

## Service Dynamic Trust Evaluation Model based on Bayesian Network in Distributed Computing Environment

Libin Wang<sup>1</sup>, Xiangjun Li<sup>2\*</sup>, Xinquan Yan<sup>3</sup>, Song Qing<sup>2</sup> and Yuanlu Chen<sup>2</sup>

<sup>1</sup>Fuzhou Medical College of Nanchang University, Jiangxi Fuzhou 344000, P R China

<sup>2</sup>Department of Computer Science and Technology, Nanchang University, Nanchang 330031, P.R China

<sup>3</sup>Linchuan No.1 Middle School of Jiangxi Province, Jiangxi Fuzhou 344000, P R China

Corresponding author (Xiangjun Li), E-mail: lxjun\_alex@163.com

### Abstract

*In recent years, with the rapid development of computer network, distributed computing system has a very vast application prospect and potential utility value, which opens up a wealth of opportunities for different applications. With the characteristics of dynamic, heterogeneity, distribution, openness, voluntariness, uncertainty and deception, how to obtain trustworthy computing resource becomes a key issue in large-scale distributed computing research. Therefore, with considering the complex characters of trust in distributed computing environment, firstly, we construct STE architecture to rank and observe trust, which includes STE Broker, Monitoring and STE Catalogue. Secondly, a more comprehensive dynamic trust evaluation model is constructed based on Bayesian network. Finally, we apply simulation platform to imitate trust evolution process and collect related data, and the proposed method has been serviced in complex simulation system, and the results have indicated that the model is unbiased and effective. The first part is the research status and related problems. The second part is the establishment of an evaluation model. The last part is the experimental analysis and conclusion.*

**Key words:** Distributed computing, Bayesian network, Trust evaluation, Cloud service

### 1. Introduction

In recent years, distributed computing technology has been one of the cutting edge technologies for its low power and cost [1-2]. Last several years, with the rapid development of computer network, distributed computing system has a very vast application prospect and potential utility value, which integrates a large number of relative technology together [3-4], which opens up a wealth of opportunities for different applications, such as information processing, energy management, data delivery and so on [5-7]. More attention has been paid to the further development and more applications emerging, distributed computing is no longer confined to the traditional area, for example cloud computing and big data, moreover improves the efficiency of computing tasks while reducing energy consumption, and additionally augment the safety and security systems [8]. Large scale distributed computing infrastructure are unified computing platform which tries to connect and share all resources in the Internet, including computation resource, storage resource, information resource, knowledge resource and equipment for scientific research, and then solves the problems of large-scale engineering computing and commercial computing as well. However, with the characteristics of dynamic, heterogeneity, distribution, openness, voluntariness, uncertainty and deception, how to obtain trustworthy computing resource becomes a key issue in large-scale

distributed computing research [9-10]. The high availability and flexibility of service enable its potential in distributed online collaboration to handle dynamic service requests. Loosely coupled applications often have dependencies among tasks and use less for inter process communication. Efficient support for these sorts of applications on large scale systems will involve substantial technical challenges and will have big impact on science. Then, the trustworthiness of service nodes should also be evaluated in distributed computing environment.

At present, in all kinds of open dynamic distributed computing systems including the current pervasive computing, P2P computing, grid computing, cloud computing and so on, service nodes have more freedom, the links between the nodes are more frequent and close [11]. Because all the interactive objects (including data interaction and service interaction) are distributed in the new network environment, risks to the interaction between nodes are high. In order to reduce the irresponsible behavior in the network, the trust mechanism, usually using the node previous interaction experience to establish trust relationship should be constructed from the third party. A trustworthy entity will typically have a high reliability, and a trustworthy person will tell the truth and be honest with respect to interactions. Actually, trust is a complex subject that relates to different aspects of elements, such as belief in honesty, truthfulness, competence, and reliability of the trusted person or services. Trust plays an important role in computing service. A conceptual trust model of computing nodes was proposed by Marmol F, *et al.*, [12-13]. It utilizes the average rating given by end-users to automatically determine the selection of services. A novel metric named Verity was introduced by Omar M *et al.*, to quantify the consistency in compliance levels of a service contract [14]. Several Bayesian approaches to compute trust value based on the beta probability density functions were proposed in [15-16]. Messina F, *et al.*, presented a model to address service selection problem, but trust happens to be one of those considered quality criteria and this model cannot detect malicious consumers [17]. Zhao H and Li X investigated the trust-aware component service selection and established mathematical models, but they did not give a method to calculate trust [18]. Da Costa, *et al.*, proposed the measurement and evaluation models of trust-QoS in manufacturing grid and gave a trust-QoS-based manufacturing grid resource service scheduling framework [19]. Eymann, *et al.*, studied how to determine the trustworthiness of the composite service and used probability theory to determine the trustworthiness of the service nodes [20]. Shen Z and Li L present an abstract trust model  $TM = (G, D, O, C, P)$  from the qualitative perspective as a formal definition [21]. In order to solve this problem, more and more researchers devoted themselves into the research problems of computer node reliability assessment, which makes the trust evaluation has become one of the research hotspots.

