encyclopaedia, January 13, 2007 as of 4:30PM MST USA, http://en.wikipedia.org/wiki/Information_security
12. University of Miami Leonard M. Miller School of Medicine: Confidentiality, Integrity and Availability (CIA). Learn About: Educational Content, Miami (USA) (1997 - 2008), http://it.med.miami.edu/x904.xml
13. Peltier, T.R.: Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach publications, Boca Raton, FL (2002) ISBN 0-8493-1137-3
14. Dhillon, G.: Principles of Information Systems Security: text and cases. John Wiley & Sons, NY (2007)

Nonlinear Frequencies for Transverse Oscillations of Axially Moving Beams: Comparison of Two Models

Yao Yuju[1], Zhang Jiguang[1,3], Xiang Yingchang[1], Meng Liyuan[2], and Ding Hu[3]

[1] Rizhao Polytechnic, Shandong 276826, China
[2] Tongji university, Shanghai 200092, China
[3] Shanghai institute of Applied Mathematics and Mechanics,
Shanghai 200072, China
{Yaoyuju,xiangyingchang}@sina.com
{zhangjiguang2005,dinghu3}@163.com

Abstract. The fast Fourier transform (FFT) algorithm is commonly used to derive the power density spectrum of scattered point data in the frequency domain. The standard fast Fourier transform is used to investigate the natural frequencies of nonlinear free transverse oscillations of axially moving beams. The transverse motion of an axially moving beam can be governed by a nonlinear partial-differential equation or a nonlinear integro-partial-differential equation. Numerical schemes are respectively presented for the two governing equations via the differential quadrature method under the fixed boundary condition. For each nonlinear equation, the natural frequencies of axially moving beams are investigated via the fast Fourier transform with the time responses of the transverse vibration. The numerical results illustrate the tendencies of the natural frequencies of nonlinear free transverse vibration of axially moving beams with the changing vibration amplitude, axially moving speed, the nonlinear coefficient and the flexural stiffness.

Keywords: Axially moving beams, Nonlinearity, oscillations, Natural frequency, The fast Fourier transform, The differential quadrature.

1 Introduction

The axially moving structures have received a great deal of attention due to their manifestation in a wide class of engineering fields. The belt drives, power transmission band, band saw blades, and high-speed magnetic tapes are the typical examples of such axially moving structures. Most of the one-dimensional structures with flexural rigidity, which are axially moving over two supports, have been represented by the beam models. Understanding transverse vibrations of axially moving beams is important for the design of the devices.

The wide diffusion of axially moving systems in industrial processes has motivated intense research activity. Mote [1] first investigated the first three frequency and modes for simple supported boundary conditions via the Galerkin method. Wickert and Mote [2] presented a complex model method for axially moving continua including beams where natural frequencies and modes associated with free vibration

serve as a basis for analysis. Öz and Pakdemirli [3] and Öz [4] computed the first two natural frequencies values in the cases of pinned-pinned ends and clamped-clamped ends, respectively. Kong and Parker [5] combined perturbation techniques for algebraic equations and phase closure principle to determine approximate natural frequencies of an axially moving beam with small flexural stiffness. Ding and Chen [6] gave the first two frequencies of axially moving elastic and viscoelastic beams on simple supports with torsion springs. Ghayesh and Khadem [7] calculated natural frequency for the first two modes in free non-linear transverse vibration of an axially moving beam in which rotary inertia and temperature variation effects have been considered. Matbuly et al. [8] employed the method of differential quadrature to determine the natural frequencies and the mode shapes for the free vibration of an elastically supported cracked beam. Özkaya et al. [9] investigated natural frequencies for a slightly curved beam carrying a concentrated mass. All of above literatures, the natural frequency of axially moving beams was calculated from linear governing equation of transverse vibration. The known exception is that Wickert [10] used a perturbation method to investigate the fundamental frequency of axially moving materials from a nonlinear integro-partial-differential equation of transverse vibration. However, so far there are very limited researches on the first few natural frequencies of nonlinear vibration. To address the lacks of research in this aspect, the present investigation studies the first two natural frequencies of nonlinear free transverse vibration of axially moving beams via the numerical solutions and the FFT.

2 Mathematical Models

Consider a uniform beam is moving in its axial direction at a uniform constant transport speed of γ between two boundaries. The span between two boundaries is l. The structural properties of the beam are given by the mass density ρ, the cross-sectional area A, the moment of inertial I, the initial tension P0, and the Young's modulus E. Assume the beam has small amplitude vibrations in the axial and transverse directions. For a slender beam, the linear moment-curvature relationship is sufficiently accurate. The fixed axial coordinate x measure the distance from the left boundary. The transverse displacement v(x,t) related to a spatial frame. The beam is subjected to no external loads. The nonlinear the partial-differential equation and the integro-partial-differential equation for transverse motion of axially moving elastic beam can be cast into the dimensionless form [11]

$$v_{,tt} + 2\gamma v_{,xt} + \left(\gamma^2 - 1\right)v_{,xx} + k_{\mathrm{f}}{}^2 v_{,xxxx} = \frac{3}{2}k_1^2 v_{,x}{}^2 v_{,xx} \tag{1}$$

and

$$v_{,tt} + 2\gamma v_{,xt} + \left(\gamma^2 - 1\right)v_{,xx} + k_{\mathrm{f}}{}^2 v_{,xxxx} = \frac{1}{2}k_1^2 v_{,xx} \int_0^1 v_{,x}{}^2 \, \mathrm{d}x \tag{2}$$

where a comma preceding *x* or *t* denotes partial differentiation with respect to *x* or *t*, and The dimensionless variables and parameters as follows

$$v \leftrightarrow \frac{v}{l}, \ x \leftrightarrow \frac{x}{l}, \ t \leftrightarrow t \sqrt{\frac{P_0}{\rho A l^2}}, \gamma \leftrightarrow \gamma \sqrt{\frac{\rho A}{P_0}}, \ k_1 = \sqrt{\frac{EA}{P_0}}, \ k_f = \sqrt{\frac{EI}{P_0 l^2}} \qquad (3)$$

In the present investigation, only the boundary conditions of the beam is fixed at both ends are considered as follows

$$v(0,t) = v(1,t) = 0, \ v_{,x}(0,t) = v_{,x}(1,t) = 0 \qquad (4)$$

In this paper, the natural frequencies of nonlinear transverse vibration of an axially moving beam are focused on.

3   Numerical Methods

In the following investigation, the differential quadrature method [11] is applied to calculate time responses of transverse vibration from equations (1) and (2) under fixed boundary conditions (4).

Introduce N unequally spaced sampling points as

$$x_i = \frac{1}{2}\left[1 - \cos\frac{(i-1)\pi}{N-3}\right], \quad (i = 3, 4, \ldots, N-2) \qquad (5)$$

$$x_1 = 0, x_2 = 0.0001, x_{N-1} = 1 - 0.0001, x_N = 1$$

The quadrature rules for the derivatives of a function at the sampling points yield

$$v_{,x}(x_i,t) = \sum_{j=1}^{N} A_{ij}^{(1)} v(x_j,t), \ v_{,xx}(x_i,t) = \sum_{j=1}^{N} A_{ij}^{(2)} v(x_j,t), \ v_{,xxxx}(x_i,t) = \sum_{j=1}^{N} A_{ij}^{(4)} v(x_j,t) \qquad (6)$$

where the weighting coefficients are as follows

$$A_{ij}^{(1)} = \frac{\prod\limits_{k=1,k\neq i}^{N}(x_i - x_k)}{(x_i - x_j)\prod\limits_{k=1,k\neq j}^{N}(x_j - x_k)} \quad (i, j = 1, 2, \cdots, N; \ j \neq i) \qquad (7)$$

and the recurrence relationship

$$A_{ij}^{(r)} = r\left[A_{ii}^{(r-1)}A_{ij}^{(1)} - \frac{A_{ij}^{(r-1)}}{x_i - x_j}\right] \quad (r = 2,3,4,5; i, j = 1,2,\cdots,N; \ j \neq i) \qquad (8)$$

$$A_{ii}^{(r)} = -\sum_{k=1,k\neq i}^{N} A_{ik}^{(r)} \quad (r = 1,2,3,4,5; i = 1,2,\cdots,N) \qquad (9)$$

The weighting coefficients Ig (g=1,2,…,N) for integrals are solved from [11]

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ x_1 & x_2 & \cdots & x_{N-1} & x_N \\ \vdots & \vdots & & \vdots & \vdots \\ x_1^{N-2} & x_2^{N-2} & \cdots & x_{N-1}^{N-2} & x_N^{N-2} \\ x_1^{N-1} & x_1^{N-1} & \cdots & x_{N-1}^{N-1} & x_N^{N-1} \end{pmatrix}\begin{pmatrix} I_1 \\ I_2 \\ \vdots \\ I_{N-1} \\ I_N \end{pmatrix} = \begin{pmatrix} 1 \\ 1/2 \\ \vdots \\ 1/(N-1) \\ 1/N \end{pmatrix} \qquad (10)$$

Substitution of Eq. (6) and Ig into Eqs. (1) and (2) and boundary condition (4) makes v(xi,t) solvable for a set of given parameters kf, γ, k1, initial conditions. In this way, equation (1) or (2) can be solved numerically. For an odd N, v(x(N+1)/2,t) is the beam center displacement.

4 The Natural Frequencies of Nonlinear Models

In all numerical examples here, the initial conditions are chosen as second eigenfunction of a stationary beam under the fixed boundary conditions, namely

$$v(x,0) = D\left\{\cosh(\beta_1 x) - \cos(\beta_1 x) + \zeta_1\left[\sin(\beta_1 x) - \sinh(\beta_1 x)\right]\right\}, v_{,x}(x,0) = 0 \qquad (11)$$

Where

$$\zeta_1 = \frac{\cosh\beta_1 - \cos\beta_1}{\sinh\beta_1 - \sin\beta_1}, \quad \beta_1 = 7.8532 \qquad (12)$$

and D represents the amplitude of vibration. The transverse displacement of the beam center for equations (1) and (2) will be numerically solved via the differential quadrature schemes under the boundary conditions (4) and the initial conditions (12).

The Fourier transform has been widely used in circuit analysis and synthesis, from filter design to signal processing and image reconstruction. The principle of transform in engineering is to find a different representation of a signal under investigation. The discrete Fourier transform (DFT) is an approximation of the Fourier transform in a digital environment for computing the Fourier transform numerically on a computer. The FFT is an algorithm to speed up DFT computation. The maximum frequency in the FFT depends on the sampling interval, and the frequency resolution is determined by the record length of the signal. That is, N samples of a time signal recorded during a finite duration of T with a sampling period of Δt ($N=T/\Delta t$) can be transformed into N samples in the frequency domain. In the present investigation, the natural frequencies of the nonlinear transverse vibration of axially moving beams are calculated from the time signals of the transverse center displacement the of beam via the FFT, and $N=4096$, $\Delta t=0.025$.

Consider a beam with modulus of elasticity $E=2.1\times10^{11}$ Pa and density $\rho=7850$ kg/m^3. Let the initial tension $P_0=7850$ N, the axial speed $\gamma=51.72$ m/s, and the cross-section of the beam being a rectangle with the width $W=0.0135$ m and the height $H=0.0277$ m. Then equation (3) yields $\gamma=1.0$, $k_f=0.8$, $k_1=100$. As k_1 represents the effect of nonlinearity, it is called the nonlinear coefficient.

Figs.1 and 2 respectively illustrate the effects of the nonlinear coefficient with $k_f=0.8$ and the vibration amplitude $D=0.0001$ on the first two natural frequencies of Eq. (1) and Eq. (2) versus axial speed. In Figs.1 and 2, the dash-dot lines, the solid lines and the dots respectively stand for the natural frequencies to $k_1=2000$, $k_1=100$ and $k_1=0$. The nonlinear coefficient $k_1=0$, means the natural frequencies are calculated from the linear elastic system. For the given k_1, the natural frequencies decrease with the growth of axial speed. The comparisons also indicate that the nonlinear coefficient k_1 has little effects on the natural frequency when vibration is rather small, especially for the small axial speed and the first natural frequency, even if the nonlinear coefficient rather large.
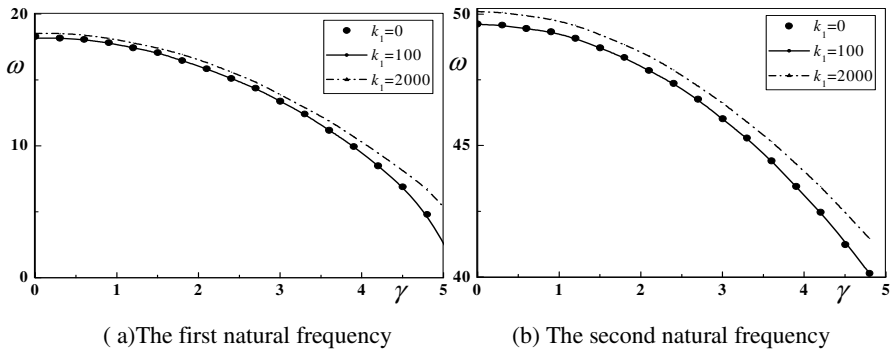
(a)The first natural frequency   (b) The second natural frequency

Fig. 1. The effects of the nonlinear coefficient on the natural frequencies versus axial speed: Eq. (1)

(a)The first natural frequency   (b) The second natural frequency
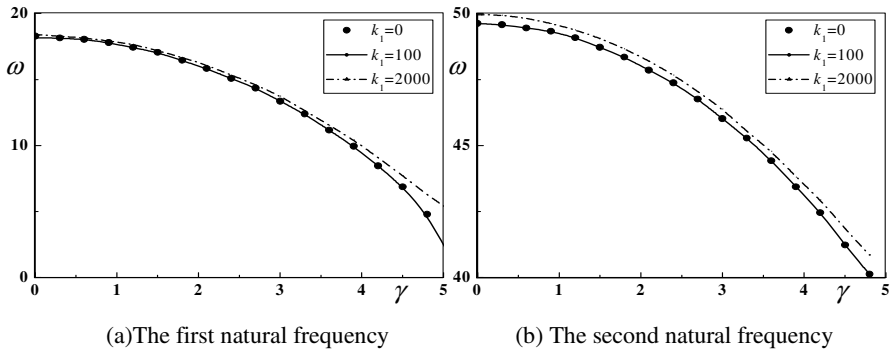
Fig. 2. The effects of the nonlinear coefficient on the natural frequencies versus axial speed: Eq. (2)

5   Comparisons

Based on numerically solutions of the (1) and (2), the differences between the two nonlinear models can be investigated via the first two natural frequencies of equations by the FFT.

Fig.3 illustrates the natural frequencies versus axial speed with fixed the flexural stiffness k_f=0.6, k_f=0.8 and k_f=1.0 respectively and the nonlinear coefficient k_1=100, the vibration amplitude D=0.0001. Fig.3 shows that the natural frequencies of two models are overlapped with the changing axial speed γ and flexural stiffness k_f for rather small vibration. The numerical results demonstrate that the flexural stiffness the axial speed has little effects on the different of the natural frequency of the two nonlinear models when the vibration is rather small. Figs.4 and 5 respectively illustrate the natural frequencies versus nonlinear coefficient and vibration amplitude with fixed the flexural stiffness k_f=0.8 and the axial speed γ=1.0. In Fig.4, the vibration amplitude D=0.0001. In Fig.5, the nonlinear coefficient k_1=100. The comparisons indicate that the natural frequencies of two models qualitatively predict the same tendencies with the changing nonlinear coefficient and vibration amplitude,

while quantitatively, there are certain differences for really big nonlinear coefficient and rather large vibration, the difference increase with the nonlinear coefficient and vibration amplitude, and the natural frequencies from equation (2) are smaller to those from equation (1).

(a) The first natural frequency   (b) The second natural frequency
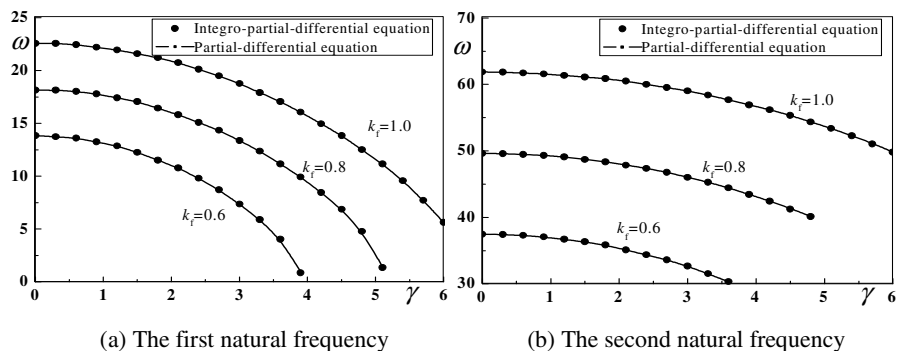
Fig. 3. The natural frequency calculated from equations (1) and (2) versus axial speed

(a) The first natural frequency   (b) The second natural frequency
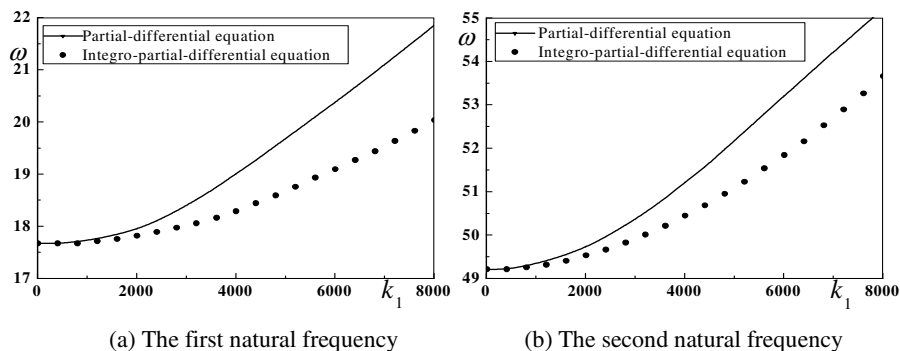
Fig. 4. The natural frequency calculated from equations (1) and (2) versus nonlinear coefficient

(a)The first natural frequency   (b) The second natural frequency
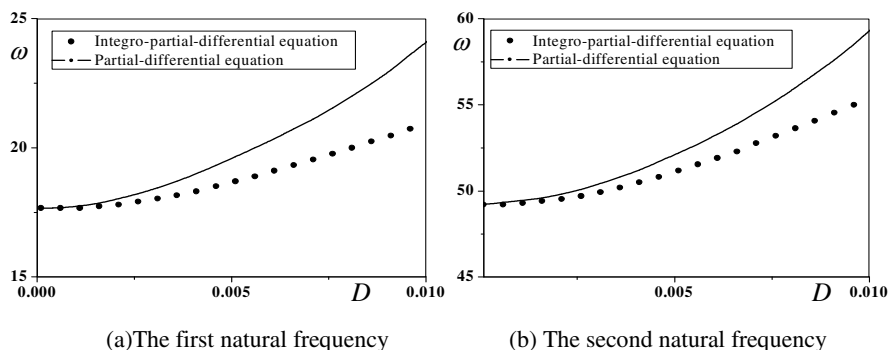
Fig. 5. The natural frequency calculated from equations (1) and (2) versus vibration amplitude

6   Conclusions

Natural frequencies of nonlinear free oscillations of axially moving elastic beams are numerically investigated via the differential quadrature method and the fast Fourier transform. The transverse motion of an axially moving beam can be governed by a nonlinear partial-differential equation or a nonlinear integro-partial-differential equation. The time histories of transverse displacements of the centre of axially moving beams are respectively solved via the differential quadrature scheme for the two nonlinear models under the fixed boundary. The FFT is a computational tool for efficiently calculating the discrete Fourier transform of a series of data samples by means of digital computers. Time series of the discrete Fourier transform is defined as numerically solutions of two nonlinear governing equations. The standard fast Fourier transform is used to investigate the natural frequencies of nonlinear free transverse vibration of axially moving beams. The investigation leads to the following conclusions: (1) The nonlinear coefficient has little effects on the first two natural frequencies of nonlinear vibration of axially moving beams for rather small vibration, and the first two natural frequencies increase with the nonlinear coefficient for the large vibration. (2) The first two natural frequencies increase with the flexural stiffness and the vibration amplitude and decrease with the axially speed. (3) The two nonlinear models predict the same tendencies of the first two natural frequencies with the changing flexural stiffness, axially speed, nonlinear coefficient and vibration amplitude. (4) The nonlinear partial-differential equation leads to the bigger natural frequency for big nonlinear coefficient and rather large vibration and this difference increase with nonlinear coefficient.

References

1. Mote Jr., C.D.: Dynamic stability of an axially moving band. Journal of the Franklin Institute 285, 329–346 (1968)
2. Wickert, J.A., Mote Jr., C.D.: Classical vibration analysis of axially moving continua. ASME Journal of Applied Mechanics 57, 738–744 (1990)
3. Öz, H.R., Pakdemirli, M.: Vibrations of an axially moving beam with time dependent velocity. Journal of Sound and Vibration 227, 239–257 (1999)
4. Öz, H.R.: On the vibrations of an axially traveling beam on fixed supports with variable velocity. Journal of Sound and Vibration 239, 556–564 (2001)
5. Kong, L., Parker, R.G.: Approximate eigensolutions of axially moving beams with small flexural stiffness. Journal of Sound and Vibration 276, 459–469 (2004)
6. Ding, H., Chen, L.Q.: Stability of axially accelerating viscoelastic beams multi-scale analysis with numerical confirmations. European Journal of Mechanics A/Solids 27, 1108–1120 (2008)
7. Ghayesh, M.H., Khadem, S.E.: Rotary inertia and temperature effects on non-linear vibration, steady-state response and stability of an axially moving beam with time-dependent velocity. International Journal of Mechanical Sciences 50, 389–404 (2008)

8. Matbuly, M.S., Ragb, O., Nassar, M.: Natural frequencies of a functionally graded cracked beam using the differential quadrature method. Applied Mathematics and Computation 215, 2307–2316 (2009)
9. Özkaya, E., Sarigul, M., Boyaci, H.: Nonlinear transverse vibrations of a slightly curved beam carrying a concentrated mass. Acta Mechanica Sinica 25, 871–882 (2009)
10. Wickert, J.A.: Non-linear vibration of a traveling tensioned beam. International Journal of Non-Linear Mechanics 27, 503–517 (1992)
11. Ding, H., Chen, L.Q.: On two transverse nonlinear models of axially moving beams. Science in China E 52, 743–751 (2009)

Convergence of Upper and Lower Bounds
on the Bayes Error

Xiang Yingchang[1], Zhang Jiguang[1], Chen Dechang[2], and Michael A. Fries[3]

[1] Rizhao Polytechnic, Shandong 276826, China
xiangyingchang@sina.com
[2] Department of Natural and Applied Sciences,
University of Wisconsin, Green Bay, WI 54311, USA
zhangjiguang2005@163.com
[3] School of Computer Science, Telecommunications and
Information Systems DePaul University, Chicago, IL 60604, USA
chend@uwgb.edu, mfries@cti.depaul.edu

Abstract. The convergence behaviors of the arbitrarily tight upper and lower bounds on the Bayes error are obtained. It implies that these bounds will become arbitrarily close to the Bayes error very quickly, as α increases. A much stronger result is derived.

Keywords: Bayes error, convergence behavior, oscillation upper and lower bounds.

1 Introduction

This chapter studies the convergence behavior of the arbitrarily tight upper and lower bounds on the Bayes error proposed by Avi-Itzhak and Dizep [1]. We show that bounds converge to the Bayes error uniformly with a vary fast convergence rate.

2 Mathematical Models

Conisder the pattern recognition problem of two classes C_1 and C_2. Suppose for class C_i the prior probability is π_i and the probability density function is $f_i(x)$. It is know in classifying C_1 and $C2$,the bayes error, denoted by $P(e)$, is

$$P(e) = \int_x \min(p, 1-p) f(x) dx \tag{1}$$

Where $p = \mathrm{Prob}(C_1|x)$, $f(x) = \pi_1 f_1(x) + \pi_2 f_2(x)$.