Lots of research works have been conducted on various aspects of trust management including trust concept model, reliability assessment, trust mechanism and trust evaluation, *etc.* [22-23]. Service dynamic trust evaluation in distributed computing environment is still remained as an open field of research from diverse perspectives. At present, there is no longer a unified standard and rank framework, according to the evaluation indexes of trust. To evaluate the trust of service nodes scientifically, we need a new framework and evaluation method to determine the weight of different index, and fully reflect the objectivity and accuracy. In summary, current research of trust evaluation is still in its infancy, there is considerable problem space to explore and solve. On the one hand, the influence factors usually are very limited [24-25], which neglects the other factors which have huge effect on trust. On the other hand, we need a whole evaluation framework of trust evaluation, which can help users choose and monitor the operation state. Therefore, with considering the complex characters of trust in distributed computing environment, firstly, we construct STE architecture to rank and observe trust, which includes STE Broker, Monitoring and STE Catalogue. Secondly, a more comprehensive dynamic trust evaluation model is constructed based on Bayesian network. Finally, we

apply simulation platform to imitate trust evolution process and collect related data, and the proposed method has been serviced in complex simulation system, and the results have indicated that the model is unbiased and effective.

## **2. Service Trust Evaluation System Architecture**

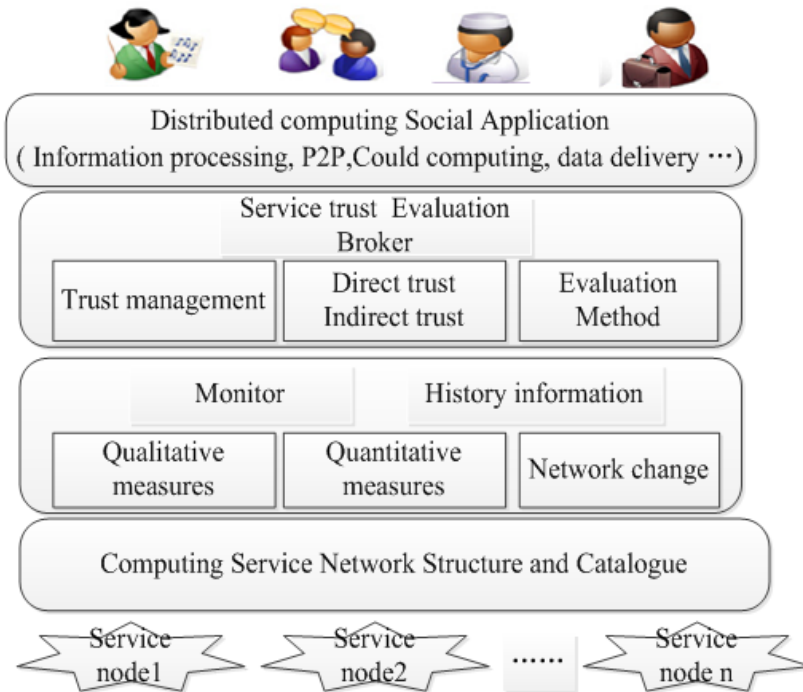
The components of the proposed SOA framework are organized in a small-world way. In order to generate successful collaborated applications, a trust mechanism is incorporated. In this Section, a system framework of SOA for trust management is presented, where the trust evaluation model of service nodes is built. A node's trust value is assessed based on direct observations and indirect information like recommendations. The trust of one node toward another node is updated upon encounter and interaction events. Each node will execute the trust protocol independently and will perform its direct trust assessment toward an encountered node based on specific detection mechanisms designed for assessing a trust property. Later we will discuss these specific detection mechanisms in our protocol.

The STE framework provides features such as service selection based on trust requirements and ranking of distributed computing based on previous user experiences and real time performance. Figure 1 shows the key elements of the framework:

(1)STE Broker: This component is responsible for interaction with customers and understanding their application needs, and performs discovery and ranking of suitable trusted services using other components such as the Trust management, direct/indirect trust and Evaluation Method. Evaluation method evaluates service trust selected by the STE Broker. The Trust management computes the various trusts which are used by the ranking system for prioritizing service nodes.

(2) Monitoring and history information: this component first discovers services that can satisfy users' needs. Then, it closely monitors the trust performance of the services, such as direct and indirect trust. At the same time, related history records are stored in service database.

(3) Computing service network structure and catalogue: builds the service network and their features advertised by various different providers, divides computing resources into different classes.



**Figure 1. Service Trust Evaluation System Architecture**

Two important issues in building the framework, as previously mentioned, are the measurement of various STE and the trust evaluation of service nodes. In the next Section, we put forward a trust evaluation model based on Bayesian network.

### 3. Dynamic Trust Evaluation Model based on Bayesian Network

A computing node displays a message, reflecting the characteristics of its behavior when it cooperates with other nodes; a node has sufficient choices; and the node is duty bound to offer recommendations to other nodes. Thus, the node can evaluate the copartner through its behavior. Nodes can also exchange and transmit evaluation messages in order to obtain the trust of target node and guide its cooperation decision. In this paper, we define the ‘trust’ in distributed computing environment as the evaluation of the target node’s ability of providing service (resource) through the reliability shown by its behavior in certain context, including the observation of its former behaviors and the recommendations from other nodes.

For the sake of simplicity, we only considered a distributed computing system within the same context during a period of time. For two nodes  $x$  and  $y$ , the successful cooperation probability between them is denoted by  $\theta$ . If there are direct interactions between  $x$  and  $y$ , we can obtain direct probability of successful cooperation, which is called direct trust degree, denoted by  $\theta_{dt}$ . If there is an intermediate node  $z$  between  $x$  and  $y$ , and there are interactions between  $x$  and  $z$ , and  $z$  and  $y$ , then we can also obtain an indirect probability of successful cooperation between  $x$  and  $y$ , which is called recommendation trust degree, denoted by  $\theta_{rt}$ . Thus, there are two kinds of probabilities of successful cooperation, which can be aggregated into global trust degree as follows:

$$f(\lambda_0 \cdot \theta_{dt} + (1 - \lambda_0) \cdot \theta_{rt}), \quad \lambda_0 \in (0,1) \quad (1)$$

where  $f(\cdot)$  is trust degree combination function, satisfying the property of convex function, that is, let  $S \subset R^n$  be a nonempty convex set, for every  $\theta_{dt}, \theta_{rt} \in S$ ,  $\lambda \in (0,1)$ , we have  $f(\lambda \cdot \theta_{dt} + (1-\lambda) \cdot \theta_{rt}) \leq \lambda f(\theta_{dt}) + (1-\lambda)f(\theta_{rt})$ ,  $f(\cdot)$  is decided by the subject factors of  $x$ , such as personality and emotion. For example, a common trust degree combination function is  $\hat{\theta} = \lambda \theta_{dt} + (1-\lambda) \cdot \theta_{rt}$ ,  $\lambda \in (0,1)$  and a node will choose  $\lambda > 0.5$  if it trusts more his direct experiences rather than others' recommendations. In light of this, we analyze how to obtain these two kinds of trust degree by Bayesian method.