Due to the term $\min(p,1\text{-}p)$, theoretical evaluation of $P(e)$ may become impossible. Thus it is interesting to find elementary functions bounding $\min(p,1\text{-}p)$, from which the corresponding bounds on $P(e)$ will de derived. Avi-Itzhak and Diep[1] introduced the following upper and lower bounds for $P(e)$:

$$\int_x L_\alpha(p) f(x) dx \leq P(e) \leq \int_x U_\alpha(p) f(x) dx \tag{2}$$

Where for any $\alpha > 0$ and $p \in [0, 1]$,

$$L_\alpha(p) = \frac{1}{\alpha} \ln \left[\frac{1 + e^{-\alpha}}{e^{-\alpha p} + e^{-\alpha(1-p)}} \right] \leq \min(p, 1-p) \qquad (3)$$

and

$$U_\alpha(p) = L_\alpha(p) + \left[1 - 2L_\alpha\left(\frac{1}{2}\right) \right] C(p) \geq \min(p, 1-p) \qquad (4)$$

In(4), $C(p)$ is any bounded function satisfying

$$\begin{cases} C(p) \geq \min(p, 1-p) \quad \text{for all } p \in [0,1] \\ C(p) = C(1-p) \quad \text{for all } p \in [0,1] \\ C(0) = C(1) = 0, \quad C\left(\frac{1}{2}\right) = \frac{1}{2} \end{cases} \qquad (5)$$

Examples of function $C(p)$ include the Bhattacharyya bound $\sqrt{p(1-p)}$ ([5]), the equivocation bound $0.5[-p\log_2(p)-(1-p)\log_2(1-p)]$ ([4]), the Bayesian distance bound $2p(1-p)$ ([2]), and the Gaussian-Sinusoidal bound $0.5\sin(\pi p)\exp[\alpha(p-0.5)^2]$ ([3]).These bounds were introduced as the upper bound of $\min(p,1-p)$.

Avi-Itzhak and Diep[1] claimed that $\int_x L_\alpha(p)f(x)dx$ and $\int_x L_\alpha(p)f(x)dx$ can be arbitrarily tight by showing $\lim_{\alpha \to \infty} L_\alpha(p) = \min(p,1-p)$ and $\lim_{\alpha \to \infty} U_\alpha(p) = \min(p,1-p)$. In this paper, we provide a much stronger result in support of their claim .We show the following inequalities hold for any $\alpha > 0$.

$$0 \leq P(e) - \int_x L_\alpha(p)f(x)dx \leq \frac{2M \ln 2}{\alpha} \qquad (6)$$

$$0 \leq \int_x U_\alpha(p)f(x)dx - P(e) \leq \frac{2M \ln 2}{\alpha} \qquad (7)$$

Where $M = \sup_{p \in [0,1]} C(p)$.

Therefore as $\alpha \to \infty$ both $\int_x L_\alpha(p)f(x)dx$ and $\int_x L_\alpha(p)f(x)dx$ converge to $P(e)$ uniformly with a convergence rate $O(1/\alpha)$. This fact implies that these bounds will become arbitrarily close to the Bayes error very quickly, as α increases.

3 Proof of (6) and (7)

By the definition of $L_\alpha(p)$ and $U_\alpha(p)$, we have

$$U_\alpha(p) - L_\alpha(p) = \left[1 - 2L_\alpha\left(\frac{1}{2}\right)\right]C(P)$$

$$\leq \left[1 - \frac{2}{\alpha}\ln\left(\frac{1 + e^{-\alpha}}{2e^{-\alpha/2}}\right)\right]M$$

$$= \frac{2M}{\alpha}\ln\left(\frac{2}{1 + e^{-\alpha}}\right)$$

$$\leq \frac{2M}{\alpha}\ln 2$$

(8)

Using the above estimate and fact that $L_\alpha(p) \leq \min(p, 1-p) \leq U_\alpha(p)$, one has

$$0 \leq \min(p, 1-p)f(x) - L_\alpha(p)f(x) \leq \frac{2M\ln 2}{\alpha}f(x) \tag{9}$$

and

$$0 \leq U_\alpha(p)f(x) - \min(p, 1-p)f(x) \leq \frac{2M\ln 2}{\alpha}f(x) \tag{10}$$

Integrating with respect to x yields

$$0 \leq \int_x \min(p, 1-p)f(x)dx - \int_x L_\alpha(p)f(x)dx \leq \frac{2M\ln 2}{\alpha}f(x) \tag{11}$$

and

$$0 \leq \int_x U_\alpha(p)f(x)dx - \int_x \min(p, 1-p)f(x)dx \leq \frac{2M\ln 2}{\alpha}f(x) \tag{12}$$

Now (6) and (7) follow the equation (1), (12) and (13) and fact that $\int_x f(x)dx = 1$.

References

1. Avi-Itzhak, H., Dipe, T.: Arbitrarily tight upper and lower bounds on the Bayesian probability of error. IEEE Trans. Patter Analysis and Machine Intelligence 18(1), 89–91 (1996)
2. Devijver, P.A.: On a new class of bounds on Bayes risk in multihypoth-esis pattern recorgnition. IEEE Trans. Computer, 70–80 (1974)
3. Hashlamoun, W.A., Varshney, P.K., Samarasooriya, V.S.: Atight upper bound on the Bayesian probability of error. IEEE Trans. Pattern Analysis and Machine Intelligence 16, 220–224 (1994)
4. Helloman, M.E., Raviv, J.: Probability of error, equivocation, and Chenoff bound. IEEE Trans. Information Theory 16, 368–372 (1970)

5. Kailath, T.: The divergence and Bhattacharyya distance measures insignal selection. IEEE Trans. Communication Technology 15, 52–60 (1967)
6. Vajda, I., Vašek, K.: Majorization, concave entropies and comparison of experiments. Problems of Control and Information Theory 14, 105–115 (1985)
7. Maley, C.C., Galipeau, P.C., Finley, J.C., et al.: Ecological Diversity Measures Predict Cancer Prograssion In Barrett's Esophagus. Gastroenterology 131, 672–673 (2006)
8. Horáček, M.: Míry biodiverzity a jejich aplikace (Measures of biodiversity and their applications.) Master thesis. Prague, Charles University. Supervisor J. Zvárová (2009)

Research on Evaluation of Scheduling Algorithms for TS Multiplexers Based on GSPN[*]

Cheng-An Zhao and Chunlai Zhou

Information Engineering College, Communication
University of China, Beijing 100024, China
zhaochengan@gmail.com, clzhou@cuc.edu.cn

Abstract. In this paper, we studied performance evaluation of scheduling algorithms for MPEG-2 TS multiplexer in digital television systems using formal method. We presented a general framework for modeling and analyzing multiplexing architecture of MPEG-2 TS multiplexer using generalized stochastic petri net (GSPN), and then evaluated constant bit rate (CBR) algorithm, first come first serve (FCFS) algorithm, queue length threshold (QLT) algorithm, and longest queue first (LQF) algorithm by analyzing throughput, delay and fairness of them based on the proposed model. We evaluated the fairness of scheduling algorithms by introducing coefficient of variation (CV). Our results show that CBR algorithm is poor in all aspects of performance. Although FCFS algorithm has a smaller time delay of system, its fairness is not good. LQF algorithm has the nice fairness, but its time delay is great when total input rate is higher than output rate. QLT algorithm is comparatively well balanced in all respects.

Keywords: TS multiplexer, scheduling algorithm, GSPN, VBR.

1   Introduction

In present digital television systems, the video and audio programs are encoded using the MPEG-2 standard. In order to improve the quality of programs, the video programs are compressed into variable bit rate (VBR) streams. However, if the VBR streams are transmitted in the services adopted the constant bit rate (CBR), either delay jitter or bandwidth wastage may occur. So each stream ought to be dynamically allocated demanded bandwidth to decrease delay jitter and bandwidth wastage when VBR streams are multiplexed to share the fixed channel bandwidth. To satisfy this requirement, it is imperative to study the available and effective scheduling algorithm in the multiplexer. Generalized stochastic petri net (GSPN), which is an extension of petri net, is a powerful formal tool for performance evaluation and scheduling problem. In this paper, we present a general framework for modeling and analyzing multiplexing architecture of MPEG-2 TS multiplexer using GSPN, and evaluate the usual scheduling algorithms in the TS multiplexer. We also give a GSPN model for

---

VBR source which is considered as a two-state markov modulated poisson process (MMPP) source. We evaluate the fairness of scheduling algorithms by introducing coefficient of variation (CV).

The rest of this paper is organized as follows. The overview of the multiplexing architecture for MPEG-2 TS multiplexer and problem statement are explained in detail in Section II. The GSPN modeling and analysis for the scheduling algorithms are discussed in Section III. Some numerical results are given in Section IV. Finally, some conclusions are given in section V.

2   Problem Overview

The details of the MPEG-2 system layer can be found in the ISO/IEC 13818 specification [1]. In this paper, we focus on the transport stream (TS) multiplexer. There are two phases of multiplexers, as shown in Fig.1. The first phase multiplexer carries on multiplexing several packetized elementary streams (PES) of a MPEG-2 program or data into a single-program TS. Because the MPEG-2 encoder compresses a video program at a constant frame rate, e.g., 24 frames/sec for PAL, these frames have different size for each other. So the output coded streams have variable bit rate (VBR). The coded VBR streams then are multiplexed by the first phase multiplexer. Because the processing time is nearly constant for each input frame, the output TS of the first phase multiplexer is still VBR with a constant frame rate [2][3].The second phase multiplexer carries on multiplexing several single program TS and private data into a single TS with multiple MPEG-2 programs. Our study focuses on the second phase multiplexer.
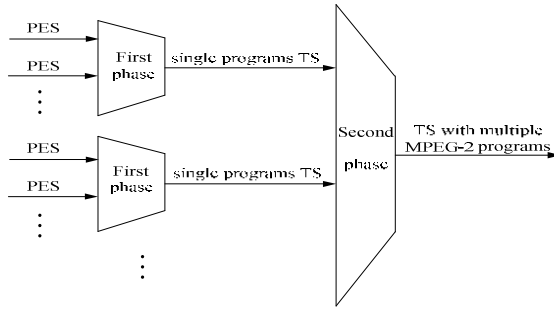
Fig. 1. Structure of two-phase multiplexer

One of problems for the second phase multiplexer is how to find a method that can allocate sub-bandwidth dynamically for each input stream to meet the need of each input stream depending upon the total bandwidth [3]. This allocation should realize that all input streams share the total output bandwidth adaptively to prevent the deadline violation and to improve the utilization of the bandwidth. In order to solve the above problem, it is necessary to study a feasible and effective scheduling algorithm for the second phase multiplexer. Reference [2] analyzed a timestamp-insensitive CBR scheduling algorithm, and presented a timestamp-sensitive

scheduling algorithm for MPEG-2 TS multiplexers, and improved the proposed algorithm by adding a scheme to prevent buffer underflow and overflow in multiplexers and set-top-boxes. In [3], the authors introduced a concept of scheduling matrix, and presented CBR scheduling algorithm and VBR scheduling algorithm based on the scheduling matrix.

In fact, from the standpoint of implementation, especially hardware implementation, the multiplexing architecture of multiplexer is shown in fig.2. TS packets of each program are respectively transferred into input buffers which usually is FIFO queue. Every time the scheduler must select a single TS packet from among those packets of all the input queues, and transmit it to the output buffer which also are FIFO queue. At last the TS packets of output buffer are sent out. Obviously, this multiplexing architecture can be considered as a queuing model. For evaluating the scheduling algorithms, it is necessary to analyze the queuing model of TS multiplexer using queuing theory. GSPN, as a graphical and mathematical modeling tool, can effectively describe and analyze a variety of queuing models. The usual scheduling algorithms in the TS multiplexer include CBR algorithm, FCFS algorithm, QLT algorithm, and LQF algorithm. The timestamp-insensitive CBR algorithm and the VBR algorithm described respectively in reference [2][3] are essentially LQF algorithm. In this paper, we model multiplexing architecture of TS multiplexer by means of GSPN, and evaluate throughput, delay and fairness of these algorithms.
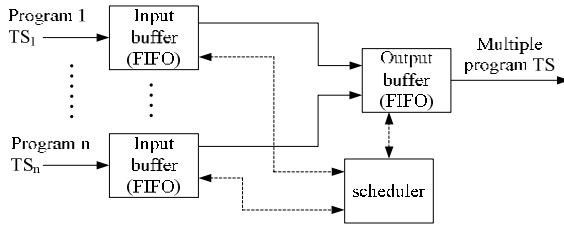
Fig. 2. The multiplexing architecture of multiplexer

3   Modeling

Due to space limitations, we don't introduce GSPN. The definition and details of the GSPN theory can be found in [4] and [5].

3.1   Model Description

We assume that a TS multiplexer in which time is divided into discrete intervals of fixed length known as slots. The time required to transmit each TS packet corresponds to the length of a slot.

The GSPN model of multiplexing architecture is shown in fig.3. A token in GSPN model denotes a TS packet.
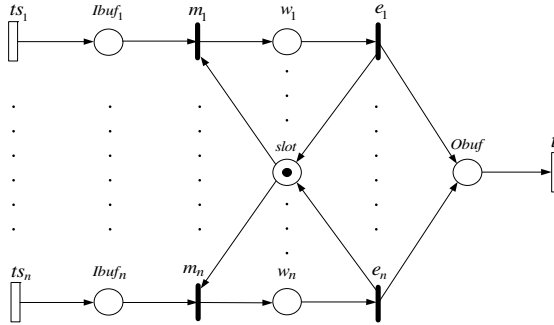
Fig. 3. GSPN model of multiplexing architecture

The transitions and places shown in Fig.3 are described below:

$i \in [1,n]$ in the following description.

ts_i is a timed transition, which is a VBR source of TS packets from program i.

$Ibuf_i$ is a place, which is the input buffer of program i, it's a FIFO queue. Its capacity is b_I tokens when the enabling rule of ts_i is $M(Ibuf_i) <b_I$, where $M(Ibuf_i)$ denotes the number of tokens in the place $Ibuf_i$. Similarly hereinafter.

m_i is a immediate transition which models TS packet processing. When it fires, a TS packet of program i is transferred to place w_i. The enabling priority of m_i is equal each other. The various enabling rules of m_i can reflect the various scheduling algorithms.

w_i is a place which models processing status of TS packet. Its capacity is one token.

e_i is a immediate transition which models TS packet processing. When it fires, a TS packet of program i is transferred to place $Obuf$.

$Obuf$ is a place, which is the output buffer, it's a FIFO queue. Its capacity is b_O TS packets when the enabling rule of e_i is $M(Obuf) <b_O$.

t is a timed transition, which models TS packet transmission. When it fires, a TS packet is sent out. Its rate is associated with μ.

$slot$ is a place, which includes one token in the initial state. This token represents a slot which is assigned by scheduler for transferring a TS packet. Its capacity is one token.
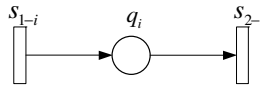
Fig. 4. The input traffic model for VBR source

Because the input TS of the second phase multiplexer is VBR, we assume that the TS packets arrival process of each program is a two-state markov modulated poisson process (MMPP) [6]. Its GSPN model is shown in fig.4.

The transitions and places shown in fig.4 are described below:

$i \in [1,n]$ in the following description.

s_{1-i} is a timed transition. Its rate is associated with α_i, which is Poisson arrival rate.

s_{2-i} is a timed transition. Its rate is associated with β_i, which is Poisson arrival rate.

q_i is a place, the capacity of which is one tokens when the enabling rule of s_{1-i} is $M(c_i) < 1$.

The place q_i and transitions s_{1-i}, s_{2-i}, ts_i in fig.4 model the two-state MMPP arrival process to the ith queue. When the place q_i is not empty, transition s_{1-i} will fire with rate α_i, otherwise transition s_{2-i} will fire with rate β_i. Transition ts_i has marking dependent firing rate. If the place q_i is not empty, the firing rate of transition ts_i is λ_{1-i}, otherwise it is λ_{2-i}. This model can be very easily extended to MMPPs with larger numbers of states.

We study the performance of such a multiplexer under four different scheduling algorithms:

Constant Bit Rate (CBR). Under this policy, a fixed number of slots are allocated to TS packets of each queue. The CBR algorithm described in fig.5 is a polling algorithm. The place c_i ($i \in [1,n]$) is used for achieving firing of m_i in the order from m_1 to m_n. Place c_n includes one token in the initial state.
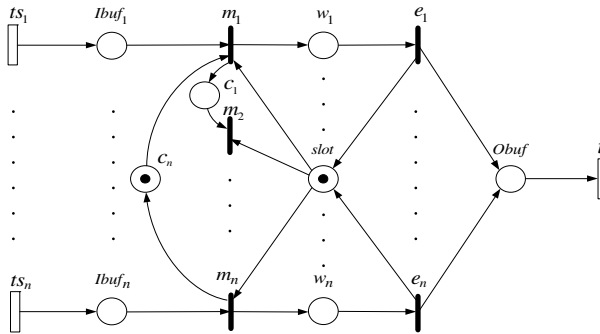
Fig. 5. GSPN model for CBR algorithm

First Come First Serve (FCFS). According to this policy, TS packets are served in the order of arrival. For our model in Fig.3, the enabling rule of m_i is $M(Ibuf_i) \geqslant 1$. If packets of several queues arrive in the same slot, they are transmitted in random order.

Queue Length Threshold (QLT). Under this policy, whenever the number of TS packets in a queue is greater than or equal to threshold value, *TH*, packets in this queue are transmitted. QLT is usually used in the scheduling framework with the priority. The smaller threshold of a queue is, the higher priority of the queue is. For our model in Fig.3, owing to the equality of all the queues in the TS multiplexer, all

thresholds are assigned the same value. The enabling rule of m_i is $M(Ibuf_i) \geqslant TH$. If the number of TS packets in several queues is greater than or equal to TH in the same slot, their TS packets are transmitted in random order.

Longest Queue First (LQF). Under this scheduling discipline, scheduler firstly selects the queue which contains the most TS packets. For our model in Fig.3, the enabling rule of m_i is $M(Ibuf_i) > M(Ibuf_j)$, where $1 \leqslant j \neq i \leqslant n$.

3.2   Performance Analysis

Three steps with regard to analyzing performance of system with GSPN, are as follow:

a. To create the GSPN model of the system.
b. To obtain the embedded markov chain (EMC) which is isomorphic with GSPN model.
c. To analyze the performance of system is based on the steady-state probability which is derived from EMC.

This subsection describes how to analyze the performance of system after the steady-state probability is derived from EMC.

For our model in fig.3 and fig.5, throughput of the whole system can be regarded as throughput of transition t, recorded as T, which is calculated as follow:

$$T = U(t) \times \mu \tag{1}$$

where $U(t)$, which is utilization ratio of t, can be calculate as follow:

$$U(t) = \sum_{M \in E} P[M] \tag{2}$$

where $P[M]$ denotes the steady-state probability of a reachable marking, and E is a set of reachable markings which enable transition t to fire.

Suppose $P[M_j]$ denotes steady-state probability of marking M_j. $P[M(x)=k]$ denotes probability of containing k tokens in any place x, which is calculated as follow:

$$P[M(x) = k] = \sum_j P[M_j] \tag{3}$$

The average number of tokens that any place x contains, u_x, is calculated as follow:

$$u_x = \sum_k k \times P[M(x) = k] \tag{4}$$

The average number of all the places, N, can be calculated as follow:

$$N = \sum_{x \in P} u_x \tag{5}$$

where P is a set of all the places in our model.

According to Little rule, average time delay of system, D, is calculated as follow:

$$D = \frac{N}{\lambda} \tag{6}$$

where λ is average arrival rate.

The packet loss rate (PLR) of queue *Ibuf$_i$*, *L$_i$*, can be calculated as follow:

$$L_i = P[M(Ibuf_i) \geq b_I] \tag{7}$$

We evaluate the fairness of a variety of scheduling algorithms by introducing coefficient of variation (CV). CV_{PLR} denotes a normalized measure of dispersion of PLRs of all the queues under a scheduling algorithm, which is calculated as follow:

$$CV_{PLR} = \frac{\sigma_{PLR}}{L} \tag{8}$$

where L is mean of L_i ($i \in [1,n]$). σ_{PLR}, which is standard deviation of L_i, can be calculated as follow:

$$\sigma_{PLR} = \sqrt{\frac{\sum_{1}^{n}(L_i - L)^2}{n}} \tag{9}$$

Generally, the smaller CV_{PLR} of scheduling algorithm is, the better the fairness is.

4   Numerical Results

In this section we present numerical results obtained by solving the GSPN model presented in the previous section using Stochastic Petri Net Package (SPNP) [7].

Suppose $n=4$, $b_I=6$, $b_O=16$, $\mu=20$, *TH* under QLT algorithm is equal to 3. The parameters of MMPP source are shown in table 1. Table 2 shows various input rates of ts_i from low to high.

Table 1. Parameters of MMPP source

Const	α_1	β_1	α_2	β_2	α_3	β_3	α_4	β_4
value	0.05	0.5	0.1	0.8	0.08	0.4	0.2	0.9

Table 2. Various input rates of ts_i

Variable	Value								
$\lambda_{1\text{-}1}$	2.8	4	4.5	5	5.5	6	6.5	7	8.3
$\lambda_{2\text{-}1}$	3.5	3	3.5	4	4.5	5	5.5	6	7
$\lambda_{1\text{-}2}$	3.8	3	3.5	3.6	4.5	5	6	6.5	7.6
$\lambda_{2\text{-}2}$	2.5	3.2	3.6	3.9	4.8	5.2	5.7	6.1	6.7
$\lambda_{1\text{-}3}$	3.1	4.1	4.6	5.1	5.9	6	7.8	7.6	7.8
$\lambda_{2\text{-}3}$	2.9	2.9	3.7	4	4.6	5.1	6.8	7.2	8.2
$\lambda_{1\text{-}4}$	4.3	5	5.6	6.5	7.3	7.5	7.7	8	8.5
$\lambda_{2\text{-}4}$	3.2	4.2	4.7	5	5.2	5.6	6.4	7.3	7.1

Fig.6 shows the relationship between the throughput and total input rate under four different scheduling algorithms. The CBR algorithm has the lowest throughput among four scheduling algorithms, while other three algorithms have almost same throughput. Fig.7 shows the relationship between the average time delay and total input rate under four different algorithms. The CBR algorithm always has great time delay. The time delay under the LQF algorithm becomes larger than others when total input rate is higher than output rate. The FCFS algorithm has the smallest time delay. The time delay of QLT algorithm is situated between FCFS and LQF when total input rate is very high. Fig.8 shows the relationship between CV_{PLR} and total input rate under four different algorithms. CBR and FCFS have greater value of CV_{PLR}. LQF has the smallest value. CV_{PLR} of QLT algorithm is situated between FCFS and LQF.
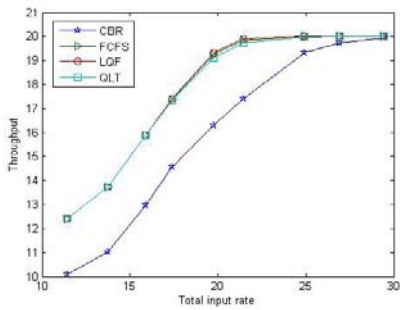
Fig. 6. Relationship between throughput and total input rate
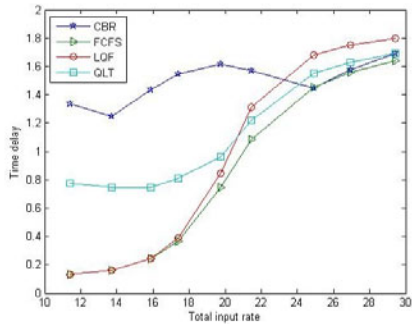
Fig. 7. Relationship between time delay and total input rate
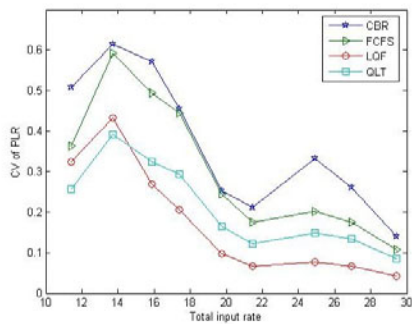
Fig. 8. Relationship between CV_{PLR} and total input rate

5   Conclusion

In this paper, we propose a GSPN model for multiplexing architecture to evaluate scheduling algorithms of MPEG-2 multiplexer in digital television systems. Using this model, we can conveniently analyze throughput, delay, and fairness of those

scheduling algorithms. Numerical results show that CBR algorithm is poor in all aspects of performance. Although FCFS algorithm has a smaller time delay of system, its fairness is not good. LQF algorithm has the nice fairness, but its time delay is great when total input rate is higher than output rate. Moreover, the complexity of LQF algorithm for implementation is higher due to sorting the number of TS packets in the queues. QLT algorithm is comparatively well balanced in all respects.