### 3.1. Direct Trust

For the interaction probability here, we use Bayesian approach to compute its estimator. Let  $x$  and  $y$  be two nodes in the distributed computing system, and their interaction results are described by binomial events (successful/failure). When there are  $n$  times interactions between them,  $u$  times successful cooperation,  $v$  times failure cooperation, and define  $\hat{\theta}_{dt}$  as the probability of successful cooperation at  $n+1$  times. Then, the posterior distribution of successful cooperation between  $x$  and  $y$  is a Beta distribution with the density function:

$$Beta(\theta|u,v) = \frac{\Gamma(u+v+2)}{\Gamma(u+1)\Gamma(v+1)} \quad (2)$$

$$\hat{\theta}_{dt} = E(Beta(\theta|u+1,v+1)) = \frac{u+1}{u+v+2} \quad (3)$$

where  $0 < \theta < 1$ , and  $u, v > 0$ .

Under same situations, due to the lack of observations, it is not suitable to use  $\hat{\theta}_{dt}$  as the trustworthy of nodes. We need to estimate the confidence value of  $\hat{\theta}_{dt}$ . In fact, the measure of reliability about these intermediates is required. We evaluate the confidence level of trust degree by interval estimation in this paper. Let  $(\hat{\theta}_{dt} - \varepsilon, \hat{\theta}_{dt} + \varepsilon)$  be the confidence interval with degree  $\gamma$  of  $\hat{\theta}_{dt}$ ;  $\varepsilon$  is the error level. Confidence degree of  $\hat{\theta}_{dt}$  can be modeled as:

$$\gamma = P\left(\hat{\theta}_{dt} - \varepsilon < \theta_{dt} < \hat{\theta}_{dt} + \varepsilon\right) = \frac{\int_{\hat{\theta}_{dt}-\varepsilon}^{\hat{\theta}_{dt}+\varepsilon} \theta^{u-1} (1-\theta)^{v-1} d\theta}{\int_0^1 \theta^{u-1} (1-\theta)^{v-1} d\theta} = \frac{\Gamma(u)\Gamma(v)}{\Gamma(u+v)} \int_{\hat{\theta}_{dt}-\varepsilon}^{\hat{\theta}_{dt}+\varepsilon} \theta^{u-1} (1-\theta)^{v-1} d\theta \quad (4)$$

We can select a threshold of confidence level  $\gamma_0$ , and then improve the accuracy by increasing the number of interactions. When the accuracy is at an acceptable level, that is  $\gamma \geq \gamma_0$ , the trust degree can be evaluated with the evidences at this time. The relationship between number of samples  $n_0$ ,  $\gamma_0$  and  $\varepsilon$  can be modeled as follows:

$$n_0 \geq -\frac{1}{2\varepsilon^2} \ln\left(\frac{1-\gamma_0}{2}\right) \quad (5)$$

### 3.2. Indirect Trust

With respect to recommendation trust, we also use the approach above to evaluate it, as the recommendation is formed by several direct interactions. The selection of recommend nodes can also be decided by the trust degree of them.

Let the interactions between  $x$  and  $y$ ,  $z$  and  $y$  be independent, and the number of interactions between them be  $n_1$  and  $n_2$  separately, in which the successful cooperation is  $u_1$  and  $u_2$ , and failure cooperation is  $v_1$  and  $v_2$ . Then, the trust degree of  $x$  to  $y$  by  $z$  can be modeled as follows:

$$\hat{\theta}_{rt} = E\left(\text{Beta}\left(\theta|u_1 + u_2 + 1, v_1 + v_2 + 1\right)\right) = \frac{u_1 + u_2 + 1}{n_1 + n_2 + 2} \quad (6)$$

When there are several recommendation nodes, it is easy to extend formula (6), and combined with the accuracy analysis above, we can obtain the following:

$$\hat{\theta}_{rt} = \frac{\sum_{\gamma \geq \gamma_0} u + 1}{\sum_{\gamma \geq \gamma_0} (u + v) + 2} \quad (7)$$

Considering the confident level of trust degree, we can define the confidence of the recommendation  $y$  to  $x$  as the real number of interactions to the total required numbers between them.

$$w_{xy} = \begin{cases} \frac{n_{xy}}{n_0}, & \text{if } n_{xy} < n_0 \\ 1, & \text{otherwise} \end{cases} \quad (8)$$