References

1. Generic coding of moving pictures and associate audio information, Part 1: System, Part 2: Video, Part 3: Audio, CD 13818, ISO/IEC JTC 1/SC 29/WG 11 (1995)
2. Lin, Y.-D., Chun-MoLiu: A timestamp-sensitive scheduling algorithm for MPEG- II multiplexers in CATV networks. IEEE Transactions on Broadcasting 44(3), 336–345 (1998)
3. Jianghong, D., Zhongyang, X., Hao, C., Hui, D.: Scheduling algorithm for MPEG-2 TS multiplexers in CATV networks. IEEE Transactions on Broadcasting 46(4), 255–294 (2000)
4. Ajmone Marsan, M., Conte, G., Balbo, G.: A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems. ACM Transactions on Computer Systems 2, 93–122 (1984)
5. Wang, J.: Timed Petri Nets Theory and Application. Kluwer, Norwell (1998)
6. Fischer, W., Meier-Hellstern, K.: The Markov modulated Poisson process (MMPP) cookbook. Performance Evaluation 18, 149–171 (1993)
7. Trivedi, K.S.: SPNP User's Manual Version 6.0 (1999)

Dynamic Analysis of Fractional Order Systems

Wen-Xian Xiao[1], Zhen Liu[1], Ji-Tian Wang[2], and Wen-Long Wan[3]

[1] Network Center
[2] School of Information Engineer
[3] Foreign Language Department
Henan Institute of Science and Technology, Xinxiang, China, 453003
Xwenx@yeah.net

Abstract. Based on the fractional ordinary differential stability theory of dynamical systems and dynamic simulation of generalized predictor - corrector algorithm for numerical simulation, this paper fractional complex dynamic behavior of the system studied. First, theoretical analysis, this paper gives a typical homogeneous fractional order systems in the scope of the order of chaos should meet the necessary conditions; further, through the state bifurcation diagram, Poincare section, and the power spectrum analysis, we numerically Discussed the different orders homogeneous fractional order systems dynamic behavior typical results of the study design appropriate for the engineering and technical personnel chaotic circuit has a certain significance.

Keywords: fractional order systems, Bifurcation, Poincare section, powers.

1   Introduction

Chaotic anti-control of continuous systems in recent decades has developed very quickly, in fact, the new chaotic attractor has been found and investigators continue to give the physical circuit, which greatly promoted the progress of chaos theory from a simple mathematical or physical theory of towards real practical application. In recent years, fractional calculus and its application are also being rapidly developed. For the study of fractional calculus stems from the fact: in reality many of the objects are fractal dimension, although most of the fractal dimension of the system is relatively low. Typical practical examples from the electrical, thermal studies researchers are given[1]. Fractional calculus is the mathematical tool of such proposal, allow researchers to describe the dynamic behavior of some objects become more accurate. For example, another typical fact is: the physical electronic components of the non-ideal nature of property, some non-linear circuit applications of fractional order systems would be more accurate to describe the literature[2] in the discussion of fractional Chua circuit Characterize the problem of fractional states.

In the past, the classical differential equation theory believed that autonomous system to produce the minimum-order chaotic project should not be less than 3 times, when the introduction of the concept of fractional derivative, the autonomous system to produce chaos head into a minimum order number can be less than 3, Even smaller[3]. Previous studies showed that: power system has the integral of fractional order

dynamical systems that are not characteristic, for example, fractional order Chua circuit in the order of 2.7 to the possible chaos, such an interesting phenomenon has attracted many Physics, mathematics, and engineering and technical personnel of interest. Currently, from the fractional order chaotic system control and anti-control theory in the ascendant, has become a frontier field of nonlinear science field[4].

In recent years, fractional circuit design and research attracted the attention of many researchers. Based on Fractional Ordinary Differential stability of dynamical systems theory and the generalized dynamic simulation of Adams-Bashforth-Moulton predictor - corrector simulation algorithm, this preliminary study of the fractional complex dynamic behavior of chaotic systems. Through theoretical analysis, this paper shows the typical homogeneous fractional order systems in the chaotic behavior of the order of the minimum necessary conditions; further, through the state bifurcation diagram, Poincare section, and the power spectrum analysis, this paper will also discuss the scope of the order of the typical range homogeneous fractional complexity of the system dynamics. This paper gives theoretical analysis and numerical results for the engineering design of the appropriate application of technology; the researchers' chaotic circuit has a certain significance.

2   Chaotic System and Its Corresponding Fractional Order System

1963, E. N. Lorenz in three-dimensional autonomous system in the discovery of the first classical chaotic attractor. In 1999, Professor Chen Guanrong in three-dimensional autonomous system, found another chaotic attractor. Subsequently, Dr. Lv Jinhu, Professor Chen Guanrong and Zhang Suochun researchers found a new chaotic attractor: attractor. The dynamic equations of the chaotic system as follows [5,6]:

$$\begin{cases} \dfrac{dy}{dt} = a\,(\,y - x\,) \\[2mm] \dfrac{dy}{dt} = -\,xz + c\,y \\[2mm] \dfrac{dz}{dt} = x\,y - b\,z \end{cases}$$

The system is connected to the famous Lorenz and Chen's attractor, when the system parameter values as a=30, c=22.2, b=2.9333, the system has a chaotic attractor, shown in Figure 1. System build a bridge between the Lorenz and Chen's chaotic attractor, this realized from a chaotic system to another is that not topological equivalent chaotic system, the transition. In fact, the three systems are the newly proposed parameters of Lorenz system, the typical family situation, family dynamics for the Lorenz system analysis and detail on the above three systems Dynamic Analysis and Control of research progress, the reader can read Chen Guan-Rong and Lvjin Hu monograph published[7,8].
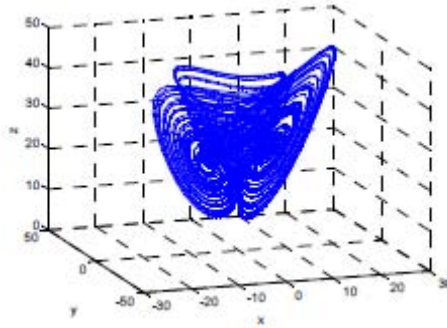
Fig. 1. Integer-order chaotic system of three-dimensional phase diagram

The corresponding definition is as follows system fractional power system (2)

$$
\begin{cases}
\dfrac{d^{q1}x}{dt^{q1}} = a(y-x) \\[2mm]
\dfrac{d^{q2}y}{dt^{q2}} = -xz + cy \\[2mm]
\dfrac{d^{q3}z}{dt^{q3}} = xy - bz
\end{cases}
$$

All are equal when the order of parameters, namely q1q2q3q, the termed homogeneous fractional chaotic system, otherwise known as non-homogeneous fractional chaotic system. In Figure 2 shows the order of the fractional order parameter chaotic system. In Figure 2 shows the parameters of the order of 0.95 space dynamics of the system phase diagram, the relevant system parameter values with the corresponding integer-order system (1) the same parameters
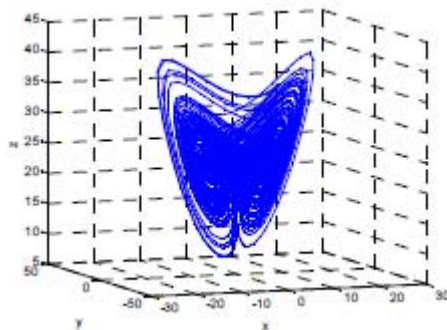
Fig. 2. Fractional phase diagram of three-dimensional chaotic systems: q = 0.95

3   Homogeneous Fractional Dynamics of Chaotic Systems

For simplicity, this article discusses only homogeneous fractional order systems dynamics. For non-homogeneous fractional ynamics of chaotic systems can refer to

this method for dynamic analysis; the same time, all of the following discussion, homogeneous fractional order systems (2) the parameters are kept with the integer order system (1) consistent. Analysis; the same time, all of the following discussion, homogeneous fractional order systems (2) the parameters are kept with the integer order system (1) consistent.

3.1   Fractional the Emergence of Chaotic Systems Necessary Conditions for Chaos

First of all, this section will give the decision by the integer-order chaotic system constructed corresponding homogeneous fractional chaotic nonlinear system to maintain a necessary condition, here are a few need to use Lemma[9,10].

Lemma 1. For the fractional order system $\frac{d^q X}{dt^q} = AX, (0 < q < 1),$ at $\left| \arg(eig(A)) \right| > \frac{\pi q}{2}$ its equilibrium point is asymptotically stable.

Lemma 2. For the fractional order systems $\frac{d^q x}{dt^q} = f(X), (0 < q < 1, X \in R^n)$ of nonlinear equations to meet the record X f (X) = 0 for all the equilibrium point, then, $\left| \arg(eig(\frac{\partial f}{\partial X}|_{X*})) \right| > \frac{\pi q}{2}$ the equilibrium point X * is locally asymptotically stable within.

Lemma 3. Assuming that the number of λ -2 for the nonlinear system $\frac{dX}{dt} = f(X)$ corresponding to a linear saddle point of the premises Jacobian eigenvalue, the corresponding fractional order system: $\frac{dX}{dt} = f(X)$ still maintaining the necessary conditions for chaos: the eigenvalue λ in Lemma 2 identified within the region of instability is met: $\tan(\frac{q\pi}{2}) > \frac{|Im(\lambda)|}{Re(\lambda)} \Rightarrow q > \frac{2}{\pi} \tan^{-1} \frac{|Im(\lambda)|}{Re(\lambda)}$.

For a three-dimensional nonlinear system, the equilibrium point at the saddle point, the equivalent linearization eigenvalues of the Jacobian matrix must have an eigenvalue in the stable region, and another in the unstable region; general, in the Systems, such as the saddle point in the linear Jacobian matrix corresponding to a characteristic value is unstable, while the remaining eigenvalues are stable, then the saddle point is called saddle point index -1; if the saddle point linear Jacobian matrix of a feature value is stable, while the remaining two eigenvalues is unstable, then the saddle point is called saddle point index of -2. For chaotic systems, the saddle point index -1 is considered to be a key factor in generating a continuous roll, and the production of multi-volume index of -2 is derived from the existence of saddle point [8-10].

For   example,   for   three-dimensional   continuous   chaotic   systems: $\frac{dX}{dt} = f(X), (0 < q < 1, x \in R^n)$ Assuming that the system has only three equilibrium points,when it has an index of -1 saddle point, the two index -2 saddle point, the system will have a two-roll attractor. For fractional order systems, you can use the lemma 3 of the necessary conditions for chaos analysis the system to produce a minimum order of parameters q range.

Theorem 1. Homogeneous fractional order systems (2) the order of chaos phenomena range: q> 0.8426. In fact, when taking parameters a = 30, b = 2.9333, c = 22.2, the system of homogeneous fractional (2) has three equilibrium points: S + (8.0697,8.0697,22.2), S-(-8.0697, -8.0697,22.2), O (0,0,0), easy to find the system in unstable equilibrium point of S +, S-eigenvalue at λ, respectively:

λ1 = -17.9535, λ2 = 3.6101 +14.3037 i, λ = 3.6101-14.3037i,

3.2   Homogeneous Fractional Chaotic System Bifurcation Diagram, Poincare Section and Power Spectrum Analysis

1) homogeneous fractional bifurcation diagram of chaotic systems
To state x (t) the local maximum for the vertical axis, change the order of parameter q, in the following Figure 3 shows the necessary conditions for chaos generation included in the parameter ranges given in the [0.82,1.00] interval of the bifurcation Figure
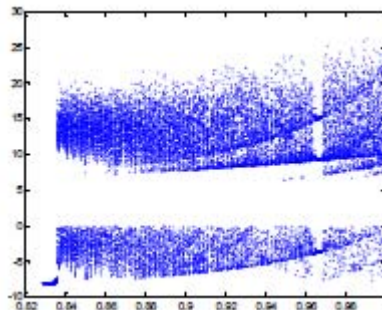
Fig. 3. Fractional order systems state x (t) of the Order of the bifurcation parameter
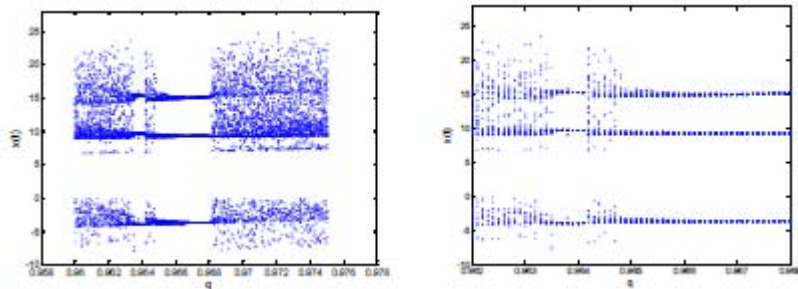
Fig. 4. Fractional local bifurcation range of magnification in Figure 3

Bifurcation diagram by observing that: when q1 = q2 = q3 = q, in the q values in [0.83,0.835] segment system dynamics is not very clear, and in the q values in [0.965,0.970] paragraph appeared in the range of a typical cycle window. Figure 4 shows the fractional order systems state x (t) vs q bifurcation diagram (Figure 3) the local magnification range, from which you can see clear down bifurcation. In fact, two cycles can be observed from the window, the window in the middle of two cycles,

corresponding to the unstable equilibrium point by two homoclinic orbits to form the sense of chaos. Figure 4 shows the system corresponding to the typical cycle times from low to high power cycle to low cycle times typical attractor graph.

2) homogeneous fractional chaotic systems Poincare
Next, the first order of parameters given q = 0. 9 5 0, the too chaotic attractor in Figure 5, the unstable equilibrium point S + Poincare sections of three typical
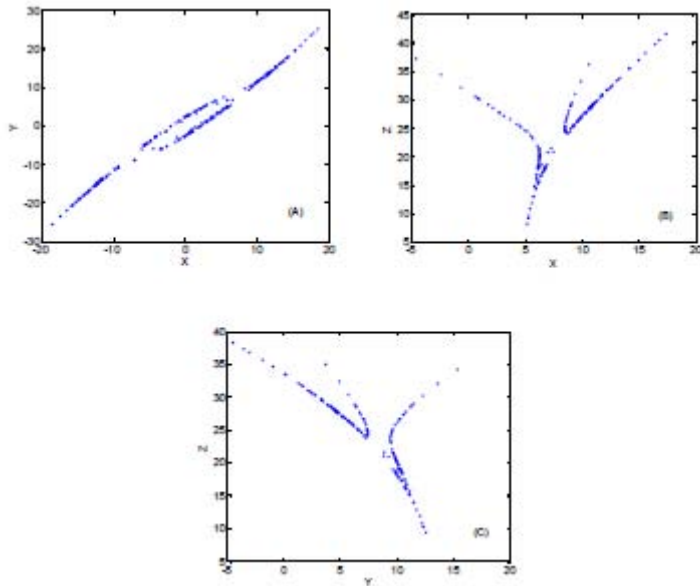
Fig. 5. Parameters of the order of 0.95, the chaotic attractor state typical Poincare interface
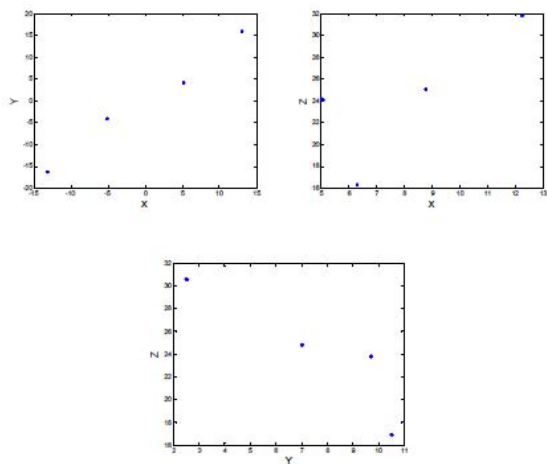
Fig. 6. Order parameter is 0.9675, the typical periodic state phase diagram and the Poincare sections

A) plane z0 = 22.2000: B) plane y0 = 8.0697: C) plane x0 = 8.0697 from Figure 6, we can see clearly leaves fold, indicating that the fractional order systems at this time showed typical chaotic state. Figure 7 shows the parameters obtained when the order of q=0.9675, over at the unstable equilibrium point S(system was a typical cycle of state) interface of the three typical Poincaré. Order values for other parameters can be used for similar studies, the limited space does not discuss in detail in this

3) homogeneous fractional power spectrum of chaotic systems
Despite the continuous broadband power spectrum only can be as a necessary condition to determine chaotic, it still would be a indicator weather the fractional order systems showing chaotic behavior. In Figure 7, shows the different order parameters of the system state components x (t) of the power spectrum. N for the periodic motion, the frequency power spectrum only in the state of the i/n (i is a positive integer) occurring at the peak, as shown in Figure left. For chaotic motion, the background noise power spectrum showed a broad peak of the continuous spectrum, which corresponds with the peak with the periodic motion.
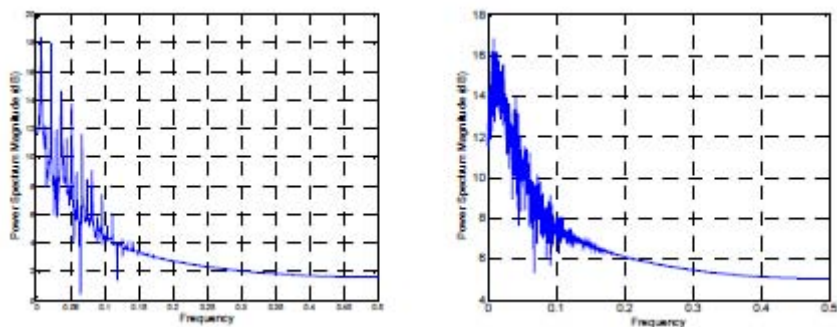
Fig. 7. The state x (t) the power spectral density map q = 0.9675 (left), q = 0.9500 (right-

4   Conclusion

Fractional often based on reliable power system stability of micro theory, this paper homogeneous fractional order systems in the chaos of the system the minimum necessary conditions for the range of the order of q> 0.8426. Through dynamic simulation, this paper studied the homogeneous fractional complex dynamic behavior of chaotic systems, including the characteristics of the state bifurcation diagram, Poincare section features, and power spectrum characteristics. In this paper, the theoretical analysis and numerical methods for the study similar fractional order systems with complex dynamic behavior of some guidance, and relevant results for researchers in the field of electronic engineering design of the appropriate application of chaotic circuit has some reference value. In the future, we will be through the Lyapunov exponent analysis and the theory of topological horseshoe for further discussion of the complexity of the system dynamics and its applications.

References

1. Podlubny: Fractional Differential Equations. Academic Press, New York (1999)
2. Petrá, I.: Method for simulation of the fractional order chaoticsystems. Acta Montanistica Slovaca 11(4), 273–277 (2006)
3. Ahmad, W.M., Sprott, J.C.: Chaos in fractional-order autonomous nonlinear systems. Chaos, Solitons & Fractals 16, 339–351 (2003)
4. Hu, L., Jun-ALu, Chen, S.-H.: Chaotic Time Series Analysis and Its Applications. Wuhan University Press, Wuhan (2002)
5. Guan-Rong, C., Hu, L.: Lorenz system family dynamics analysis, control and synchronization. Science Press, Beijing (2003)
6. Chen, G., Yu, X.: Chaos Control: Theory and Applications. Springer, Berlin (2003)
7. Tavazoei, M.S., Haeri, M.: Unreliability of frequency-domain approximation in recognising chaos in fractional-order systems. IET Signal Processing 1(4), 171–181 (2007)
8. Tavazoei, M.S., Haeri, M.: A necessary condition for doublescroll attractor existence in fractional-order systems. Physics Letters A 367, 1-2(16), 102–113 (2007)
9. Tavazoei, M.S., Haeri, M.: Chaos control via a simple fractional-order controller. Physics Letters A 372, 6(4), 798–807 (2008)

The Control Plane Models
Based on Virtualization Router

Wen-Xian Xiao[1], Zhen Liu[1], Ji-Tian Wang[2], and Wen-Long Wan[3]

[1] Network Center
[2] School of Information Engineer
[3] Foreign Language Department
Henan Institute of Science and Technology, Xinxiang, China, 453003
Xwenx@yeah.net

Abstract. Reconfigurable next-generation network router technology is an important part in the system of the net. This paper analyzes the shortcomings of existing network equipment control soft thing in support of reconfigurable part, and proposes software model based on virtualization reconfigurable router control. This model based on mature and stable multi-process operating system, provides the same operation environment and support system resources of the administration of quotas through the operating system kernel virtualization for reconfigurable router different members software, and cuts off the impact on performance from the different component software running on the same control software system, which improves the openness and safety of entire reconfigurable router control software system.

Keywords: Plane model, Routing protocols, Virtualization.

1 Introduction

Internet as a worldwide maximum data network, which has been exposed to many inadaptability and the rigidity, currently, it shares an Internet2 reflection wave in the global scope. At the same time, being as the fastest developing speed in a wide-area infrastructure, Internet attracts the traditional telecom network and television network to become generally the next generation combination of three nets basic flat platform.

Efforts to settle on the next generation network system exploration from three angles respectively depicts a next-generation network system technology outline: packet-switching as the foundation, support for multiple business amalgamation of integrated network architecture (such as 13NGN, 3Tnet, FP6); enhance network service abilities (such as the FAN, FLexNET, ACCA) flexibly from the network of programmability, expansibility and intelligent aspects; reflect the current problems of Internet and relearn idea and concept, establish a set of safe and controllable, flexible department and good business adaptability of new network structure. From the research of development on the next generation network, which can be seen with programmability, expansibility and intelligent characteristics of reconfigurable routing inverter system will gradually replacing the traditional high-performance core

routers, while the traditional closed since distribution of Internet control to separation independent, it is easy to expand new control management function direction. In the traditional framework of network technology, network equipment relies on expanding links transmission bandwidth, improves the node processing speed, increases the node processing capacity to meet growing demand through increasing the performance of complex control algorithm and the coordinated re-debate series such as technology, meeting the performance between ever-growing user business bearing demand. However, the traditional network equipment control in the plane of the tight coupling has its closeness and sketched characteristic, which causes network equipment controlling function into difficulties of prolongation and new network application and development of agreement deployment in slowing [1]. Obviously, the traditional network equipment system software from the embedded systems development cannot meet the reconfigurable routing device system requirements, so we must seek for breakthrough.

2   Related Research

2.1   Cluster Router Technology

Single ark (single2box) router systems cannot have met interface link rate and port density enhancing unceasingly development request, it can be solved link rate and port density improving performance requirements through multiple arcing of interconnections cluster router systems. Equipment manufacturers in recent years has introduced a variety of high performance cluster router systems, the typical delegate includes routers, CRS routers and T640 system.

The above the commercial cluster router systems are using isomorphism system and internal for special interconnection interface. This used cluster system of each isomorphism ark itself is a complete set of router systems, which improves performance through cluster interconnection, operating parallel. This isomorphism cluster is difficult to solve function reconfigurable and dynamic upgrade, while it can only achieve scale reconfigurable.

With the current commercial systems in difference, some research results in cluster router aspect are not limited to the pursuit of performance improvements, but will be expanded functional flexibility as the main purpose, among them, the most typical delegate includes Pluris company's large-scale parallel router [2], NEC (USA) C&C laboratory CLARA (CLr2basedAcUstetive Router Architecture [3], state university of new Su2 ez[4] and Princeton university of VERA[5]. Pluris large-scale parallel routers, by a group of single trigger (processing node) through cable lubricator interconnecting constitute the cluster routing platform, by synchronizing multiplexing mixer several low-speed flows clumped into backbone network of high-speed flow. CLARA routing function uses a PC or traditional commercial router to complete, the router is fully compatible with the existing, Computing power can be extensible, by general PC constitute the processing engine cluster to complete. CLARA's goal is to provide with "Internet message do force forwarding thought" similar, based on the packet to calculation service. CLARA system structure particularly is suitable for

streaming media coding solution code etc treatment process, it can be more flexibility to support various thin clients, reduce on the client's calculation and storage requirements.

Suez is a high-speed packet forwarding, which holds branch allowing to safe and effective in the way of adding new functionality routing device of high-performance router architectures. Its goal is to develop scalable router systems, combining high-performance turn hair and in the network increasing intelligent processing, and even gives attention to two or more things load calculation functions, the core function of router provides the powerful protection and isolation performance. VERA and Suez is similar, it researches IP layers message forwarding paths scalability, while in the lateral heavy layer should be with the extension of ask questions. Exhibition V ERA for router IP layer defines the upper application oriented to the router abstract interface and facing to lower hardware platform of hardware abstraction, and improves the router interface of software system expandability.

Heterogeneous extensibility is system-level reconfigurable router's development goals, in the system; it realized the router granularity of flexible reconstruction, extension and increased performance ability and so on.

2.2   Open Router Technology

According to the router bearing function clustering division, the router is usually divided into forwarding plane and control plane, and the forwarding plane and further is divided into interconnection exchange, forward engine and link treatment 3 large parts. Because computer system adopts the standard open architecture, it can establish a complete user's system from different manufacturers purchase different parts, according to user's request of assembly customization. The openness of computer architecture broke a few manufacturers for system of monopoly in tremendously inspired each component technology development, but also the user won more cost-effective products. The internet has already started this aspect of trying, with the passage of time this trend is becoming a kind of sustenance that people inspires network innovation. Based on this thought, academe have been put forward concerning open architecture, 1 kind is open control architecture, including: the transfer of IETF GSMP itch M l Swanage2 Ment Protocol, an IEEE P1520 reference model[6], MSF, BBS (Muti2Se rvice Switch) and an IETF xsl-forC2ES[7] (xsl-forwarding and Control Element Sep a ration). This framework used open signaling (OpenSig) thoughts, as the communication network, control and forwarding is separated, each is independent. The second was component interfaces standardization, such as NPF framework BBS router reference model, this model in control and forwarding plane using xsl-forCES interface, in forwarding plane internal components between defines Csx-1, Csx-2, LA-1/2 etc interface. This framework tried to decompose into several independent components router, making the production router like computer as handy assembly, this is the component level reconfigurable router to show us the prospect. But it is hard to obtain breakthrough, one of the biggest resistance comes from the industry of self-protection, existing vested interest manufacturers are not willing to give up technology monopoly bring lucrative, so this technology needs multi-lateral strength coordinated development[8].

2.3   Programmable Router Technology

In 1968, at the NATO software engineering conference, McIIicy put forward the concept of software reuse, in the 1990s, the object-oriented technology appeared and gradually become the mainstream of software development software reuse technology, which provides basic support so that the software reuse technology research become hot. Application software users and developers hope to such as electronics product components of consumer and manufacturers as plug and play all kinds of application software, this plug and play application software called components or software component, which produced the component technology. Especially, with the development of the Internet in recent ten years, based on component design techniques gradually become maturing. Component itself is an independent unit module so that it is easy to use in deployment of third parties integrated. In the network equipment, components and application of technology is still in a primary stage. Current main network equipment is not supporting third-party components of integration, this not only influence the network operation business cost and quality of service, but also limits the technological innovation. The earliest of active network (Active Network) is network domain in this aspect at the first attempt. Active network will be stored - the traditional network model forwarding change into storage - calculations - forwarding models, according to the program and data is carrying way is divided into two modes: independent bearing mode (also called the programmable exchange strategy, node into executable code and processing of a message work separately) and mixed bearing mode (also called for encapsulation strategy, code and data using the same message to carry). "Programmable exchange strategy" maintain the previous message format, its programmability dynamically download/loader to realize, these programs to arrive at the nodes and comply with rules and conditions of message handling. An active network node includes three levels within the NodeOS, node operating system EE (execution Environment) and running at different EE environment in the active application AA (Active Application). Here the EE can cut solutions of component of containers; AA is equivalent to functional components. Due to security reasons encapsulation strategy is not continue to develop, the programmable exchange strategy is in active network development gradually after a mainstream research direction --, programmable network. Programmable exchange strategy directly influenced the aforementioned GSM P, P1520 and NPF such as control model of production and development [9]. The above research is only in local verification system, and verifies the dynamic function restructuring router's thoughts. These modular components of computer software are far from component technology. As the network service type the sharp increase in network service, business demand more present differentiation, components reconfigurable programmable routers increasingly hoping to develop network services like software programming as agile and convenient.

3   The Challenge of Reconfigurable Technology on Traditional Network Equipment Control Plane Software System

The traditional network equipment control system based on embedded system software is usually in development, such as: Cisco IOS system has constructed a

simple OS, bearing complex IOS software; Huawei constructed Vx2 work s for infrastructure own routers OS, Alcate l to Vx-works for infrastructure own routers OS. These control system software has following features or shortcomings:

1) based on traditional embedded system multithreaded programming model;

2) majorities of them have no process and virtual memory, the concept of sharing all the real address space;

3) for single kernel processor, facing the hypercore processor system support bad or does not support;

4) each agreement between software modules are very high, usually by coupling directly access other protocol modules core data structure mode realizes data sharing together;

5) the stockings software has a complex reactive function and weak ability in line liters level.

Reconfigurable router to control system software, puts forward the new functional requirements are mainly embodied in the following several supportive aspects of abilities:

(1) open interface ability through standard description language and tasseled a way to define the interface calls reconfigurable router control system software operating system call interface, forward plane access interface, routing heavy release interface, routing protocol information access interface and the user control command interface, etc; Through the open joint support, supporting third-party to control system software of various agreement module independent development.

(2) dynamic deployment ability based on open interface implementation of various agreement module can be in reconfigurable router control plane the normal operation of the cases of dynamic add/remove, it doesn't need to control plane restart or to the kernel image to compile links;

(3) advanced programmable ability based on open interface technology of all kinds of routing protocol to abstract, establish unified agreement routing visit mold type and agreement interactive control model, size of senior support module abstract language programming ability and upper application on the network topology information and routing information query access;

(4) shielding hardware platform of differentiated network equipment and hardware platform concrete realization way flat ward, in order to support system software flat platform of open interfaces and dynamic deployment, it must network equipment hardware platform which abstract modeling, it provides consistent underlying hardware access platform and operation environment for the upper level protocol module through independent hardware abstraction layer.

(5) unified concentration of users to control the traditional network equipment control functions through the centralized and unified access control interface (such as: UI, SNMP, etc.) reveal to users. In order to guarantee the configuration management based on multiple independent component compatibility and the realization of reconfigurable router control plane must support unified concentrated control method, and try to interface with the original user control compatible.

4   Based on Kernel Virtualization Reconfigurable Router Control Plane Models

Reconfigurable router in control system software support reconfigurable, first in choosing router an operating system kernel, we should use current main processes operating system to avoid embedded operating system between threads sharing the same physical address space caused by security and deployment of problems Secondly, we must limit router in the operating system operation of each functional component resource usage and authority restriction to avoid malicious component or achieve defect affect system usability. Finally, because all sorts of router manufacturer hardware platform realization ways differ in thousands ways, we must have a special hardware abstraction layer to a hardware function abstraction to establish unity of hardware platform abstraction description model and access interface for upper operating systems, forwarding module, routing protocol module of access.

Based on the above analysis, this paper puts forward a method based on kernel virtual technology of reconfigurable router control plane models, as shown in figure 1 show. The whole model consists of four levels constitute, respectively is: reconfigurable router hardware platform, the kernel operating system layer, routing and forwarding layer and application plugin layer .

Reconfigurable router hardware platform includes reconfigurable router various underlying hardware equipments, such as: line card, high-speed packet switching network, master card, etc.

(2) Kernel operating system layer consists of hardware abstraction layer and reconfigurable road by device OS kernel and kernel virtualization service platform for upper composed, various component function module provides resource management, scheduling and system reactive services, etc.

Hardware abstraction layer to a hardware function abstraction, establish unity of hardware platform abstraction description model and access interface for upper operating systems, forwarding module, routing protocol module of access. Hardware abstraction layer shield the underlying hardware implementation details, is supporting third-party components of independent development and dynamic deployment of the key.

Reconfigurable router OS kernel: based on current main processes operating system design, Solving the key problems needs to establish a suitable for router course, thread scheduling mechanism; To supply high-performance inter-process communication mechanism. Support efficient chunks of memory copy mechanism and sharing mechanism.

Kernel virtualization service platform: operating system level virtualization separated user layer function from components mutual isolated and supported for each virtual machine inner component of resource access control strategy and system service access control.

Disposal layer in corresponding forwarding treatment cots message look-up table and forwarding operations. Due to the high performance router packet forwarding mainly by the hardware, software forwarding to complete the performance requirements of is not high, the user space forwarding component will not become system performance bottleneck. At the same time, from the kernel virtualization

service platform ensure forwarding component and routing components between isolation, ensure individual component problems won't affect the entire system usability and stability .

5   The Key Problems Need to be Solved

The key problems based on the kernel virtualization reconfigurable router control flat surface model needed solving mainly includes:

(1) The high-performance kernel virtualization reconfigurable router control plane in need of the deployment of the functional components number, each functional component needs independent virtualization of running environment support. Therefore, facing reconfigurable router's high-performance kernel virtualization must be able to support 1000 magnitude and independent virtualization operation environment that supports flexible access control strategy and resource quota strategy. High-performance kernel virtualization is very important to reconfigurable router control plane performance.

(2) Reconfigurable router hardware abstraction model and access interface

The router manufacturer realization of hardware platform have bigger difference, at the same time with the development of technology, in hardware platform implementing continuously introducing new hardware devices and new interconnection forwarding structure. How to establish unity of hardware platform abstraction description model oriented to the upper software, defined the hardware access interface for upper operating systems, forwarding module, routing protocol module of visits reconfigurable router control of graphic design key.

(3) High-performance inter-process communication and memory sharing technology reconfigurable router component with independent operation space, component interaction between the controls must pass through the communication between processes or memory sharing technology to complete. Due to the existing high-end router support the routing table a huge number, the component of routing information sharing between the mass of inertest communication technology and the memory sharing technology existence big challenge.

(4) Packet forwarding control model and open access interface technology Internet as the fastest developing speed In a wide-area infrastructure, is gradually becoming the next generation combination of three nets foundation platform. In reconfigurable routers can include how to define three kinds of network data forwarding demand characteristic newspaper wen forwarding control model, and the forwarding processing components general access interface, decided reconfigurable router technology can become future network technology bearing platform basic requirements.

6   Summary and Prospect

This paper analyzes the next generation network system of technological development outline, as for the next generation network system is an important part of reconfigurable router technology, it analyzes the reconfigurable router systems to control the plane of system software function requirements, and points out that the existing network equipment system software in support of reconfigurable deficiency.

Aiming at the router control system software in reconfigurable insufficiency of proposed based on virtualization reconfigurable router control software model, this model based on mature and stable multi-process operating system, different members software provides the same operation environment and support system resources of the administration of quotas through the operating system kernel virtualization for reconfigurable router, cuts off the impact on performance from the different component software running on the same control software system, improves the entire reconfigurable router control software system of openness and safety. Finally, it points out that the model to solve the key technical problem by analyzing the control reconfigurable router characteristics of plane models.

Reconfigurable router control software model is shirt-sleeve tradition data transmission network architecture and the current research hotspots of cascade network architecture, routing and forwarding layer can support three net fusions of various business data transmission requirements, while application plugin layer of third-party supporting user development of network components, can deploy in reconfigurable router data transmission network layer above structure of virtual, service-oriented user layer fold network, providing various in existing network environment is difficult to deploy service. Reconfigurable router control software model research, service oriented around fusion principle, both the principle on keeping the traditional Internet open, simple, flexible advantages and don't change bottom network infrastructure, to solve the ever-increasing demand changes network provides a good solution.

References

1. Juniper Networks. Juniper networks t640 internet routing node with matrix technology. Solution Brief (2002)
2. Halab, S.: Pluris massively parallel routing. Technical report, Pluris Inc. (1999)
3. Welling, G., Ott, M., Mathur, S.: A cluster based active router architecture. IEEE Micro 21(1), 16–25 (2001)
4. Pradhan, P., Chiueh, T.: A cluster based scalable and extensible edge router architecture. Technical report, ECSL Techincal Report (2000)
5. Karlin, S., Vera, P.L.: An extensible router architecture. Computer Networks 38(3), 277–293 (2000)
6. IEEE P1520 Proposed IEEE Standard for APIs for Networks (S /OL) (2008-03-01), http://www.ieeepin.or/
7. IETF. For CESWG home page (EB /OL) (2007-12-01), http://www.ietf.org/html.charters/forces2charter.html
8. Montz, A., Mosberger, D., O' Malley, S., et al.: Scout: A Communications Oriented Operating System. IEEE Hot OS Workshop 5, 58–61 (1995)
9. Kohler, E., Morris, R., Chen, B., et al.: The Click modular router. ACM Trans. Computer Systems 18(8), 263–297 (2000)
10. Peterson, L., Muir, S., Roscoe, T., et al.: Planet Lab Architecture: An Overview. PDN 2062031, 5 (2006)

The Design of Generalized Synchronous Observer Based on Fractional Order Linear Hyper Chaos System

Zhen Liu[1], Wen-Xian Xiao[1], Ji-Tian Wang[2], and Wen-Long Wan[3]

[1] Network Center
[2] School of Information Engineer
[3] Foreign Language Department
Henan Institute of Science and Technology, Xinxiang, China, 453003
Xwenx@yeah.net

Abstract. The paper firstly by using fractional order ordinary differential dynamic stability of system theory, through the judgment linearization after equilibrium of constant characteristics, aided by bifurcation diagram analysis is presented, the numerical methods such as recently proposed improved hyper chaos L u system corresponding fractional system to produce chaos phenomena in order of the parameter scope，Then further design for a class of the generalized linear synchronous observer. Through numerical simulation further confirmed the proposed observer design the effectiveness of the proposed scheme.

Keywords: equation, synchronization, observer, chaos.

1   Introduction

Fractional calculus is known as integral exponent calculus expands; it refers to a differential and integral order of the score, or is any meaning times. In recent years, because of its fractional calculus in physics, circuit, engineering, signal processing the application fields has caused the researchers of extensive interest [1]. applied mathematics model of fractional calculus, is considered to be well improve the circuit on dynamic system design, the ability of intrinsically and control table. For example, most classic Chua 's circuit was proof can use fractional chaotic system better token, Because of this, for many classical chaotic circuit, such as the Lorenz, Lu, Chen chaos circuit, Rssle Rchaos and ō hyper chaos Rōssle Rsystem, etc, the researchers put forward corresponding fractional systems[1], and through the test or several value simulation found: when the system's order number for points, the system may still be in a certain order of the present chaos or within the scope of hyper chaos dynamic learning behavior of, and more things to reverse kingie should cut the essential characteristic of system dynamic performance.

Drive-coupling chaotic synchronization framework, was the first in 1990 by beautiful kingdom sea army real inspection room Pecora and Carro first carry out the DLL rate, it is a kind of make two chaotic system through a single variable injection, thus realize their dynamic behavior occurrence pace: namely synchronous behavior

methods, and their first in circuit experiment phenomenon observed in chaos synchronization. The discovery let people for chaos system can not be used for the initial value sensitive, the impression to gradually change. Then nearly 20 years, chaos control and synchronization aspects of theory and applied research rapid development. At present, the researchers suggest a variety of synchronous concepts such as completely in sync, effectively completely in sync, Q-S synchronization, expectations, delay synchronization, projection synchronization etc, in fact, these phenomena can be regard as Rulkov etc in 1995 puts forward "promotion chaotic synchronization" type of, is "generalized synchronization" special case. So-called generalized step[2], refers to the response system state variable and drive system state variables of the function of synchronous, according to the different function relationships, natural meeting observed referred to above all kinds of interesting phenomenon.

2   Fractional Order Differential and Its Numerical Algorithm

Fractional order differential has several definitions, most commonly used is Rie2mann - Liouville (R - L), its mathematical expressions defined as follows:

$$\frac{d^q f(x)}{dt^q} = \frac{1}{\Gamma(n-q)} \frac{d^n}{dt^q} \int_0^t \frac{f(\tau)}{(t-\tau)^{q-n+1}} d\tau \tag{1}$$

Type of gamma function for Γ, n -1$\leq$ q <n, n as integer

At present, the implementation of fractional calculus of computation methods of solving a variety of, commonly used methods are mainly geometric approximation method and estimate correction method, because geometric approximate potter figure approximation method in fitting frequency interval at both ends of the existing biggish error is easy to cause the frequency response distortion, so in discussion fractional order nonlinear systems such as chaos pseudo exist complex phenomena appears chaotic may, a growing number of engineering and technical personnel began to consider using more reliable numerical study method[3].journal of commonly used method is one of the generalized Adams - Bashforth - Moulton method. Next, to facilitate further analysis, this paper discussed briefly introduced the first will adopt such guesstimation correction methods

Consider the following differential equations:

$$\begin{cases} \dfrac{d^q y(t)}{dt^q} = f(t,y(t)), & 0 \leq t \leq T \\ y^{(K)}(0) = y_0^{(K)}, K=0,1,\cdots,m-1,(m=[q]) \end{cases} \tag{2}$$

Type (2) with the next type

$$y(t) = \sum_{k=0}^{m-1} \frac{t^k}{k!} y_0^{(k)} = \frac{1}{\Gamma(q)} \int_0^t (t-\tau)^{q-1} f(\tau, y(\tau)) d\tau \tag{3}$$

Equivalence.

Take $h=\dfrac{T}{N}$, $t_n=nh, n=0,1\cdots,N\in Z^+$ then type can discrete into

$$y_h(t_{n+1})=\sum_{k=0}^{m-1} t^k_{n+1} y_0^{(k)}+\frac{h^q}{\Gamma(q+2)}(f(t_{n+1},y_h^P(t_{n+1})+\sum_{j=0}^{n} a_{j,n+1}f(t_j,y_h(t_j)))$$

This paper will the by using this algorithm points out of new nearly mention chromatography a class hyperchaos system corresponding fractional chaotic system dynamics and synchronous control problem.

3   Fractional Hyperchaos Lu System and Its Produce Chaos Phenomena in Order of the Scope

Recently, by introducing a state feedback control equation of simple method, the literature is a new fourth-order hyperchaos system, and its corresponding the fractional order system dynamics equation is as follows:

$$\begin{cases} \dfrac{d^q x}{dt^q}=a(y-x-yz) \\[2mm] \dfrac{d^q v}{dt^q}=-xz+by+u \\[2mm] \dfrac{d^q z}{dt^q}=xy-cz \\[2mm] \dfrac{d^q u}{dt^q}-dx \end{cases} \tag{4}$$

Among them q (0<q≤1) System order of the parameters, a, b, c, d are parameters. Especially when q equals 1, a equals 35, b equals 14, c equals 3, d equals 5, the system is integral exponent hyperchaos system.
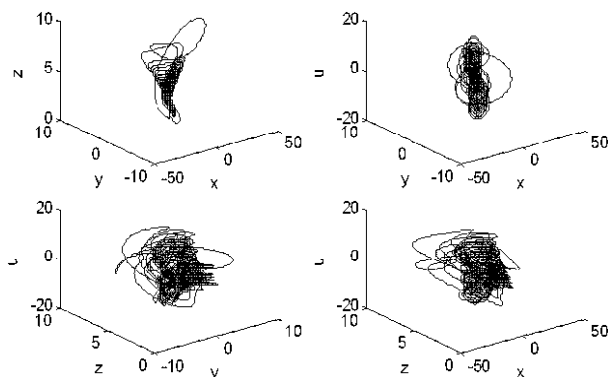
Fig. 1. Phase portrait of the hyper - chaotic system where q = 1
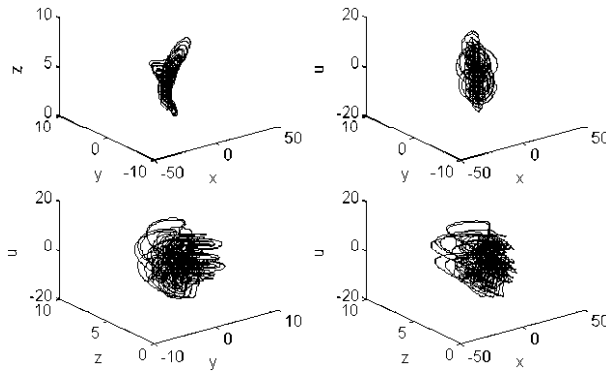
Fig. 2. Phase portrait of the hyper - chaotic system where q = 0. 95246

In figure 1, we provide the integral exponent of chaotic system three-dimensional phase diagram. Figure 2 is given the q = 0. 95 when system 3d phase diagram.

Fractional order nonlinear system to produce chaos phenomena in order of the range discussion: theory and numerical analysis.

Firstly, this festival will be given decision by integral exponent chaos system structure made corresponding homogeneous fractional systems (means higher order parameter for constant vector situation) appears chaotic characteristic of a necessary condition, here needs to use the following several lemma[5].

Lemma 1. when in the fractional order system $\dfrac{d^q X}{dt^q}=AX,(0<q\leq 1, X\in R^n)$ and $\left|\arg(eig(A)\right|>\dfrac{q\pi}{2}$, the balance point is asymptotic stability .

Lemma 2. when the fractional order $\dfrac{d^q X}{dt^q}\, f(X),(0 < q \leq 1, X \in R^n, f \in C^1)$, Remember X * to meet equation f (X) = 0 all balance, Then, when the, its balance X * local are asymptotically stable .
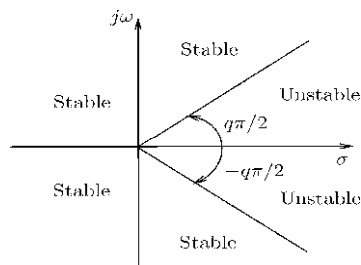
Fig. 3. Stab le and UN stab le region of the fractional l order system

Lemma 3. presumed lambda nonlinear system unstable equilibrium premises corresponding linearization of jacobian matrix eigenvalues, the corresponding the fractional order system: maintaining the necessary conditions for chaos: the eigenvalue lambda located in lemma 1 determined in unstable area, namely to meet:

Conclusion 1. the homogeneous fractional systems (5) chaos phenomena of higher order should satisfy the conditions q > 0.

In fact, homogeneous fractional hyperchaos LU system (5) is the only place the eigenvalues of the equilibrium O given. Instancing respectively is: lambda 1 = - 35.1015, lambda 2 = 0.3629, lambda 3 = 13.7387, lambda 4 = - 3), using the above lemma 0000 calculation available: q > 0 May generate chaos phenomena, and obviously it only is only (5) produce chaos phenomena in a necessary condition.

Further, below in figure 4, we provide the bifurcation parameter number is higher order parameter bifurcation diagram, from numerical results can be seen: only when q value is 0. 865 ~ 1 000, the system will appear more complex aspects of dynamic behaviors.
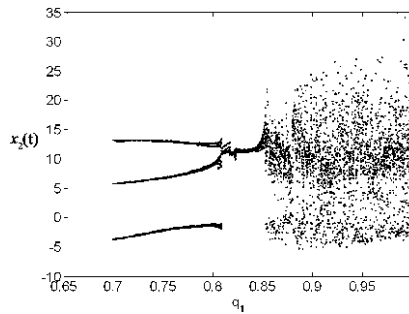
Fig. 4. Bifurcation graph of the hyper - chaotic system: state x2 (t) v. s. order parameter q

In the following discussion, we will only discuss (5) take chaotic higher order parameter (to be mixed Dun department number order points with steps of stockings) control system ask questions, of course, for the corresponding period, all kinds of circumstances theoretical analysis still stand.

4   Fractional Hyperchaos Lu System Generalized Synchronization

4.1   Generalized Synchronous Concept

First review the generalized synchronization of chaotic system concept. Consider the following two different fractional systems

$$
\begin{cases}
\dfrac{d^q X}{dt^q} = f(X), & (a) \\[3mm]
\dfrac{d^q Y}{dt^q} = g(Y, X) & (b)
\end{cases}
\tag{6}
$$

type (6a) represent the system for drive system, type (6 b) represent the system is controlled response system. Type variables meet

$$X \in R^n, y \in R^m, f:R^n \to R^n, g:R^n \times R^m \to R^m, X=(x_1,|x_2,\cdots,x_n)^T,$$

$$Y=(y_1,y_2,\cdots,y_m)^T, \frac{d^q X}{dt^q}=(\frac{d^q x_1}{dt^q},\frac{d^q x_2}{dt^q},\cdots,\frac{d^q x_n}{dt^q}),\frac{d^q Y}{dt^q}=(\frac{d^q y_1}{dt^q},\frac{d^q y_2}{dt^q},\cdots\frac{d^q y_m}{dt^q}).$$

If Y (t) orbit by driving signal X (t) only truly calm, namely response system state output Y (t) and driving system state X (t) meet some function relation, and in response system to attract domain, remaining to change in response to a system of initial Y (0), the system will tend with initial condition Y (0) unrelated solution, at this moment, we say Y (t) and X-ray (t) synchronization. When the two synchronization of chaotic signal, Y (t) and X-ray (t) may not equal, even their dimension can be different. This phenomenon is called two fractional system realizes the generalized synchronous (Gen-realized-Synchronization). Obviously, common-sense P-C completely in sync is generalized synchronous (GS synchronous) exceptions [6].