Considering the global trust degree is affected by positive and negative feedbacks separately, the value of  $\hat{\theta}_{rt}$  can be mapped onto  $[-1, 1]$ . Therefore, formula (7) can be modified as follows:

$$\hat{\theta}_{rt} = \frac{\sum w \cdot (u - v)}{\sum w \cdot (u + v) + 2} \quad (9)$$

### 3.3. Effect of Time and Trust Relationship Analysis

As the trust degree is also affected by time, the impact of time varies according to the trust degree. The more recent the history information is, the more impact the factor has. The interaction of nodes is composed with a serial of time sequences. Given a certain sequence  $i$ , and the number of the successful and failure interactions are  $u_i$  and  $v_i$  separately, the following formula with the decay factor can be modeled:

$$u(n) = \sum_{i=1}^n u_i \cdot \eta^{(n-i)}, v(n) = \sum_{i=1}^n v_i \cdot \eta^{(n-i)} \quad 0 \leq \eta \leq 1 \quad (10)$$

Where  $u(n)$  and  $v(n)$  is the number of successful and failure interaction after  $n$ th sequence. When  $\eta = 1$ , nothing is affected by history interactions, the whole record is aggregated; when  $\eta = 0$ , the latest history record is considered. We can solve it by proposing the following recursive algorithm:

$$u(i) = u(i-1) \cdot \eta + u_i, v(i) = v(i-1) \cdot \eta + v_i \quad (11)$$

The relationships between two nodes,  $x$  and  $y$ , can be classified into four categories according to whether there are direct interactions and/or recommendations between them. Suppose  $dt = 1(\text{or } 0)$  represent that there are (not) interactions between  $x$  and  $y$ , and  $rt = 1(\text{or } 0)$  represent there are (not) intermediate nodes between them. Then, the four kinds of relationships can be described as  $TR(dt, rt)$ . We analyze the evaluation of trust degree in those relationships one by one as shown in Table 1.

**Table 1. The Evaluation of Trust Degree in Four Kinds of Relationships between Two Nodes**

$TR(dt, rt)$	$\gamma$	$\hat{\theta}_{dt}$	$\hat{\theta}_{rt}$	$\hat{\theta}$
(0,0)	-	1/2	0	1/2
(1,0)	$\gamma \geq \gamma_0$	$\frac{u+1}{u+v+2}$	0	$\hat{\theta}_{dt}$
	$\gamma < \gamma_0$	1/2	0	1/2
(0,1)	-	1/2	$\frac{\sum w \cdot (u-v)}{\sum w \cdot (u+v)+2}$	$f(\lambda_0 \cdot \theta_{dt} + (1-\lambda_0) \cdot \theta_{rt}), \lambda_0 \in (0,1)$
(1,1)	$\gamma \geq \gamma_0$	$\frac{u+1}{u+v+2}$	$\frac{\sum w \cdot (u-v)}{\sum w \cdot (u+v)+2}$	$f(\lambda_0 \cdot \theta_{dt} + (1-\lambda_0) \cdot \theta_{rt}), \lambda_0 \in (0,1)$
	$\gamma < \gamma_0$	1/2	$\frac{\sum w \cdot (u-v)}{\sum w \cdot (u+v)+2}$	$f(\lambda_0 \cdot \theta_{dt} + (1-\lambda_0) \cdot \theta_{rt}), \lambda_0 \in (0,1)$