Note 1. the type (9) knowable, according to the matrix theory, for any reversibly matrix P, total can through proper selection constant matrix K,

4.2   Linear Generalized Synchronous Observer Design

According to common nonlinear system characteristic, generally, arose a drive system for concrete form below the equation:

$$\frac{d^q X}{dt^q} = AX + BF(X) + C \tag{7}$$

Based on the traditional observer theory, tectonic category response system is as follow: (8)

Type: $A \in Rn\ Xn$, B, $C \in Rn\ Xn \in Rn * 1$, $0 < q$ acuities 1, $P \in Rn\ Xn$ can be arbitrary full rank matrix, W m (X), w. s. (Y) respectively, and drive systems (7) and response system (8) state of output.

Easy to get, when W m (X), w. s. (Y) full enough one set, established the thing below theorem:

Theorem 1. (fractional order linear generalized synchronization of chaotic system theorem.

When (A, B) can control, measurable, W m (X) = PX, w. s. (Y) = Y] and, response system (8) and drive system (7) state output satisfy following evolution shut fasten: i.e., drive and corresponding system realizes the generalized synchronization and evolve over time, and finally response system state Y (t) and driving state X (t) meet relationships: Y = PX, specifically, says full rank matrix P for determination of the generalized synchronous state variables linear relationship of concrete relation matrix.

Proof. set e = Y - PX, according to the fractional order differential properties, by type (7), type (8)

$$\frac{d^q e}{dt^q} = \frac{d^q Y}{dt^q} - P \frac{d^q X}{dt^q} =$$

$$PAP^{-1}Y + PBF(X) + PC + K(W_m(X) - W_s(Y)) - P(AX + BF(X) + C) =$$

$$PAP^{-1}(Y - PX) + K(PX - Y) =$$

$$(PAP^{-1} - K)(Y - PX) =$$

$$(PAP^{-1} - K)|e$$

As: at the right of $\frac{d^q e}{dt^q} = (PAP^{-1} - K)e = \wedge e$ is: Λ = PA P - 1 - K .is real constant

matrix. According to lemma 3 $\left|\arg(\lambda^i_\wedge)\right| > \frac{q\pi}{2}$,

(i = 1, 2, ···, n, $\lim\limits_{t \to 0} \|e\| = 0$, as : $\lim\limits_{t \to +\infty} \|Y - PX\| = 0$.

Note 2: The type (9) knowable, according to the matrix theory, for any reversibly

matrix P, total can through proper selection constant matrix K, making $\left|\arg(\lambda^i_\wedge)\right| > \frac{q\pi}{2}$.

Then there will be e - 0 was founded, it means that two fractional chaotic system dynamics reached the proofs of generalized synchronous (GS.

Note 3: derived from above theorem proving had process may be seen, when can inverse matrix P to timing, want to design a given generalized synchronization of chaotic system linear response system, only need to take Λ = PA P - K all eigenvalues lambda Λ, (I = 1, 2,.., n) is located in fractional chaotic system, i.e. stable region can be located in figure 1 stab le area. Therefore, could start at any chosen according to the relationship Λ, then K = PAP - 1 - Λ sure response system (8) the concrete expression.

5   Conclusion

By using fractional order ordinary differential dynamic stability of system theory, this paper firstly by judging linearization of equilibrium constant after, sex, aided by bifurcation diagram analysis is presented, the numerical methods such as newly mention a modified hyperchaos Lu system corresponding fractional system to produce mixed Dun phenomenon order of the parameter scope, Further, design a kind of generalized linear synchronous observer, the observer dynamic behavior can with the original department tasseled realize arbitrary linear relationship of generalized synchronization and classic completely in sync, inverse-phase synchronization and projection synchronization method proposed in this paper can be regarded as the exception. Fang results of this study are to secure communication research in the field of person with partial reference value, in future studies, we also will further research realize arbitrary differentiable relations of the generalized synchronous observer design scheme, whether by using single scalar signal realizes synchronization observer design can surely be the next phase needs to be further studied the important lesson topic.

References

1. Podlubny, I.: Fractional differential equations. Academic Press, New York (1999)
2. Hartley, T.T., Lorenzo, C.F., Qamer, H.K.: Chaos in a fractional order Chua's system. IEEE Trans. CAS - I 42, 485–499 (1995)
3. Petrá, I.: Method for simulation of the fractional order chaotic systems. Acat Montanistica Slovaca 11, 273–277 (2006)
4. Ahmad, W.M., Sprott, J.C.: Chaos in fractional - order autonomous nonlinear systems. Chaos, Solitons & Fractals 16, 339–351 (2003)
5. Hu, G., Xiao, J.H., Zhen, Z.G.: Chaos control. Shanghai Press of Scientific Education, Shanghai (2002) (in Chinese)
6. Chen, G., Lu, J.H.: Dynamics and lysis, control and synchronization of the Lorenz system family. Scientific Press, Beijing (2003)

The Analysis of Fractional Chen Chaotic System Composite Structure

Zhen Liu[1], Wen-Xian Xiao[1], Ji-Tian Wang[2], and Wen-Long Wan[3]

[1] Network Center
[2] School of Information Engineer
[3] Foreign Language Department
Henan Institute of Science and Technology, Xinxiang, China, 453003
Xwenx@yeah.net

Abstract. In this paper, the range of order for the Chen's system behaving chaotic is investigated based on a necessary condition for the existence of double scroll attractor in fractional order dynamical systems firstly. Then, dynamics analysis of the fractional Chen's system is carried out numerically via bifurcation analysis based on the modified predictor-corrector algorithm for fractional ODEs. Furthermore, we investigated the compound contracture of frictional order Chen's attractor. It is found that, the constant controlling's strength value, which leads to the compound contracture, is closely related to the period-doubling bifurcation point of controlled system. Generally speaking, the higher the order parameter is, the larger absolute value of the constant controller will be, at which point it will occurs doubling period bifurcation in the controlled Chen's system. Our research has some hints for understanding the compound structure of the fractional order dynamical attractor similar with the Chen's attractor.

Keywords: fractional order Chen's system, predictor-corrector algorithm, compound contracture, constant control.

1 Introduction

Chaotic system has a complicated conduct of dynamics. According to the theoretical analysis and numerical simulation, we have found that we can express more exactly the conduct of dynamics in the chaotic system with the factional differential equations, which has been a heated issue in the scientific research field of nonlinearity. And that has been widely applied in the field of science, program and digital communication.

Since the chaotic system is sensible to initial value and unpredictable for a long time, chaotic control becomes a key problem to chaotic application. Moreover, there are many methods of chaotic control; and this essay based on the fractional order Chen system as a research object uses the method of adding constant controller on the right to the uncertain state weight of the system. Then, we discover that the fractional Chen system has a similar compound structure to the integral Chen system; Meanwhile, we discover that there is a close relationship between the constant

controller ´samplitude (which results in this compound structure) and the multiple circle bifurcation point of the controlled system.

2   The Introduction of Fractional Order Differential Definition and Common Estimate - Correction Algorithms Profile

In fractional calculus theory development process, the fractional order differential has the several definitions of [2], such as integral formulas, the fractional calculus definitions of Cauchy Grunwald - Letnikov (G - L), the fractional calculus definition of Riemann - Liouville (R - L) and Caputo's definition, commonly used is Riemann - Liouville (R - L)s', its mathematical expressions defined as follows:

$$_aD_t^q f(t) = \frac{d^q f(t)}{d(t-a)^q} = \frac{1}{\Gamma(n-q)} \frac{d^n}{dt^n} \int_0^t \frac{f(\tau)}{(t-\tau)^{q-n+1}} d\tau \tag{1}$$

In this formula, Γ is the Gamma function, $n-1 \le q < n$, n for an integer.

At present, there are a variety of means to analyze the implementation of fractional calculus computing algorithm .The most common used algorithms is mainly potter figure approximate algorithm and estimate - correction algorithm [2]. The following simple introduced by using the estimated - correction algorithms, namely the generalized Adams - Bashforth - Moulton algorithm. Consider the following differential equations:

$$\begin{cases} \frac{d^a y(t)}{dt^a} = f(t, y(t)) & 0 \le t \le T \\ y^{(k)}(0) = y_0^{(k)} & k = 0,1,\cdots,[q]-1 \end{cases} \tag{2}$$

Formula (2) and formulas (3) are equivalent

$$y(t) = \sum_{k=0}^{[q]-1} \frac{t^k}{k!} y_0^{(k)} + \frac{1}{\Gamma(q)} \int_0^t (t-\tau)^{q-1} f(\tau, y(\tau)) d\tau \tag{3}$$

Let them be: $h = \frac{T}{N}, t_n = nh, n = 0,1\cdots\cdots, N \in Z^+$

Formula (3) can be discretized as following: formula (4)

$$y_h(t_{n+1}) = \sum_{k=0}^{[q]-1} \frac{t_{n+1}^k}{k!} y_0^{(k)} + \frac{h^q}{\Gamma(q+2)} (f(t_{n+1}, y_h^p(t_{n+1}))$$

$$+ \sum_{j=0}^{n} a_{j.n+1} f(t_j, y_h(t_j))) \tag{4}$$

$$a_{j,n+1} = \begin{cases} n^{q+1} - (n-q)(n+1)^q & j = 0 \\ (n-j+2)^{q+1} + (n-j)^{q+1} \\ -2(n-j+1)^{q+1} & 1 \le j \le n \\ 1 & j = n+1 \end{cases}$$

$$y_h^p(t_{n+1}) = \sum_{k=0}^{[q]-1} \frac{t_{n+1}^k}{k!} y_0^{(k)} + \frac{1}{\Gamma(q)} \sum_{j=0}^{n} b_{j,n+1} f(t_j, y_h(t_j))$$

$$b_{j,n+1} = \frac{h^q}{q}((n+1-j)^q - (n-j)^q)$$

The inaccuracy between formula (3) and formula (4) is:

$$\max_{j=0,1,\cdots N} |y(t_i) - y_h(t_j)| = O(h^p)$$

3   The Degree Region Discussion of Chen's System Behaving Chaotic

First of all, let's discuss the stability of fractional differential. Generally speaking, comparing with the stability region range of integral order differentiation, fractional-order differential system is much larger. This point [3,4] can be found through comparing the stability region. Consider the following fractional order systems:

$$D^q x = f(x) \quad (0 < q \le 1, x \in R^n) \tag{5}$$

Lemma1 [5]: let system (5)'s equilibrium be x*(that is the solution of formula $f(x) = 0$), if, $A = \frac{\partial f}{\partial X}$, all the Jacobian matrix of (5)'s eigenvalue satisfies following formula at equilibrium:

$$\left| \arg(eig(A)) \right| > \frac{q\pi}{2} \tag{6}$$

Then kinetics of system (5) is stable.

Fractional order Chen's system can be described as:

$$\begin{cases} \frac{d^q x}{dt^q} = a(y - x) \\ \frac{d^q y}{dt^q} = (c - a)x - xz + cy \\ \frac{d^q z}{dt^q} = xy - cz \end{cases} \tag{7}$$

Among them: $0 < q \le 1$ for higher order parameter, a, b, c, q for the system parameters. According to the lemma 1, we know that the necessary condition of fractional order differential system to produce chaos phenomena is in system (7) unstable equilibria place, the corresponding jacobian matrix eigenvalues $A = \frac{\partial f}{\partial X}$ satisfy all conditions which the following type have:

$$\left| \arg(eig(A)) \right| < \frac{q\pi}{2}$$

From those, we can know that the scope of fractional Chen system to produce chaos phenomena is: $q > q^* (q^* \approx 0.82_{\circ})$

4   Fractional Chen System Composite Structure

4.1   Fractional Chen System Composite Structure

To study whether the same fractional order Chen system and the integer-order chaotic system with the same composite structure, we use the similar ways in the document of [1] and [6]. In the fractional Chen system the right of the second equation (corresponding to relatively less steady state component) is added with a constant controller $u(t) = m$. Control the intensity of the system when study the change of m the dynamic behavior in the system. At this point, the dynamic equation of the controlled system can be expressed as follows:

$$\begin{cases} \frac{d^q x}{dt^q} = a(y-x) \\ \frac{d^q y}{dt^q} = (c-a)x - xz + cy + m \\ \frac{d^q z}{dt^q} = xy - bz \end{cases} \tag{8}$$

Taking the parameters a=35, b=3, c=28, when the use of predictor - corrector algorithm are taken, we can get the three-dimensional phase diagram of the system, are shown in Figure 1and Figure 2 respectively.
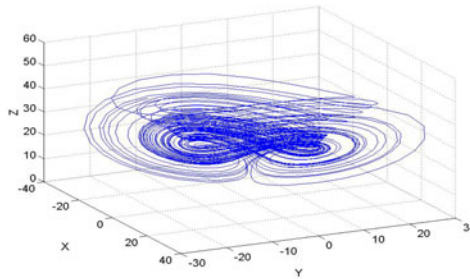
Fig. 1. Fractional three-dimensional phase diagram of Chen chaotic systems: .q=1
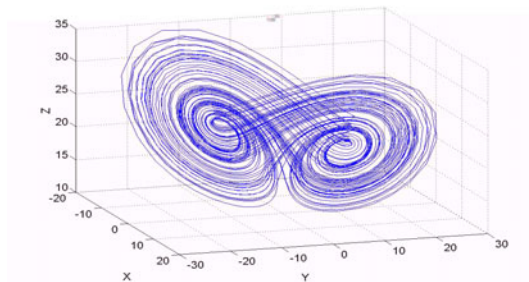
Fig. 2. Fractional Chen chaotic system phase diagram: q=0.90

In particular, when $q=1, -150 \leq m \leq 150$, Figure 3 shows the second component of the system state to control a constant state of change in the bifurcation diagram.
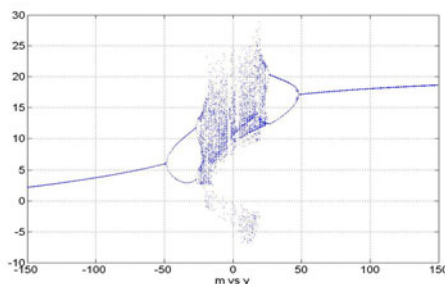
Fig. 3. The bifurcation diagram on the m in the fractional Chen system: q=1

The Figure 3 reflects in the bifurcation diagram (8) the variation of the same law in the document of [1] and [6] .Namely, when $|m| \geq 49$, the system is the limit cycle, the system is periodic; when $24 \leq |m| < 49$, the degradation becomes the left or right half of the attractor. When q=0.95, m=15, 24, 35 respectively, Figure 4,5,6 are corresponded to three-dimensional phase diagram of the system.
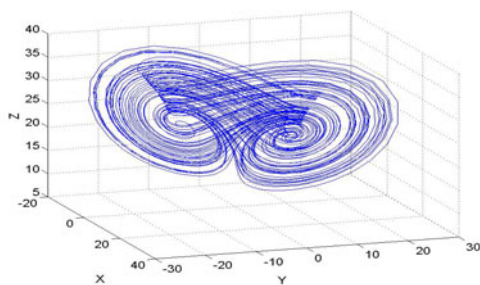
Fig. 4. Three-dimensional fractional Chen system, the phase diagram: q=0.95, m=15
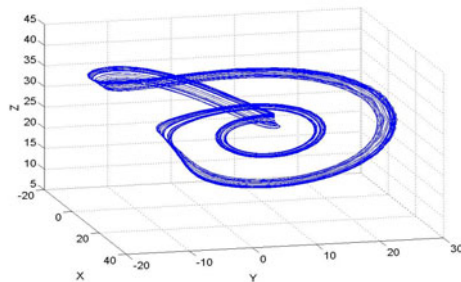
Fig. 5. Three-dimensional fractional Chen system, the phase diagram: q=0.95, m=24
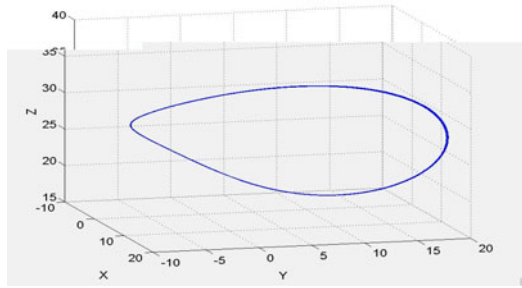
Fig. 6. Three-dimensional fractional Chen system, the phase diagram: q=0.95, m=35

4.2 The Relation between the Period-Doubling Bifurcation Point of Controlled Fractional Order Chen's System and the Control Intensity

The next, we are conducting a similar study on the relation between the period-doubling bifurcation point of controlled fractional order Chen's system and the control intensity. The figures 7, 8, 9 respectively show the order of the fractional order system's correspondence bifurcation diagram as 0.85, 0.90, 0.95.

Numerical results show that the fractional order Chen's system represents the same characters with the compound constructure. Besides, figures 10, 11 also give the partial bifurcation diagram of fractional order Chen's system whose order is 0.95. From left side (or right), a line which passes through the period-doubling bifurcation toward the chaos (or period) can be seen clearly.

By abundant numerical simulation study, we find that the constant controlling's strength value, which leads to the compound constructure, is closely related to the period-doubling bifurcation point of controlled fractional order Chen's system. Generally speaking, the higher the order parameter is, the larger absolute value of constant controller will be, at which point it will occurs doubling period bifurcation in the controlled Chen's system. Our research has some hints for understanding the compound structure of the fractional order dynamical attractor similar with the Chen's attractor. The intrinsic motivation in this character that occurs needs our further research and exploration.
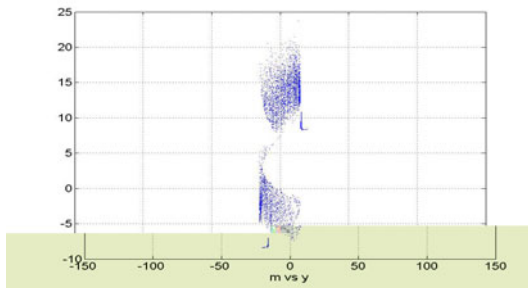
Fig. 7. Bifurcation diagram about "m" of the fractional order Chen's system: q=0.85
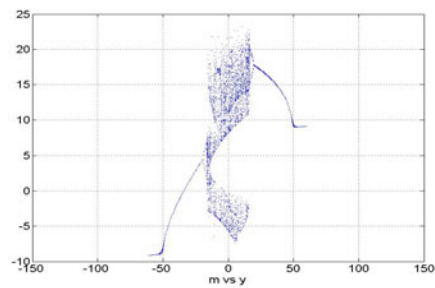
Fig. 8. Bifurcation diagram about "m" of the fractional order Chen's system: q=0.90
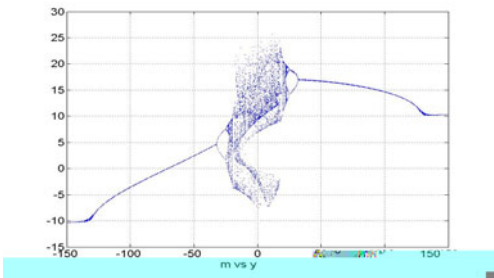
Fig. 9. Bifurcation diagram about "m" of the fractional order Chen's system: q=0.95
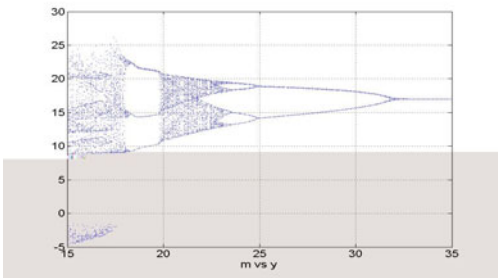
Fig. 10. Partial magnified diagram about "m" of the fractional order Chen's system: q=0.95
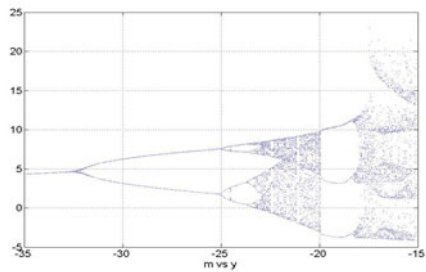
Fig. 11. Partial magnified diagram about "m" of the fractional order Chen's system: q=0.95

5   Conclusion

This paper is the case study on the fractional order Chen's system, which is based on the modified predictor-corrector algorithm for fractional ODEs, and finally defines the range of the order for Chen's system behaving chaotic. Then, we investigate the compound constructure of fractional order Chen's attractor and find some numerical regulations. The research method of this paper can be applied in other similar dynamics analysis.

References

1. Lu, J.G., Chen, G.: A note on the fractional order Chen system. Chaos, Solitions and Fractals 27(3), 685–688 (2006)
2. Diethelm, K., Ford, N.J., Freed, A.D.: A predictor corrector approach for the numerical solution of fractional differential equations. Nonlinear Dynamics 29(1), 3–22 (2002)
3. Matignon, D.: Stability results of fractional differential equations with applications to control processing, pp. 963–968. IMACS, IEEE-SMC, Lille, France (1996)
4. Tavazoei, M.S., Haeri, M.: A necessary condition for double scroll attractor existence in fractional order systems. Physics Letters A 367, 102–113 (2007)
5. Lu, J.H., Zhou, T.S., Chen, G., Zhang, S.C.: The compound structure of Chen's attractor. Int. J of Bifurcation and Chaos 12(4), 855–858 (2002)

The Design and Implementation of MP4 Coding System Based on S3C2410

Guo-Hong Gao, Xue-Yong Li, Shi-Tao Yan, and Jin-Na Lv

School of Information Engineer
Henan Institute of Science and Technology, Xinxiang, China, 453003
914747841@qq.com

Abstract. MPEG (Moving Pictures Experts Group) is an important digital audio compression algorithm. It is valued in the audio coding. This paper discusses the MP4 system based on S3C2410 development technology, has studied the MPEG-2 audio frequency code algorithm standard with emphasis, using S3C2410 (ARM9-core processor chip) designed a MP4 system. Finally has achieved the design requirements through the test.

Keywords: S3C2410, MP4, MPEG-2, Audio encoding.

1   Introduction

MP4 audio coding system is the MPEG-2 standard coding algorithm. MPEG-2 audio coding can be provided in left and right and two surround channels, as well as a heavier bass channel, and up to seven audio channels. Since MPEG-2 treatment in the clever design, makes the most of the MPEG-2 decoder can also play MPEG-1 format data, such as MP3. MPEG-2 encoding bit stream is divided into six levels. To better represent the encoded data, MPEG-2 with a syntax provides a hierarchical structure. It is divided into six layers, from top to bottom are: image sequence layer, group of pictures (GOP), picture, macro block section, the macro block, block. Since the 80's, due to integrated circuit production techniques and digital signal processing theory, the continuous development, ARM chip has made rapid development, increasing the performance of the microprocessor, costs continue to decline, can be done to achieve a lower cost real-time processing of large amounts of data, its processing capacity has been greatly improved, so that the ARM chips used widely. Based on this, choose to S3C2410ARM9 high-performance chip for real-time audio encoding.

2   MP4 Coding Principles and Technology

MP4 encoding algorithm process can be divided into three parts: the time-frequency mapping, psychoacoustic model and quantitative and coding. Time-frequency mapping part of which includes sub-band filters and MDCT (modified discrete cosine transform), psychoacoustic model of the building to the 1024-point FFT computation, quantization coding, including bits and scale factor allocation and Huffman coding, as shown in Figure 1 instructions.
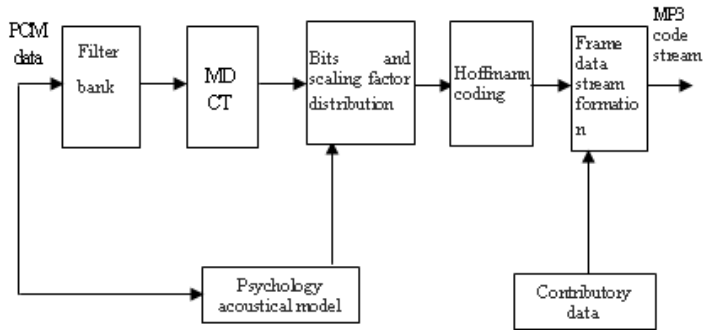
Fig. 1. MP4 encoding algorithm process

PCM sample values into the first sub-band filter banks, the sub-band filter evenly divided into 32 sub-post-band signal, each sub-band contains 18 sample values, and then again for each sub-band MDCT transform, thus spaced by 576 samples in frequency domain values.

The time-frequency transform obtained values of left and right channel frequency-domain samples to be carried out according to the required mode channel mode processing, MP4 standard provides a 5-channel mode:

(1) single-channel mode: only one channel model.

(2) Dual channel mode: with two independent channels model.

(3) Stereo Mode: two-channel and two channels with a certain correlation between the patterns.

(4) Intensity stereo mode: It is in stereo mode, based on the scale factor band for some kind of value, only the sum of left and right channels and the coded sub-band energy to get higher compression rates.

(5) And differential stereo mode: on the left and right channel frequency-domain samples and the difference between value and values are encoded in stereo mode.

3   MP4 Coding System

3.1   The Overall Design of the System

The system is based on S3C2410 chip as the main part of the encoder, which is mainly collected by the audio module, compression module and the data communication module consists of three parts. As shown in Figure 2.

First, the input analog audio signal amplification, and then the signal from the audio processor, A/D conversion, into PCM(pulse code modulation) format for digital audio signals. MP4 encoder encodes the input digital signal, compressing the data stream with the MP4 format, MCU receives the compressed stream, and after certain treatments, it is stored in the MP4 player's memory.

MP4 encoder is the core of the whole system, it is a high performance ARM9 S3C2410 chip components. S3C2410 is the core processor, its working frequency up to 240MHz, is used to complete real-time compression algorithm. Through multi-channel buffered serial port to DMA directly receive digital audio data, and in the establishment of frame buffer RAM chip. Through the EMIF port, connects to the
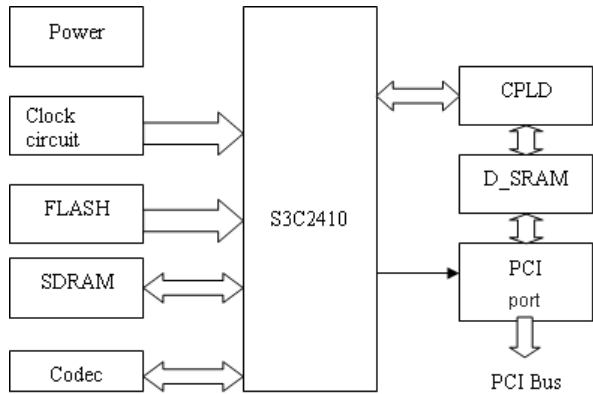
Fig. 2. Real-time hardware encoder block diagram

industry standard high-capacity, high-speed SDRAM memory devices to meet the storage requirements of audio data; programmed application stored in the chip FLASH Memory, the system power on, S3C2410 chip plus the application loader set to the on-chip high speed RAM in the system is realized off-line operation. Due to time and other influences, far as the system in this part provide an explanation.

3.2   SDRAM Interface Design

SDRAM by Micron's MT48LC2M32B2, the device is a high-speed synchronous dynamic level COMS RAM, storage capacity is 64Mbit. Working voltage is 3.3V, compatible with LVTTL level, to support read and write burst mode, the refresh period 64ms. The maximum clock up to 100MHz, 80MHz synchronous interface work in EMIF clock state. Column address can be changed within each clock time. Figure 3 shows the diagram of SDRAM interface with the processor.
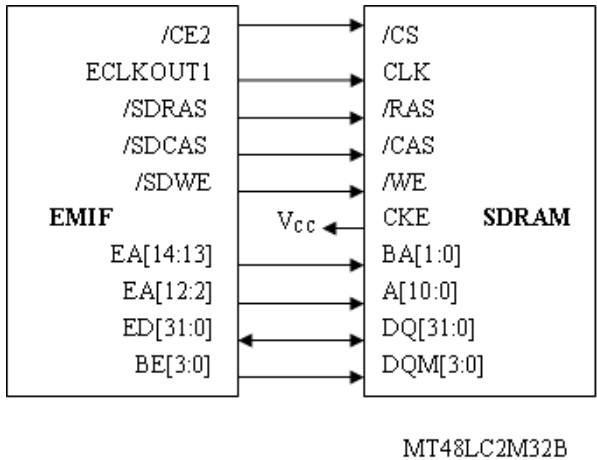
Fig. 3. SDRAM external memory interface diagram

3.3   MP4 Encoding Program Design

Audio coding using C language program to realize the audio coding standard MPEG-2 encoding. Program completed by the main program and subprograms various functions, procedures, structured writing, debugging and maintenance is very convenient. Program is structured as follows:

(1) The main program .Main function is to call each subroutine, to complete the appropriate signal processing. In the main program, the program can accept a variety of encoding parameters, such as encoded MPEG audio bit rate, channel selection, mental model selection, stereo mode selection. Defined in the main signal processing in the intermediate variables generated by the buffer, according to the parameters set, the audio signal on the input alignment, respectively, and call the sub-band filtering subroutine psychoacoustic model, according to mental model output Pair with a cover letter than the value of filter output samples to quantify and coding.

(2) Sub-band filtering. Each sub-band filtering subroutine 1152 audio input samples, which constitute an audio sample frame. 1152 audio samples, each 576 as a set of input, resulting in 586 sub-band sample output, and a total output of 2 groups. Each output sample of the corresponding sub-sub-band 32 sub-band filter with the output of the 18 samples of each sub-band.

(3) Psychoacoustic model .Psychoacoustic model calculation of the 1152 audio sample cover letter of each sub-band ratio, calculated cover letter will be used for sub-band than the quantification of sample trees.

(4) Framing bit allocation and quantization .Bit allocation is based on psychoacoustic model letter of mask output ratio of the sample for each sub-band bit allocation. The bit allocation sub-band samples after the samples were quantified with a pair, the last formatted encoded bit stream.

4   System Test Results Analysis

Through comprehensive system testing, results showed that the code rate of 128Kbps CD or Walkman in the recorded music program, with the MP4 player, playback, get very good sound effects. Found no identifiable noise, at the end sound full, rich treble, MP4 player, fully meet the quality requirements of the music. 16Kbps bit rate by recording the site language is clear, the introduction of the noise is very small, since more than a 32Kbps audio playback quality of ADPCM coded voice playback quality, and store more energy than double the ADPCM encoding format. Also, because the system's hardware configuration is reasonable, software programming tight, so the stability of the system is relatively high, the product is very small probability of crashes. In addition, to using a variety of measures to reduce system power consumption, making a battery 7 to 8 hours of continuous recording, reaching the advanced level of similar products, enhanced product market competition. However, due to a number of factors, problems, and to meeting the broader needs of the public.

5   Conclusion

In this paper, MPEG-2 audio coding algorithm based on analysis and research, using S3C2410 MP4 encoding algorithm implemented hardware and software design. Through comprehensive testing system, the results show that the system stability, low power consumption, reaching the advanced level of similar products.

References

1. Zhu, W., Wang, Q., Ma, H.: Design of Embedded Network Interface Based on ARM9. Microcomputer Information (September 2007)
2. Cirruslogic. CS8900A Product Data Sheet. Cirrus Logic, Inc., Texas (2001)
3. Li, W.: Research on Network Loading Balancing Based Intelligent Dns. Journal of Beijing Technology and Business University (May 2008)
4. An implementation method of embedded network interface. Journal of Nanyang Normal University (December 2009)
5. Xun, L., Shui-Dong, X.: Embedded Ethernet Interface Development with DM642. Computer Engineering (August 2007)

The Applied Research of Simple Pendulum Experiment Based on the Photoelectric Timing Circuit Technology

Qiang-Lin Su[1], Guo-Hong Gao[2], Jun-Jie Cen[1], and Ji-Tian Wang[2]

[1] Department of Computer Science & Technology
Henan Mechanical and Electrical Engineering College, Xinxiang, China, 453003
[2] School of Information Engineer
Henan Institute of Science and Technology, Xinxiang, China, 453003
`914747841@qq.com`

Abstract. This paper describes the working principle of photoelectric timing circuits, and puts forward the photoelectric timing circuit design and realization method and explains the photoelectric timing circuits which applies to physical pendulum in details, and discusses simple the circuit application error causes, finally proposes the expansion of the photoelectric timing circuits in applications.

Keywords: Photoelectric timing, Clock, Single pendulum experiment, Measurement error.

1 Introduction

Photoelectric timing circuits also called Electro-optical gate, which makes use of the variation of mechanical motion position in optical path shaping and reflection, and it does not exposes to detect effectively object displacement and time so that it can measure objects movement speed quickly, which is widely used in industrial automation production control, transportation, and measurement fields. According to the different fields of application, photoelectric timing circuits can be classified a simple circuit, which bases on single-chip devices in the measurement circuit and digital circuit primarily[1]. SCM in photoelectric gate can not only achieve time direct measurements but also realize other physical parameters calculation and control through the software. Electro-optical gate physical experiment in the application is mainly to the time measurement instead of previous artificially stopwatch, making the experiment data measure results not only is fast but also precise and reliable. Experiments of timing circuits in physics uses simple digital systems in general.

2 Circuit Design of Principle

2.1 Circuit Design Basis

Physical exercise of measurement in Physical experiment mainly researches model as the object, due to the object of small size, it determines the measurement system using optical path distance in the selection of short in general, such as rigid-body dynamics inertia experiments of photoelectric sensor. According to the measuring objects of the

different nature, light path generates available laser, visible and infrared, accept parts choose photoconductive resistance and photoelectric diode. According to the particularity of movement, it can choose the penetration and reflected light way[1].

In order to improve the measurement precision, counts circuit output by many data show that counts circuit of the clock decides circuit of measurement errors in important factors, it can use multiple resonance swings circuit in less demanding experiments, while in high accuracy requirements of experiment needs crystal oscillator circuit, through separate frequency get counts circuit external clock and timing circuits output data bits, the more clock, the higher the frequency, the circuit reliability requirement higher[2].

In this paper, the measurement circuit to eliminate physics experiments in other objects of the strength of the influence of light using infrared sensor, the clock frequency for 100 Hertz, measurement accuracy for milliseconds orders of magnitude.

2.2 Circuit Design Principle

The photoelectric timing circuit mainly includes sensor circuit, clocking produce circuit, count and display circuit, control circuit and power circuit five sections.

1) Counter and display circuit

Using CMOS device 4543 and small amounts 4553 and separation devices to realize three decimal count and data output, in Figure 1, 4553 is three decimal add counter, 4543 is digital decoding drive. CP stands for clock input, CR stands for reset control. Digital tube uses common cathode type.
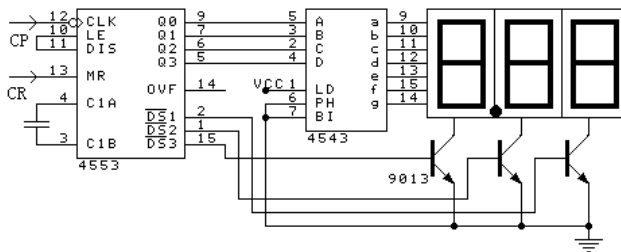
Fig. 1. Photoelectric timing circuit

2) Clock generator

As shown in Figure 2.This circuit adopts 455KHz crystal oscillator circuit, after 45.5 times, it finally obtains separate frequency 100Hz cycle for 10ms signal. The decimal add 4518 counter realizes Separate frequency circuit.
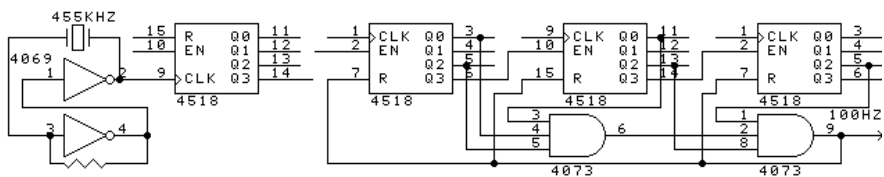
Fig. 2. Clock generating circuit

3) Sensor circuit

Sensor uses LM324 operational amplifier circuit and amplification of the signal driven R-S flip-flop to realize the counts circuit of the gate control, show in Figure 3.
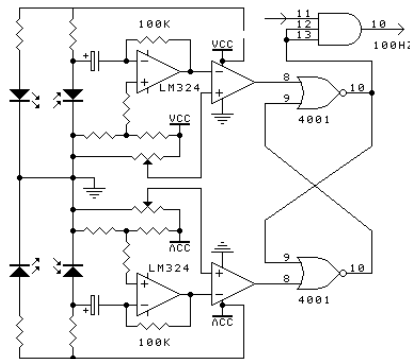
Fig. 3. Sensor circuit

3   Circuit Assembly and Debugging

3.1   Each Unit Circuit Experiment

According to above each unit circuit principle, at first, it needs the connection and testing in digital electronic experiment box, after achieving the desired effect, each unit circuit can be combined into a complete circuit system to have a overall test. Circuit also can use the software schools Bench computer-aided simulation to test the feasibility of the circuit.

3.2   Circuit Design

To achieve this software available PROTEL digital system of the circuit principle diagram editing and circuit design. It improves working efficiency
with computer aided design.

Protel software consists of the circuit principle chart and design program, the simulation program, devices editing program, network output programs, device list output programs and printed output programs etc[3]. Portel software design main steps are: circuit boards of the device layout, device pad attachment namely wiring, circuit device calibration, devices tagging, print, etc[4].

(1) Circuit device layout. Device layout can use the principle diagram generation network file to have an automatic layout. Automatic layout demand principle diagram of each component have encapsulation shape, it also requires to draw circuit board appearance size at first and then it can place components automatically. Device layout also can operate in manual way, this operation will draw good circuit board appearance size firstly, and then operate manual layout. Components design layout is the most critical work, whether the device boards placed reasonable or not directly affects circuit electrical properties and electric equipment manufacture craft. In components should be paid attention to the operating process layout of the following

points: device layout wants to device for reference, the device packaging appearance between has certain interval to avoid dimension is too narrow to carry on the circuit assembly; Device layout for PCB fixing hole should be as far as possible and leave a certain size Device layout whether arrange them or mix row, it must cater to the circuit of the electrical characteristics.

(2) Device pad attachment. PCB pad attachment includes automatic and manual operation. Automatic wiring, first sets up some wiring parameters in automatic wiring, such as the line width, irrelevant spacing, line and pad spacing, then makes use of recycle principle diagram generation network file for automatic wiring. Because automatic wiring line width size is so single that it doesn't fit most of the audio circuits, and automatic wiring rate cannot achieve 100%, the computer automatically wiring is not ideal instead of manually wiring. Although manual wiring is a bit slow, the connecting mode, the randomness and wiring type of arbitrariness, making the wiring results become beautiful, meanwhile meet the electrical characteristics of circuit. In addition, in circuit design, the power cord and ground should have enough line width, small power unit and high-power unit as far away as possible, and each self-supply wires need filter pieces. High power devices use few thicker lines, circuit boards attachment and device pad as the largest area occupies board.

(3) Circuit board draft diagram output. Finally using laser printer output. According to different production circuit board crafts, output mediums are in difference, such as using a little   stamping process to make electricity board and print medium for sublimation dedicated transfer paper.

3.3   Circuit Board Production

There are several ways of making circuit board, transfer for circuit board is a method of making circuit board in recent years. Making fine craftsmanship is its characteristic, whose line have a spacing and less than 0.2 mm, smooth without jagged and can be used for double-sided making[5]. Its production process includes: Firstly, putting the made PCB board in hot conversion on paper prints with the ratio of using laser printers. Secondly, making use of fine sand paper to clean copper board and flat round, and then cover the printed thermal transfer paper into the copper board, and send it into photos color-printed machine(temperature transferred to 180.5℃~200℃) and press for several times to make melt pressure toner completely absorption in apply copper. After cooling of the copper board, peel of heat-transfer paper and take it into hydrogen peroxide + hydrochloric acid + water (1:2:3) mixture, it can be formed after work fine corrosion of printed circuit boards. The corrosion process is so quick that it is easily to see the circuit board corrosion degree in mordant transparent corrosive liquid.

4   The Application of Photoelectric Counting Circuit in the Measurement of the Gravity Acceleration

4.1   Measuring Principle

Pendulum also known as the mathematical pendulum, it is a fixed point with no elongated massless line. There is a ball whose mass is m hanging in the end of the

line, and the ball can be considered as particles. To pull away from the equilibrium position of the ball after the free hand, the small ball will do reciprocating movement in the vertical plane. During the experiment, it can not only measure small-ball in the bottom two consecutive time intervals with a photoelectric timing circuits but also can measure the total time of 30 times.

It can be proved that when the swing angle is small (less than 5°), pendulum motion can be approximated as simple harmonic motion, its period is

$$T = 2\pi\sqrt{L/g} \tag{1}$$

If can measure the pendulum swing long L and the corresponding period T, criterion

$$g = \frac{4\pi^2 L}{T^2} \tag{2}$$

Of course, the ideal pendulum does not exist actually, because suspension wire has a quality. Strict speaking, small ball is not a particle, so it is necessary to amend the coping style. Place long application pensile point and centre distance between replace namely, including line length, r pendulum radius. If fixed place long L and the corresponding vibration period T can be measured, it can use the type to make out the g.

In order to improve the measurement precision, L0 value should be selected larger. When measures the cycle, it needs to measure the swinging 30 or 50 cycles of time t, then find out a swing time used, namely cycle:

$$T = \frac{t}{30} \tag{3}$$

4.2   Error Analysis of Measured g in Pendulum System

This experiment based on the formed theoretical formula (2) is in some conditions: 1) Pendulum ball's the diameter d should be less than that of suspension line length L. 2) Suspended line quality u should be far less than quality m. 3) Swinging angle should be small. 4) Ignorance of air of buoyancy and resistance effects. These four influences caused the errors   are system errors, they are from theoretical formulas required conditions in the experiment failed to well meet, so belong to the theory method error. It should be amended for precise measurements of each of the results Correction formula for (derivation is abbreviated)

$$g = 4\pi^2 \frac{L}{T^2}(1 + \frac{2r}{5L^2}^2 - \frac{1u}{6m} + \frac{1}{8}\theta^2 + \frac{8\rho_0}{5\rho}) \tag{4}$$

r is the ball radius, ρ is the density of air, ρ_0 is the density of balls

Besides, the usage of stopped clock, meter scale and ro-distance measuring device will certainly bring instrument error. Finally, the position of mad self-alignment pivot and determine the well, timing method without correctness will lead to system error[5]. This error is due to the poor measurement by the observer, it should be avoided as much as possible. Experimental procedure is as follows:

1) fixing the single pendulum device well.

2) using spiral micro-distance measuring device to measure ball diameter d for three times and make out the average.

3) determining the suspended o 'clock position and measuring L0 of cycloid long for three times and getting the average

4) measuring 30 times time t with timer swinging and swinging Angle should less than 5°.

5) calculating L and T values, and the formula (2) numerical calculation g. Note: in order to prevent several wrong n value, it should count "zero" at beginning.

After each a cycle, 1, 2, 3,..., n. When placed over balance position into table clock can reduce the error, in addition to select the right movement point of reference.

5   Conclusion

The application of photoelectric timing circuits physics experiment, according to the different measuring objects, it can use different sensors platform. In single pendulum measurement experiment, sensor platform requires the certain precision. Sensor platform needs an accurate adjustment before experiment so that it can make the whereabouts of the ball in athletic process just blocked with infrared light path. Sensor position should be placed under a certain distance from the liquid surface to make the ball movement to the sensor become a speed of uniform motion.

The accuracy of circuit clock is a major reason on a circuit's electrical measurement error. Sensor signal processing circuits of the output pulse width also have a certain effect on circuit measurement error, but the photoelectric timing circuits for physical macro the movement of objects measurement, due to the lesser speed, it can ignore such factor.

The application of photoelectric timer circuits are introduced in single pendulum measurement, if the experiments requires multi-group data, the circuit needs to design data storage circuit, such as rigid-body dynamics inertia measurement, of course, the circuit will become complicated. Besides, it is also widely used in other measurements. For example, in viscosity coefficient measured experimental application, the application in velocity measurement, the application in object bounding experiment, application in highway speed measuring.

References

1. Lin, Q., Wang, J.: Design of Intelligent Irrigation System Based on Embedded Technology. Communications Technology 42(05) (2009)
2. Nguyen, T.-K., Kim, C.-H., Gook-JuIhm: CMOS Low = noise amplifier design optimization techniques. Microwave Theory and Techniques (IEEE Transactions on) 52(5), 1433–1442 (2004)
3. Xie, S., Li, X., Yang, S.: Design and implementation of fuzzy control for irrigating System with PLC. Transactions of the CSAE 23(6), 208–210 (2007)
4. sourceforge project, MC9S12NE64 OpenTCP Reference Manual (EB/OL), http://freescaleotcp.Sourceforge.net (July 2004)
5. Costa, J.A., Patwari, N., Hero, A.O.: Distributed multidimensional scaling with adaptive weithting for node localization in sensor networks. IEEE/ACM Trans.Sensor Networks, http://www.eecs.umich.edu/~hero/com.html (to appear)

The Design of Recording System Based on LM386

Guo-Hong Gao[1], Zhen Liu[2], Hong-Yan Jiao[3], and Ji-Tian Wang[1]

[1] School of Information Engineer
[2] Network Center
[3] Xinke College
Henan Institute of Science and Technology, Xinxiang, China, 453003
914747841@qq.com

Abstract. The paper analyses the voice of storage technology development and application of scientific and introduces the LM386, 6264 0804, 0832 etc, several important integrated circuit of the functions and application methods. The point presents based on LM386 voice storage and playback system design processes and methods, designing the voice of storage system and realizing the circuit voice storage and playback function, it meets the design requirements after test.

Keywords: Voice storage, Replay, Sampling frequency, A/D, D/A.

1   Introduction

There is a voice since the human beings have existed. A voice makes our life more colorful. With the development of science, voice storage technology has a step-by-step improvement. Modern people make the sound digitalized through integrated circuit, and make the voice more accurate, clear and the existence lasts for a long time. Nowadays, voice storage technology has been already applied in a wide field, such as medicine, education, research, spaceflight technology, which drives the development of our era[1].

   If you want the sound to digital storage, the first step is to digitize the sounds, digital is actually sampled and quantified. In an ideal state, the period of time the maximum number of selected sampling points, and the status of sampling points used to describe the infinite small, then the waves can be almost perfect recording and playback. However, due to equipment limitations and the digital storage capacity limit, we can only take a certain period of time a certain number of sampling points, and the state of the sampling points can only use a limited number of states to represent. According to theory, the sampling frequency of not less than twice the highest frequency sound signals, so the expression will be able to digitally restore the original sound of the voice, so, with 8kHz sampling frequency of the sound collected on it. The sample size is the number of bits for each voice sample bit /s (bps) said, it reflects the sound wave amplitude measurement accuracy[2]. In the past, 8-bit sampling precision in describing the sound will face the problem of insufficient accuracy. Now, 16bit/44kHz audio indicators are also widely used, we often heard the CD is the same precision. 24bit/192kHz basic specifications have reached the limits

of human hearing. However, the accuracy of Digital can continue to improve, it was discovered that the computer is always with digital sound taste, and there is always the voice of the real distance, increasing the precision of digital sound, while other people are doing the exploration.

2   Sound Storage Circuit

2.1   Physical Characteristics of Sound Signals

In essence, the sound is a continuous wave, known as sound waves. There are two basic parameters of sound: a sound range, the magnitude of the sound level, also known as the volume; the other is the sound frequency, that is, the vibration frequency of sound waves per second, as a unit with HZ or KHZ said. High frequency sounds, sounds sharp, low frequency sounds, low sounds. The sound signals stored in the computer should go into the need to continuously variable waveform signal (called analog signal) into a digital signal, because the computer can store only digital signals. The analog signals into digital signals (DAC) are generally the sound signals sampling and conversion two steps to complete. The so-called analog signal sample collects sound samples, and then converts to digital signals. Sampling capabilities of the computer the size of the sound are also used to measure two parameters: the sampling frequency and sound samples of digits. As we all know, the sound has three basic characteristics: tone, pitch, timbre. The three characteristics determine the voice of each of us difference[3]. The sound field in the human ear range, the sound of the subjective experience of hearing the main psychological loudness, pitch, timbre and other characteristics and masking effect, high-frequency and orientation characteristics. Including loudness, pitch, timbre can be used to describe a subjective amplitude, frequency and phase three physical parameters of any complex sound, it is also known as the voice of the "three elements"; loudness, also known as the sound intensity or volume, it represents the strength of sound energy level, depending on the size of the sound wave amplitude. The strength of normal human hearing range is 0dB-140dB (It was also considered to be-5dB-130dB). As known as tone pitch, tones of voice that the ear level of subjective feelings. Objective voice pitch depends mainly on the level of wavelet frequency, high frequency tone is high, and vice versa is low, in Hertz (Hz) said. The feeling of the human ear as a frequency from the lowest to the highest audible frequency of 20Hz 20kHz audible frequency range.