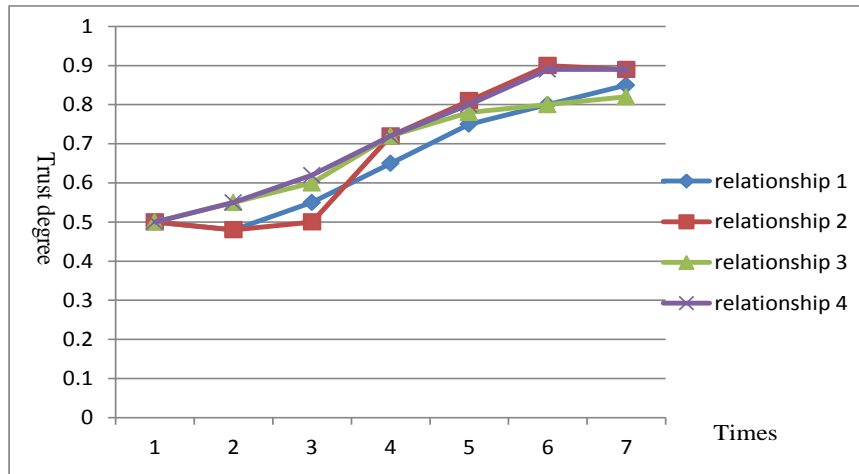
#### 4. A Numerical Example Analysis

In order to evaluate the proposed algorithm, we further developed a simulation platform based on CloudSim in PlanetLab with the benchmark model above. The simulation is performed in the laboratory including common software and hardware environment, namely CPU Intel core 4.0GHz, and memory for the DDRII4G, operating system is Windows7.0 professional edition.

Design and relevant experiments are carried out based on the experimental environment and parameter, we obtain all experimental data computing through the weighted average of 50 times, the trust model is carried out to evaluate the effectiveness.

##### 4.1. Trust Effect of Time and Relationship Analysis

For effective verification of the Bayesian cognitive model, we design 4 kinds of trust relationship of computing resources, and give the calculation method. The value of direct trust and recommendation trust degree of service nodes are all set to 0.75, the optimal sample size is 200. Repetitive execute resources and cloud resource scheduling at 6 moments, unit time for the day. Trust level and the evolution process at each time (days) is recorded, and we compare the weight of trust, confidence and effectiveness analysis. Trust evaluation results as shown in Figure 2.

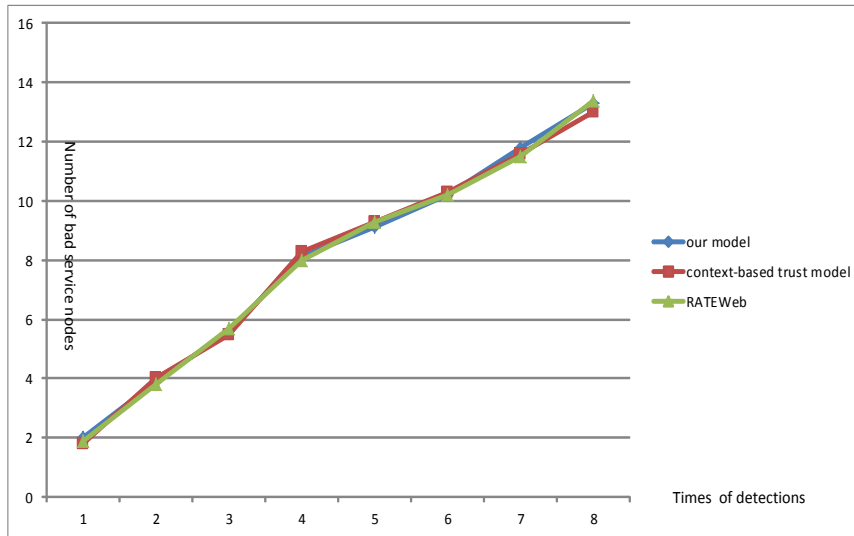


**Figure 2. Service Trust Effect of Time and Relationship Analysis**

At the initial moment, the trust degree of node  $x$  in  $y$  is 0.5. When we only consider the direct trust,  $\lambda_1=1$ ,  $\lambda_2=0$ , and until the third moment, the interaction of  $x$  to  $y$  is still not to the optimal number 200, trust value is not to 0.5. At the 5th, 6th moment, the trust confidence tends to be stable, and the executive level is [0.90, 0.95]. When we only consider the recommendation trust,  $\lambda_2=1$ ,  $\lambda_1=0$ . Until the second moment, the interaction times of  $z$  to  $y$  reaches the optimal value, which has recommendation trust ability. At the 5th, 6th moment, the trust confidence tends to be smooth, recommendation trust degree is 0.90, confidence interval is [0.8255, 0.9325]. The analysis of other trust relationships is to mix aggregation mentioned above, and the method of calculation is similar. According to the Figure 2, the direct trust and indirect trust of service nodes has the time decay utility, also verify the effectiveness of this trust assumption.