2.2   Sound Signals Stored Procedure

The circuit system consists of amplifiers, memory, counters and other devices composition. First, the sound through the audio circuit sensor acquisition, processing through the release device, and then through the ADC A/D conversion, and then after memory storage, and then through a digital to analog converter D/A conversion, and then after Amplification of a power amplifier, at last, to restore the sound emitted by the speaker[4].

The voice storage system includes three subsystems, they are sound processing, signal storage, audio playback, the three subsystems, in which the three subsystems, the most important is the second processing, following the process I will explain in details:

1) Signal Processing

This subsystem consists of the microphone, amplifier, filter, AD converter. Sound sampling the analog signal into the amplifier through the pickup, in which we use the integrated circuit LM386, LM386 is a very flexible use of the device, which can be accessed 7 pin decoupling capacitor, 1, and can be accessed by an 8-pin 10uF capacitor and a (1K ~ 20K) resistor to control the magnification. LM386 also has a wide frequency response, low power consumption using voltage range, circuit external components, when used without additional heat sink characteristics, which is one of the reasons the use of this manifold[4]. Because of its coexistence with the amplification and filtering functions, so we do not find filters, and save the component. The LM386 in this circuit connection process shown in Figure 1.
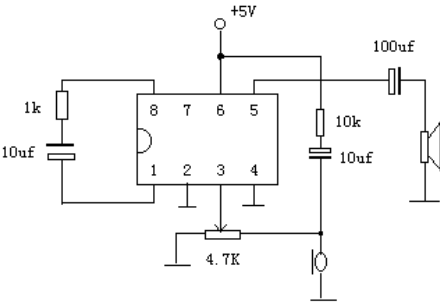
Fig. 1. LM386 circuit diagram

This process is mainly used in the LM386 to amplify the sound signal waveform, and filter out noise, the more smooth the waveform, and then wave to the ADC in the ADC. This ADC uses integrated chip ADC0804, ADC0804 is a CMOS integrated process with relatively mold made of the number of successive conversion chips, a resolution of 8 bits, conversion time 100uS, so the sampling frequency up to 10kHz, input voltage range of 0~5V, the chip 9 pins for the reference voltage power supply terminal, its input voltage range is about one-half, such as input voltage range is 0.5~ 3.5V, 1.5V increase in 9-port voltage. When the input voltage is 0~5V, then the 9-port without adding any voltage, derived from the internal VCC supply voltage. Finally, by ADC386 analog signals into digital signals, then this signal sent the memory, the storage subsystem to deal with. The process of ADC circuit connection, as shown in figure 2.
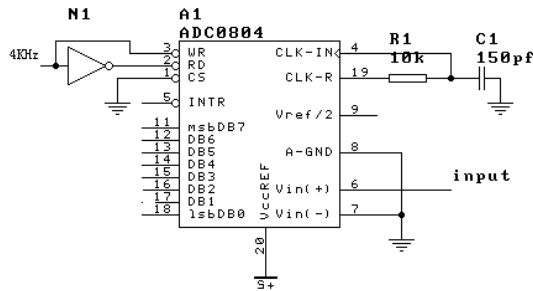
Fig. 2. ADC0804 circuit connection diagram

ADC0804 pin functions are as follows:11~18, the amount of 8-bit digital output, DB7 is high, DB0 is low, the tri-state latch output, the data output bus structure can be used; 20 for the supply side, then 5V voltage; 6 and 7 as analog voltage inputs, a differential amplifier circuit, it can maximize the common mode noise suppression, and can compensate for zero common-mode input voltage, if the input voltage is positive, the input from the 6th, 7 ground; if Input voltage is negative, the input from the 7, 6, grounding; 19 end of the internal clock pulse when the device itself provides the clock, only one external resistor and capacitor, can produce a certain frequency of the clock pulse. Shown, when R = 10KΩ, C = 150PF time, f ≈ 640KHz, for the A / D converter to use; 4 as the external clock input is also provided by the internal clock pulse, as shows; 8 analog To end; 10, a digital to end; 5 as output control terminal, active low, when the end of the first analog-digital conversion, 5 from the high to low, it can be used for computer interrupt request signal. The next time the start of conversion and 5 from low to high automatically; 1, 2 and 3 as input control terminal. When both CS and WR low, they will start conversion; when the WR from low to high, the conversion began. In the conversion process, if re-start converter, the suspensions of the ongoing conversion, the new processes of converting the contents of the output data register is still the last to complete the data conversion. Notes that the pins in the wiring of the device, do not take the wrong or shorted, or is likely to put the IC to burn out.

Above, introduced the LM386 and the use of ADC0804 map, we only use two logical connection diagram can be completed into the process of signal preprocessing.

2) Signal storage

In this process, random access memory used in 6264, it is a capacity of 8 Kbyte of SRAM, the chip uses a 20-pin plastic dual in-line package, single +5V power supply. 6264 with 13-bit address lines, so with a counter 4040 and a 4520 for 6264 jointly

Be completely addressed. 6264 and 4040,4520 in the system chip circuit 6264 as shown figure 3 for the address lines A0~A12, DQ0~DQ7 for data lines, W is allowed, G for the output enable, E1, E2 for the chip select[5].

In 6264 and 0804 connections, make 0804 online release of data to the data and 6264 data taken from the corresponding data line up in this system, we are the menu by 6264 changes in the last two lines to read and write on 6264 . 4040 is a 12-bit binary addend counter, coupled with the lowest 4520 to control 6264, a 13-bit address, its status changes from 0000000000000~1111111111111, addressing space
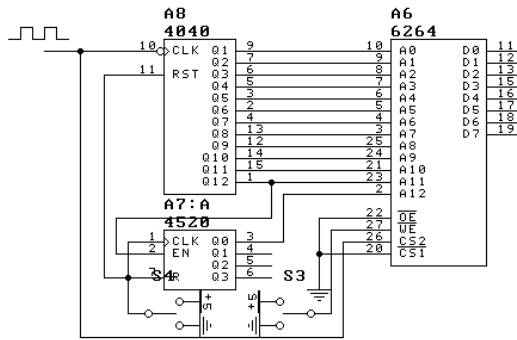
Fig. 3. 6264, 4040 and 4520 connection circuit

for the 8K. That means we only store the time is 2 seconds, mainly because the storage capacity is 6264 4k. Completion of the signals above the main part of the storage processes.

 3) Sound Playback

   Through the sound processing and sound storage process, the sound playback to enter into this process, it is mainly the reverse process of the sound process, we use a piece of this DAC DAC0832. DAC0832 as a high current output type D/A converter, the chip structure with two registers, that is, the input data in the internal latch to go through the levels, so that both sets of data stored. Double-buffered input data can be used, a single buffer or through work in three ways. In this system uses a straight-through D/A conversion, data should be made through WR1= WR2= CS=XFER= "0", ILE = "1", directly to the input digital D/A converter In the conversion. DAC0832 circuit connection as shows figure 4.
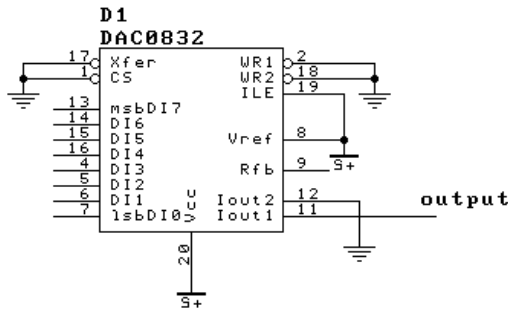
Fig. 4. DAC0832 circuit connection diagram

   DAC0832 is used as transmitted through, so it's switching frequency is determined by the frequency of 6264, is the 4KHz, word length is 8 bits. DAC0832 work process is the chip first from eight data lines connected with the 6264 to accept 8-bit digital signals, followed by digital signal is converted to put an analog signal transmitted by the No. 11 DCA0832 LM386 allowed to handle[5].

3   Circuit Design

3.1   Circuit Implementation

Based on the above features our analysis of each subsystem and the circuit, first let's experiment in digital electronics boxes one by one on small systems to connect and tests show correct connection and can get the desired results. Finally, each subsystem is to be combined into a complete circuit.

3.2   Circuit Board Design

Based on the above circuit diagram, software to design the drawing board, we generally used in circuit board design software PROTEL. PROTEL package from the schematic editor, output, printed circuit board design, output, schematic device library composed of editors and other utilities. PROTEL greatly reducing our use of design time, and effectively and accurately map the circuit board. With the development of electronic technology, PCB board smaller and smaller, more and more high density, and PCB board level continue to increase, therefore, required in the overall layout of the PCB, anti-interference ability, and manufacturability of the process to request Higher and higher. The main printed circuit board design steps:

    (1)Draw the schematic.
    (2)The creation of libraries.
    (3)Schematic and PCB to establish a network connection between the components.
    (4)The wiring and layout.
    (5)Create and mount PCB production and use of data production and use of data.

   Printed circuit board design process to consider the following questions: 1, to ensure that the circuit diagram is consistent with the physical components and the graphical schematic of the network connection is correct. 2, printed circuit board design is not just consider the network connection between the schematic and the circuit works to consider some of the requirements, the circuit requirements of the project is mainly the power line, ground wire and other wire width, cable connections, Some components of the high-frequency characteristics of impedance of the device, and interference. 3, printed circuit board machine system installation requirements, the main consideration mounting holes, plugs, positioning holes, and other reference points have to meet the requirements, the placement of various components and accurately installed in the specified location, while convenient Installation, commissioning, and ventilation. 4, printed circuit board on the manufacturability of the process and its requirements, be familiar with the design specifications and meet the requirements of production process, so that the printed circuit board designed to smooth production. 5, in considering the components in the production, ease of installation, commissioning, repair, and printed circuit board graphics, pads, via, etc. to standards, to ensure that no collision between the components, and easily installed. 6, printed circuit board design purpose is to apply, so we have to consider its usefulness and reliability, while reducing board layer printed circuit board area and thus to reduce costs, appropriate larger pad, Through-hole, walking lines, and is

conducive to improving the reliability and reduce the through-hole, optimization alignment, spacing them evenly, consistency, and the board some of the overall layout of the beautiful.

3.3   Circuit Board Production

The process of making printed circuit board is divided into three steps: first, exposure, exposure in the original style of photographic plate; second is developing, will have use of contrast media exposure for developing photographic plates; third etching, the use of Etching solution, the rest of the circuit board copper foil cleaned the rest of the design circuit[4,5].

   The first step, the first circuit schematic into a circuit board diagram, cut out a piece of the appropriate size of the Bonded Copper, the Bonded Copper side up, and then covered with a carbon paper in the above, and then draw circuit board covered in carbon on the maps, And then re-scan a pen on paper, so that the line displayed on the CCL.

   The second step, with the knife in accordance with the road map plan to open little by little, and to ensure true disconnect between the lines and lines.

   The third step, which is the prototype circuit board has been the basic form, punch in the corresponding place, and then use sandpaper to polish the copper foil, copper foil and then coated with a layer of rosin in alcohol, water, both to prevent oxidation, and help In the solder

4   Application

The system is mainly used in small recording device, and a number of multimedia technologies which, if well-transformation, will be a good application. For example: The one is that we can often see some selling in the streets, and they use the horn to put the record down to say, do not have to stop crying, and then released over and over again, so much more convenient. And this small storage system uses the sound of this principle. Through the improvement of integrated circuits can be stored longer, greatly facilitate the majority of users. The second application is then used by our home phone, the keys of the dial-up also used the sound of the sound storage technology, it can, according to a key voice on the issue of a digital signal either stored for some time, will also play back a The original sound. There are three applications that we applied to the mobile phone voice dialing function, but also used in storage technology, because their voices should be stored first, and this process must be done by storing the principle, and then use the voice Recognition technology to complete the identification. This is the sound of a simple example of storage applications. Sound application of storage technology is far from that, in all areas are covered later on in life we will use more audio storage technology.

5   Conclusion

Storage Technology through the principle of sound analysis, we designed a simple voice storage system, although we use a lot of integrated circuits, the whole system is a

bit large, but the sound principles of storage technology are the same. The system can complete a small period of time out of the sound storage and playback, to achieve the sound equipment in the civilian application of these technologies will be more convenient to our lives.

References

1. Du, Y.-Q.: Applications of LM386 in Low-power Active Sonar Transmitting Circuit and Receiving Circuit. Audio Engineering (July 2010)
2. Zhang, H.-M.: Amplifiers Self-excited Oscillation Analysis and Elimination of Causes. Journal of Henan Mechanical and Electrical Engineering College (February 2008)
3. Liang, P.-J., Zhao, J.: The Video Inspect System Bases on Embedded Linux System. Computer Knowledge and Technology 5(11) (April 2009)
4. Li, X., Ji, R., Zhang, L.: Video collection system based on embedded Linux and ARM9. Electronic Measurement Technology (February 2009)
5. Wang, D.M., Zhang, G.L., Zu, Z.H.: A Video and Audio Collection System Based on Embedded Environment. Radio Engineering 37(11) (2007)

A Research on QoS Model for IP Networks

Xiaojun Liu[1,2] and Chunxia Tu[1]

[1] School of Mathematics and Computer Science, Huanggang Normal University,
Hubei Huanggang 438000 China
[2] LIESMARS, Wuhan University, Hubei Wuhan 430079 China
`{whutliuxiaojun,tuchunxia}@126.com`

Abstract. This paper analyzes the problems of IP networks when transmitting real-time business, and describes the overall function of QoS (Quality of Service) technologies, these technologies aim to improve the quality of service IP networks.Then, we focuses on the famous service models which can meet the QoS requirements, proposed by Internet Engineering Task Force (IETF), including Integrated Services model (IntServ), Differentiated Service model (DiffServ), Multi-Protocol Label Switching (MPLS), Traffic Engineering (TE) and Constraint-based Routing, analyze their advantages and disadvantages, and then study the relationship between them. Finally, we conclude that, integrated use of various models based on MPLS is the most promising technology to provide QoS guarantee, in large IP networks.

Keywords: QoS, IP, MPLS, Intserv, Diffserv, TE.

1   Introduction

On traditional IP networks, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. A packet is assigned resources prior to all its subsequent packets. This service model is called best-effort. It delivers packets to their destinations as possibly as it can, providing no guarantee of delay, jitter, packet loss ratio, or reliability. The Internet has been growing along with the fast development of networking technologies. Real-time applications, Voice over IP (VoIP) for example, require low transmission delay. Contrarily, E-mail and FTP applications are not sensitive to transmission delay. To satisfy different requirements of different services, such as voice, video, and data services, the network must identify these services and then provide differentiated services. As a traditional IP network in the best-effort service model does not identify services in the network, it cannot provide differentiated services. The QoS technology was introduced to address this problem.

2   IP QoS Overview

For network operations, QoS (Quality of Service)including the transmission bandwidth, transmission delay, packet loss rate. In the network, it can ensure the transmission bandwidth, reduce transmission latency, lower packet loss rate and delay jitter, and other measures to improve service quality.IP QoS provides the following functions:
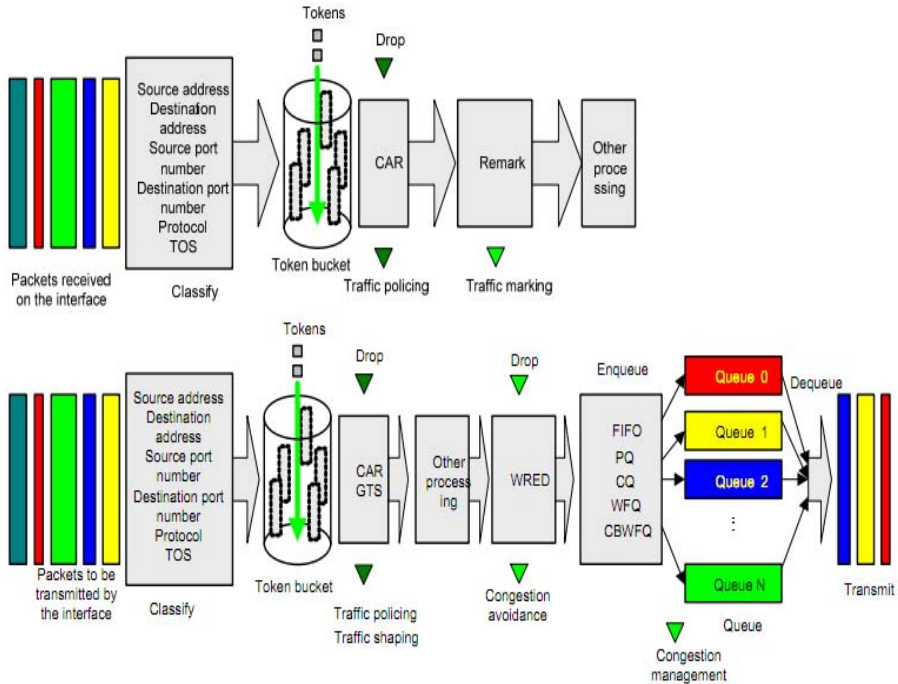
Fig. 1. Processing sequence of QoS technologies on a network device

Traffic classification and marking: uses certain match criteria to organize packets with different certain characteristics into different classes and is the foundation for providing differentiated services. Traffic classification and marking is usually applied in the inbound direction of a port.

Congestion management: provides measures for handling resource competition during network congestion and is usually applied in the outbound direction of a port. Generally, it buffers packets, and then uses a scheduling algorithm to arrange the forwarding sequence of the packets.

Congestion avoidance: monitors the usage status of network resources and is usually applied in the outbound direction of a port. As congestion becomes worse, it actively reduces the amount of traffic by dropping packets.

Traffic policing: polices particular flows entering a device according to configured specifications and is usually applied in the inbound direction of a port. When a flow exceeds the specification, restrictions or penalties are imposed on it to prevent its aggressive use of network resources and protect the business benefits of the carrier.

Traffic shaping: proactively adapts the output rate of traffic to the network resources of the downstream device to avoid unnecessary packet drop and congestion. Traffic shaping is usually applied in the outbound direction of a port.

Link efficiency mechanism: improves the QoS level of a network by improving link performance. For example, it can reduce transmission delay of a specific service on a link and adjusts available bandwidth.

Among those QoS technologies, traffic classification and marking is the foundation for providing differentiated services. Traffic policing, traffic shaping, congestion management, and congestion avoidance manage network traffic and resources in different ways to realize differentiated services. A device's support for QoS is implemented by the combination of various QoS technologies. Figure 1 describes the processing sequence of QoS technologies.

Network resources are always limited, as long as there appears to snatch the network resources, there will be QoS requirements. Quality of service is relatively in terms of network traffic, while ensuring quality of service class of business, while others may be at the expense of the quality of service. For example, a fixed total bandwidth in the network, if certain types of businesses more bandwidth, so other businesses can use less bandwidth and may affect other business use. Therefore, network resources, network managers need to make rational planning and allocation, according to various characteristics of the business, so that efficient utilization of network resources.This, QoS model concepts have come into being. The following present the most used and the most mature QoS model one by one, and compare their advantages and disadvantages.

3   QoS Models for IP Networks

IETF has proposed many service models and mechanisms to meet QoS requirements. The more famous are: Integrated Services model (IntServ), Differentiated Service model (DiffServ), Multi-Protocol Label Switching (MPLS), Traffic Engineering (TE) and Constraint-based Routing.IntServ is characterized by resource reservation, real-time applications must first establish access and reserve resources before the transmission of data,   RSVP(Resource Reservation Protocol) is used to create channels and set aside resources for the agreement. In DiffServ, the data packets to be marked, resulting in different levels, each of the packets have different service levels. MPLS is a forwarding strategy, when the data packets are sent into the MPLS scope, them will be give a certain label, then,   packet classification, forwarding and services will be completed based on the label. TE is a process which can arrange the traffic through the network Constraint-based Routing means that when looking for routes subject to certain constraints, such as: bandwidth or latency requirements

3.1   IntServ Service Model

IntServ is a multiple services model that can accommodate various QoS requirements. In this model, an application must request a specific kind of service from the network before it can send data. The request is made by RSVP signaling. RSVP signaling is out-of-band signaling. With RSVP, applications must signal their QoS requirements to network devices before they can send data packets.

An application first informs the network of its traffic parameters and QoS requirements for bandwidth, delay, and so on. When the network receives the QoS requirements from the application, it checks resource allocation status based on the QoS requirements and the available resources to determine whether to allocate resources to the application. If yes, the network maintains a state for each flow

(identified by the source and destination IP addresses, source and destination port numbers, and protocol), and performs traffic classification, traffic policing, queuing, and scheduling based on that state. When the application receives the resource allocation acknowledgement from the network, the application starts to send packets. As long as the traffic of the application remains within the traffic specifications, the network commits to meeting the QoS requirements of the application. IntServ provides two types of services:

Guaranteed service, which provides assured bandwidth and limited delay. For example, you can reserve 10 Mbps of bandwidth and require delay less than 1 second for a Voice over IP (VoIP) application.

Controlled load service, which guarantees some applications low delay and high priority when overload occurs to decrease the impact of overload on the applications to near zero.

However, IntServ to achieve end-to-end QoS, request sent to the receiving node among all the routers support RSVP signaling protocol, which is asking too much router implementation. For these shortcomings make it difficult to implement at the backbone of the Internet.

3.2   DiffServ Service Model

DiffServ is a multiple services model that can satisfy diverse QoS requirements. Unlike IntServ, DiffServ does not require an application to signal the network to reserve resources before sending data, and therefore does not maintain a state for each flow. Instead, it determines the service to be provided for a packet based on the DSCP value in the IP header.

In a DiffServ network, each forwarding device performs a forwarding per-hop behavior (PHB) for a packet based on the DSCP field in the packet. The forwarding PHBs include:

1. Expedited forwarding (EF) PHB. The EF PHB is applicable to low-delay, low-jitter, and low-loss-rate services, which require a relatively constant rate and fast forwarding;
2. Assured forwarding (AF) PHB. Traffic using the AF PHB can be assured of forwarding when it does not exceed the maximum allowed bandwidth. For traffic exceeding the maximum allowed bandwidth, the AF PHBs are divided into four AF classes, each configured with three drop precedence values and assigned a specific amount of bandwidth resources.
3. Best effort (BE) PHB. The BE PHB is applicable to services insensitive to delay, jitter, and packet loss.

DiffServ contains a limited number of service levels and maintains little state information. Therefore, DiffServ is easy to implement and extend. However, it is hard for DiffServ to provide per-flow end-to-end QoS guarantee. Currently, DiffServ is an industry-recognized QoS solution in the IP backbone network. Although the IETF has recommended DSCP values for each standard PHB, device vendors can customize the DSCP-PHB mappings. Therefore, DiffServ networks of different operators may have trouble in interoperability. The same DSCP-PHB mappings are required for interoperability between different DiffServ networks.

When selecting a QoS service model for your IP network, you need to consider its scale. Generally, you can use DiffServ in the IP backbone network, and DiffServ or IntServ at the IP edge network. When DiffServ is used at the IP edge network, there is no interoperability problem between the IP backbone network and the IP edge network. When IntServ is used at the IP edge network, you must address the interoperability issues between DiffServ and IntServ regarding RSVP processing in the DiffServ domain and mapping between IntServ services and DiffServ PHBs. There are multiple RSVP processing methods in a DiffServ domain. For example:

1. Make RSVP transparent to the DiffServ domain by terminating it at the edge forwarding device of the IntServ domain. The DiffServ domain statically provisions the IntServ domain with resources. This method is easy to implement but may waste resources of the DiffServ domain.
2. The DiffServ domain processes the RSVP protocol and dynamically provisions the IntServ domain with resources. This method is relatively complicated to implement but can optimize DiffServ domain resource utilization.

According to the characteristics of IntServ services and DiffServ PHBs, you can map IntServ services to DiffServ PHBs as follows:

1. Map the guaranteed service in the IntServ domain to the EF PHB in the DiffServ domain;
2. Map the controlled load service in the IntServ domain to the AF PHB in the DiffServ domain.

3.3 Multiprotocol Label Switching (MPLS)

Multiprotocol Label Switching (MPLS), originating in IPv4, was initially proposed to improve forwarding speed. Its core technology can be extended to multiple network protocols, such as IPv6, Internet Packet Exchange (IPX), and Connectionless Network Protocol (CLNP). That is what the term multiprotocol means.

MPLS is a three-tier exchange of technology, a combination of two rapid exchange and three-tier flexible routing, meanwhile, MPLS' Label Switching Path in (LSP) in the form of VC will provide a connection-oriented services. Although the traditional MPLS packets improve the forward speed, but do not provide QoS characteristic, and still using the Best-Effort service when it forwards packets. Therefore rely solely on the MPLS can not provide a satisfactory QoS guarantee, the deficiencies are mainly embodied in the following areas:

there is no distinction between the traditional MPLS deal packets of different application types of mechanism, and all packets are treated equally;

In the traditional MPLS, there is no admission control mechanism can not effectively avoid network overload;

MPLS routing of the three are used in traditional IP routing algorithm can not accurately reflect the network load conditions, easily lead to network load imbalance.

In fact, MPLS-based DiffServ is implemented by combining DS marking with MPLS label distribution. MPLS DiffServ is implemented by using the EXP field in the MPLS header to carry DiffServ PHBs. A label switching router (LSR) makes forwarding decisions based on the MPLS EXP. The problem is how to map

64 DiffServ PHBs to the 3-bit EXP field. MPLS DiffServ provides two solutions to address the problem. You can choose either solution depending on your network environments.

One is the EXP-inferred-LSPs (E-LSP) solution, which uses EXP bits to signal the PHB treatment for individual packets on an LSP. This solution is applicable to networks supporting no more than eight PHBs.

The other is the label-inferred LSPs (L-LSP) solution, which uses both labels and EXP bits to decide PHB treatment of packets on an LSP. This solution is applicable to networks supporting more than eight PHBs.

3.4   Traffic Engineering (TE)

Basically, the network load severe, QoS policies, such as IntServ and DiffServ; provide a steady decline in performance. When the traffic load is light when, IntServ and best business almost no difference. So why not do the first step to try to avoid congestion? This is the motivation for traffic engineering. Traffic Engineering (TE) is a resource control technology, which can be used to control network resources and improve network performance. At the implementation of the project process flow can be through the rational allocation of bandwidth resources, as well as the effective control of the routing process so that network resources be able to get the optimal use of, data packet transmission in the network can automatically bypass a network failure, network congestion and network bottlenecks. Using traffic engineering techniques, the network of the QoS indicators have been improved considerably. However, traffic engineering can only improve the quality of service, quality of service will not completely solve the problem.TE is how to arrange transport streams through the network, in order to avoid congestion. To TE automation, constrained path is an important tool. To avoid congestion and provide a good performance, in fact, TE is DiffServ to add.

3.5   Constrainted Based Routing(CBR)

Constrainted Based Routing is used to calculate a route by a variety of constraints

CBR is evolved from the QoS routing. For a given QoS request of a stream or a stream of aggregation, QoS routing can best meet the QoS requirements. CBR extends the QoS routing, considering other constraints such as control, CBR's objectives are:

1. Choose a route that meets the needs of a particular QoS
2. Increase network utilization.

CBR want to determine a route, involving a network topology, data flow's demand, the link resource availability and network administrators could control some of the provisions. Therefore, CBR may find a longer and lighter load path, this path than the shortest path heavy load. Network traffic will thus be more uniform number. To realize the CBR, the router need to calculate the new link state information, state information calculated based on these routes.RSVP and CBR are independent but complementary. CBR decided to RSVP path message, but does not reserve resources. RSVP to reserve resources, but depends on the CBR or dynamic routing decision pathway.CBR chooses the best route for data flow, so to maximize the guaranteed

QoS. CBR do not want to replace the DiffServ, but to help it better transmission. In theory, MPLS and CBR, the two are mutually exclusive independent, because MPLS is a forward strategy forward, and CBR is a routing policy. CBR determines the route between two nodes based on resources and topology information, and there is no MPLS related. MPLS label distribution protocol used to establish LSP, do not care about routing is the CBR, or dynamic routing determined.

4   Conclusion

This article describes the popular QoS models that enable IP network to provide service quality, particularly the advantages and disadvantages of these models and the relationship between them. From the paper's analysis, we draw a conclusion that any single model is difficult to solve the QoS problems .Therefore, a comprehensive solution is: the advantages of comprehensive utilization of existing models to build integrated models .For example, a QoS assurance program has been proposed by the literature 【8】, the scheme bases on the combination of integrated services, differentiated service, MPLS traffic engineering technology, and achieve end-to-end QoS assurance program. MPLS Traffic Engineering and DiffServ integration, it can retain the MPLS traffic engineering to facilitate traffic management, fast forward the advantages of the DiffServ domain can also be resources to provide polymerization transmission control, improve the network efficiency. In addition, the edge of the network domain IntServ can provide effective end-to-end network deployment mechanism. Therefore, in theory, literature 【8】 proposed an integrated model of QoS, this model combines a variety of technologies to each other, complement each other, can provide a better end to end QoS.

References

1. RFC 1633, Integrated Services in the Internet Architecture: an Overview
2. RFC 2205, Resource Reservation Protocol (RSVP)-Version1 Functional Specification
3. RFC 2211, Specification of the Controlled-Load Network Element Service
4. RFC 2212, Specification of Guaranteed Quality of Service
5. RFC 2215, General Characterization Parameters for Integrated Service Network Elements
6. RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
7. RFC 2475, An Architecture for Differentiated Services
8. Xiaojun, L., Chunxia, T., Zhe, W.: A research on integrated model to provide QoS guarantee. In: Proc. IEEE Symp. 2009 International Conference on Future Computer and Communication, FCC 2009, pp. 66–68 (2009)

An VoIP Application Design with Dynamic QoS Control

Xiaojun Liu[1,2] and Chunxia Tu[1]

[1] School of Mathematics and Computer Science, Huanggang Normal University,
Hubei Huanggang 438000 China
[2] LIESMARS, Wuhan University, Hubei Wuhan 430079 China
{whutliuxiaojun,tuchunxia}@126.com

Abstract. This paper analyzes several QoS control methods commonly used, gives a dynamic QoS scheme which used in VoIP system based on closed-loop control, and gives the specific design of the scheme. Finally, the performance of the scheme analysis and the results showed that: The detection module of the program can accurately identify the major VoIP voice stream, and can correctly monitor network traffic. Meanwhile, when the network congestion occurs, the program can dynamically adjust the QoS control mechanism, make VoIP of QoS has been significantly improved.

Keywords: QoS, VolP, Closed—loop control.

1 Introduction

The voice over IP (VoIP) network is an IP-based packet switched network. After digitization, compression, and packetization, traditional analog voice signals are encapsulated into frames for transmission over the IP network. Nowadays, with the increasing development of network technology, VoIP technology has become one of the most promising technologies, and the standardization has also been further improved. But, on traditional IP networks, devices treat all packets equally and handle them using the first in first out (FIFO) policy. All packets share the resources of the network and devices. A packet is assigned resources prior to all its subsequent packets. This service model is called best-effort. It delivers packets to their destinations as possibly as it can, providing no guarantee of delay, jitter, packet loss ratio, or reliability. Therefore, the problem of quality of service(QoS) has become the most important and most complicated one.

2 Quality of Service (QoS)

Quality of Service (QoS) measures the service performance of service providers in terms of client satisfaction. Instead of giving accurate marks, QoS emphasizes analyzing what good or imperfect services are, and they come in what kind of circumstances, so as to provide a cutting edge improvement. From the start of QoS service model, some of the current most used and the most mature QoS techniques were described one by one. In certain circumstances the rational use of these technologies can improve service quality.

2.1   Introduction to QoS Service Models

Best-Effort Service Model
Best effort is a flat service model and also the simplest service model. In the best effort service model, an application can send packets without limitation, and does not need to request permission or inform the network in advance. The network delivers the packets at its best effort but does not provide guarantee of delay or reliability. The best-effort service model is the default model in the Internet and is applicable to most network applications, such as FTP and E-mail. It is implemented through FIFO queuing.

IntServ Service Model
The basic idea of IntServ is to make RSVP as a major signaling protocol, based on each data stream to provide end-to-end guaranteed service or controlled load. IntServ model for each of the treatment required for QoS data flow through the signaling mechanism will be application-specific Service Level requirements are notified through each router, to manage information exchange, conducted at the router on and deal with resource reservation strategy setting, in order to achieve end-to-end QoS business. However, IntServ to achieve end-to-end QoS, request sent to the receiving node among all the routers support RSVP signaling protocol, which is asking too much router implementation. For these shortcomings make it difficult to implement at the backbone of the Internet.

DiffServ Service Model
DiffServ is a multiple services model that can satisfy diverse QoS requirements. Unlike IntServ, DiffServ does not require an application to signal the network to reserve resources before sending data, and therefore does not maintain a state for each flow. Instead, it determines the service to be provided for a packet based on the DSCP value in the IP header. DiffServ contains a limited number of service levels and maintains little state information. Therefore, DiffServ is easy to implement and extend. This control methods and techniques that are based on Diff-Serv service model.

2.2   Several QoS Control Methods Commonly Used

Priority Queuing (PQ)
Priority queuing is designed for mission-critical applications. Those applications have an important feature, i.e. when congestion occurs they require preferential service to reduce the response delay. PQ can flexibly design priority sequence according to different network protocols (e.g. IP and PX), interface receiving packets, packet length, source/destination IP address etc.Priority queuing lassifies the packets into four different types: top, middle, normal and bottom, in descending order. By default, the data flow enters the normal queue. During queues dispatching, PQ strictly comply with the priority sequence from high to low, and it will send packets in the high-priority queue first. When that queue is empty, PQ will begin to send packets in lower priority queue. By putting the key service packets in the high priority queues, you can ensure that they can always be served first. At the same time, the common service

packets can be put in the low priority queues and transmitted when there are no key service packets waiting for transmission. The disadvantage of PQ is that packets in the lower queues will be neglected if there are packets in the higher queues for a long time.

Weighted Fair Queuing (WFQ)

As shown in Figure 1, Weighted Fair Queuing (WFQ) classifies packets by flow. In an IP network, packets belong to the same flow if they have the same source IP address, destination IP address, source port, destination port, protocol number, and IP precedence (or DSCP value). In an MPLS network, packets with the same EXP value belong to the same flow. WFQ assigns each flow to a queue, and tries to assign different flows to different flows. The number of WFQ queues (represented by N) is configurable. When dequeuing packets, WFQ assigns the outgoing interface bandwidth to each flow by IP precedence, DSCP value, or EXP value. The higher the precedence of a flow is, the higher bandwidth the flow gets. Based on fair queuing, WFQ assigns weights to services of different priorities.
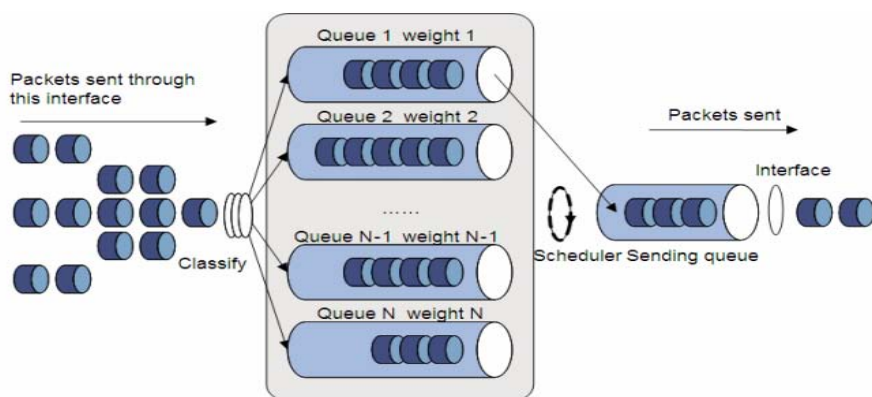
Fig. 1. WFQ

CBWFQ (Class-Based WFQ)

Class-based WFQ (CBWFQ) classifies packets according to match criteria such as IP precedence, DSCP values, and IP quintuples in an IP network or according to EXP values in an MPLS network, and then assigns different classes of packets to different queues. Packets that do not match any class are assigned to the system-defined default class. CBWFQ defines three types of queues: EF, AF, and BE. This section introduces the three queue types.

The low-delay EF queue is used to guarantee EF class services of absolute preferential transmission and low delay.

The bandwidth guaranteed AF queues are used to guarantee AF class services of assured bandwidth and controlled delay.

The default BE queue is used for BE class services and uses the remaining interface bandwidth for sending packets.

RTP (Real-time Transport Protocol) priority queuing

RTP priority queuing technology is used to solve the QoS problems of real-time service (including audio and video services). Its principle is to put RTP packets carrying audio or video into high-priority queue and send it first, thus minimizing delay and jitter and ensuring the quality of audio or video service which is sensitive to delay.
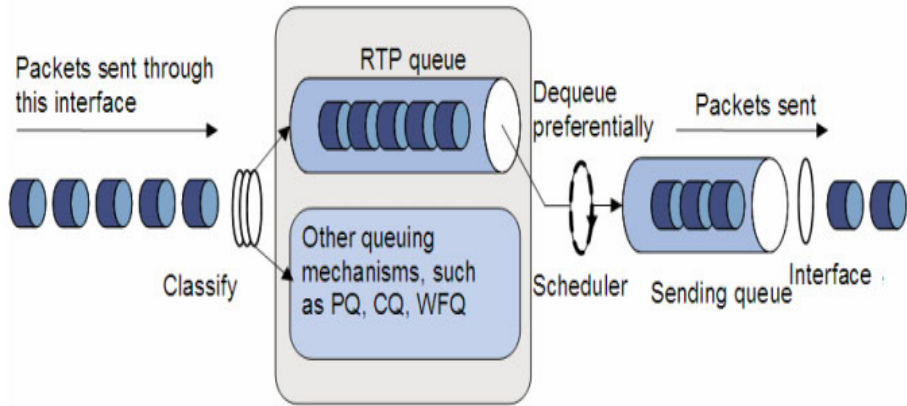
Fig. 2. RTP queuing

As shown in the above figure 2, an RTP packet is sent into a high priority queue. RTP packet is the UDP packet whose port number is even. The range of the port number is configurable. RTP priority queue can be used along with any queue (e.g., FIFO, PQ, CQ, WFQ and CBQ), while it has the highest priority. Since LLQ of CBQ can also be used to solve real-time service, it is recommended not to use RTP together with CBQ..

3   Author's Scheme

3.1   The Overall Concept of Dynamic QoS Scheme

The program is the first distinction between VoIP network flow, then uses a closed-loop control strategy to dynamically adjust the selection of the above QoS control methods to improve VoIP quality of service. The topology of the implementation of dynamic QoS adjustment is shown in Figure 3.

Feedback control PC in figure 4 captures the data flow router via port mirroring, then analyze the data stream, and identifies which is the voice stream, real-time records the source IP Address and port number of the voice streaming applications. At the same time, the control PC real-time monitorings the router's traffic information, calculates the router's packet loss rate, and then sets the appropriate QoS strategy. Then the control PC remote logins the router, and applies the selected QoS policy to the router. Thus, a closed loop controller based on the control PC appears, this controller can identify the data packet, the network status and dynamic adjust the QoS policy of network equipment. Closed-loop control schematic is shown in Figure 4 .
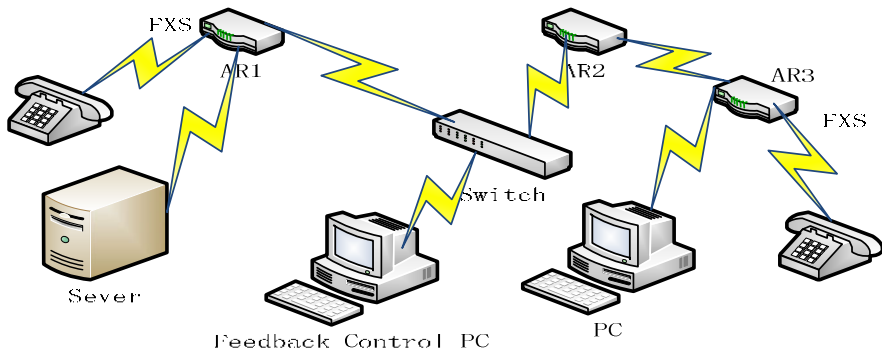
Fig. 3. The topology of the implementation of dynamic QoS adjustment
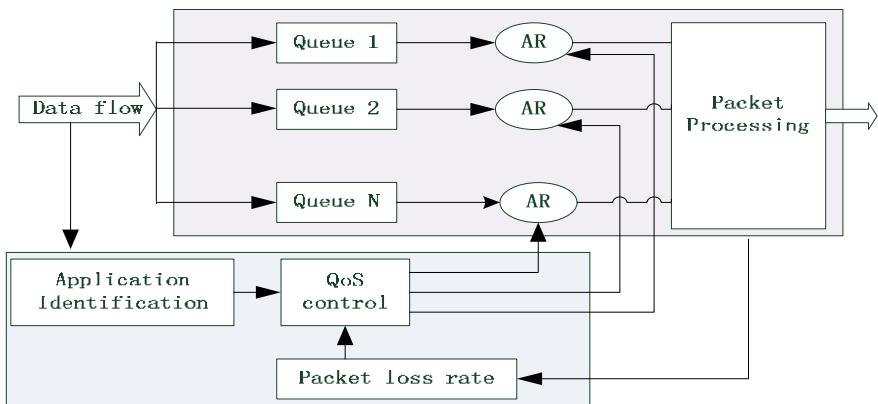
Fig. 4. Closed-loop control schematic

3.2   The Design of QoS Control Strategy

This scheme of QoS control strategy is based on network congestion, network congestion state is divided into three cases to consider, minor congestion, congestion and severe congestion. The designs are as follows:

Under severe congestion(packet loss rate $\geq 10\%$) using RTP priority queue. RTP priority queue configuration is easy, therefore, in severe congestion conditions, QoS policies can be quickly applied to the router, so that voice quality can be protected in time. When the network congestion is a serious situation, traffic monitoring frequency not too high, because the network has seriously overloaded, and generally set to 8s.

Congestion ($9\% \geq$ packet loss rate of $\geq 3\%$) with PQ. When the network is congested, the voice business has been an absolute priority, not only can guarantee the quality of voice communication, the delay impact on other businesses is also tolerable. Traffic monitoring time should be moderate, so that the burden should not increase the network congestion caused by more severe, usually set to 4s.

Mild congestion (2% ≥ packet loss rate of ≥ 1%) with CBWFQ. When the network is slightly congested, CBWFQ sends the voice stream into the EF queue, and limit certain bandwidth, the bandwidth of other network applications are not ignored, this can provide an absolute priority for the EF queue scheduling, real-time data to ensure that the delay; the same time through On high-priority data traffic restrictions, the delay of other queues have also been a degree of protection. At this point the network than the smooth, frequent monitoring time can be a little point, to grasp the network conditions change, usually set to 2s.
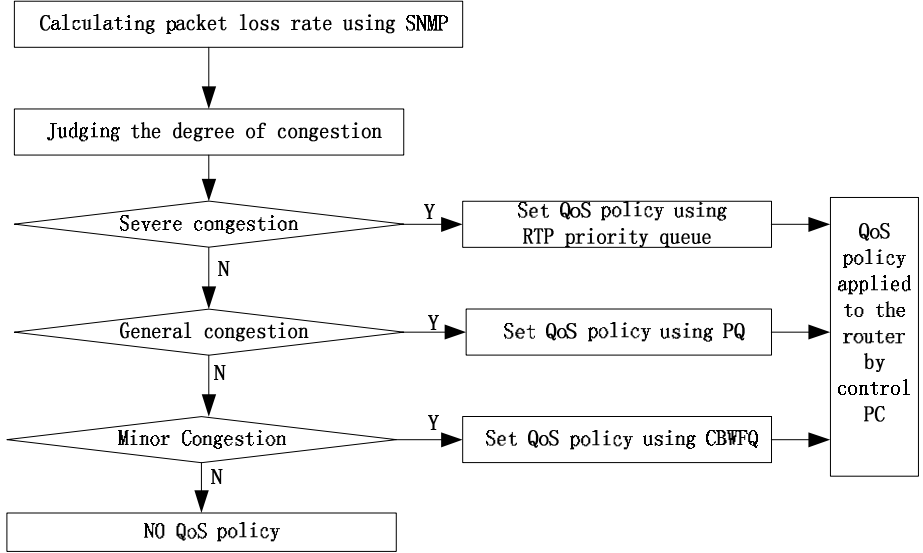
Fig. 5. The Flow chart of the control execution module

Dynamic QoS controller implementation

QoS controller of the program's main work is: VoIP voice packets feature recognition, router traffic monitoring, QoS policy setting and implementation.

VoIP transmission of voice packets are based on the RTP protocol is basically the network transmission. VoIP packet is encapsulated through the RTP, and then transmission by the UDP packet, so to analyze the voice data packets, as long as the capture UDP packets, and then you can analyze and judge. In this regard, the literature 【10】 analyses the features of four main voice stream (regular IP phone, Skype, QQ, MSN), and provide implementation scheme, which can distinguish between various audio streams, based on an analysis of the feature to. This article VoIP voice packets feature recognition in the literature on the use of the above programs.

Flow monitoring to get the final result is packet loss rate of the router interface. This article is the use of a router interface traffic statistics to achieve, these statistics using SNMP to get acquired. Calculated on the use of SGMP packet loss rate, see the relevant literature 【10】 .

On the QoS policy settings and implementing agencies, this article is so designed, control PC keeps watch on the router traffic conditions at any time, Once network congestion occurs, the control module configures QoS policies, according to the IP address and port No. is shown in Figure 5.

4   Simulation and Performance Analysis

The focus of performance analysis is to consider a variety of network conditions, QoS policy enforcement is to improve voice quality, or not. In this paper, the tester's subjective feelings and WinEyeQ voice quality software testing tools for both the combined to test the implementation of QoS policies. According to the tester's subjective evaluation, application RTP priority queue QoS policy, the call quality has been significantly improved than no application QoS strategy, the call made by the previous off smoothly. The voice quality testing by WinEyeQ tools have changed significantly too. At the same time by adjusting the sending rate of UDP packets, packet loss rate of voice data packets is shown in Table 1.

From the above table shows that PQ was the best, RTPQ second, followed by CBQ. WFQ is very poor in the VoIP application. This is because the PQ and RTPQ works send voice data packets into the priority queue, priority delivery. WFQ is very poor for voice quality, it is because WFQ more equitable for all applications to provide quality of service, due to the relative fair, it will not guarantee the high QoS requirements of applications. And WFQ does not have an individual data flow control mechanism, for each data stream can not provide bandwidth guarantee, so the program does not consider WFQ.

Table 1. The language packet loss rate under different conditions

Discard Rate / UDP Send Rate	NO Queues	PQ	WFQ	CBWFQ	RTPQ
1548.30 kbps	86.12%	0.42%	61.01%	2.08%	1.52%
436.89 kbps	57.23%	0.00%	56.55%	1.46%	1.75%
187.19 kbps	12.85%	1.41%	61.23%	2.18%	0.64%

From the above test results, the paper QoS scheme can dynamically adjust QoS strategy according to network load, does play a role in improving the QOS VOIP system.

5   Conclusion

This paper focused on network layer QoS mechanisms for the VoIP system, and provides a network layer QoS control scheme, that is dynamic QoS scheme based on closed loop control. The simulation experiments show that the scheme can distinguish various audio streams, and adjust the router's QoS mechanism real time according to

the network conditions, to achieve better VolP service quality. Future research is to continue to advance the program, improve the efficiency of identifying voice data stream, and enhance the efficiency of QoS control, focusing on closed-loop QoS control function embedded into the router, and to strengthen the program in a real network environment test and evaluation.

References

[1] RFC 1633, Integrated Services in the Internet Architecture: an Overview
[2] RFC 2205, Resource Reservation Protocol (RSVP)-Version1 Functional Specification
[3] RFC 2210, The use of RSVP with IETF Integrated Services
[4] RFC 2212, Specification of Guaranteed Quality of Service
[5] RFC 2215, General Characterization Parameters for Integrated Service Network Elements
[6] RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
[7] RFC 2475, An Architecture for Differentiated Services
[8] Lin, N., Qi, H.-m.: QoS Model of Next Generation Network Based on MPLS. Computer Engineering(CHINA) 34, 107–109 (2008)
[9] Xiaojun, L., Chunxia, T., Wu, Z.: A research on integrated model to provide QoS guarantee. In: Proc. IEEE Symp., 2009 International Conference on Future Computer and Communication, FCC 2009, pp. 66–68 (2009)
[10] Tian li, Research of VoIP Application Based on Dynamic QoS Control, Master thesis, Hunan NormalUniversity

Author Index