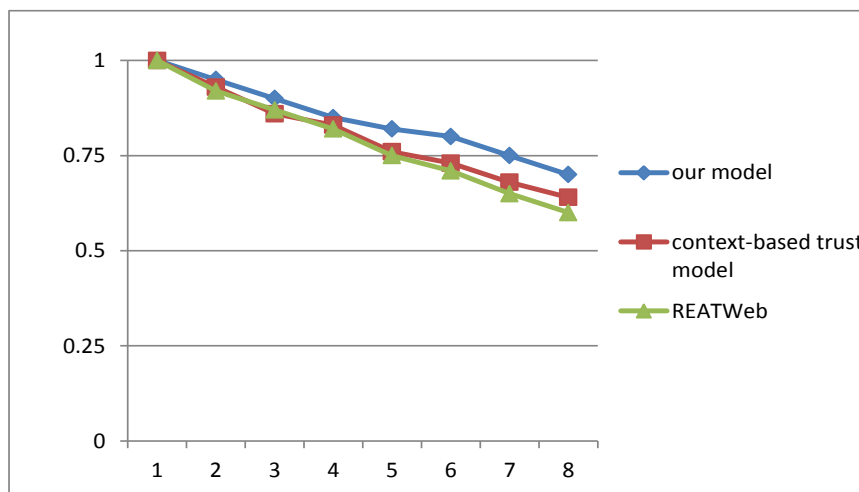
#### 4.2. The Comparison of Three Trust Evaluation Models

The purpose of this experiment is to investigate the stability and robustness to protect against malicious users attacking among the context-based trust computing model, the RATE Web model, and the model presented in this paper. The trust model is based on context to calculate trust values, including the ability-based computation and propagation-based computation of Web Service entities. The second model is an assessment framework focusing on providing a comprehensive solution for assessing the reputation of SPs. Three trust computation models are implemented to detect and prevent malicious service providers by evaluating their trust scores. The detect times for different numbers of malicious service providers are shown in Figure 3.



**Figure 3. The Detect Time over Different Numbers of Malicious Service Nodes**

Malicious service providers do not pay any attention to their service behaviors, and in turn provide false and misleading services. Thus, their notoriety would spread rapidly in the small-world relationship network. We could figure out the detection performances of three model systems from Figure 3. Generally speaking, these three models perform similarly. However, our model outperforms the other two models in terms of detection time.



**Figure 4. The Normal Performance over Different Times of Attacks**

We further examine the stability and robustness of the pro-posed model system when it faces malicious service attacks. The ratios of simulation performance for three compared models under different times of attacks to normal performance are shown in Figure 4. The context-based trust model performs the worst among the three models; while the model proposed in this paper improve the performance in stability and robustness: the ratios of its performance to normal performance reach almost over 0.8.

## 5. Conclusion

In recently years, distributed computing technology has been one of the cutting edge technologies, which has a very vast application prospect and potential utility value. Large scale distributed computing infrastructure are unified computing platform which tries to connect and share all resources in the Internet, including computation resource, storage resource, information resource, knowledge resource and equipment for scientific research, and then solves the problems of large-scale engineering computing and commercial computing as well. However, with the characteristics of dynamic, heterogeneity, distribution, openness, voluntariness, uncertainty and deception, how to obtain trustworthy computing resource becomes a key issue in large-scale distributed computing research. Therefore, with considering the complex characters of trust in distributed computing environment, we construct STE architecture to rank and observe trust, which includes STE Broker, Monitoring and STE Catalogue.

## ACKNOWLEDGEMENTS

The authors acknowledge the support for this work from the National Natural Science Foundation of China ((No.51367014, 61462040, 61262049), the Jiangxi Province Education Plan of Young Scientists Foundation of China (No.20112BCB23004), the Jiangxi Province Natural Science Foundation of China (No.20142BAB207011, 20142BAB217016), the Jiangxi Province Science and Technology Support Plan Key Projects of China (No. 20111BBE50008), and Science and Technology plan projects in Jiangxi province Education Bureau of China (No.GJJ14770).

## References

- [1] M. D. Dikaiakos, D. Katsaros, P. Mehra, *et al.*, "Cloud computing: distributed internet computing for IT and scientific research", *Internet Computing*, IEEE, vol. 13, no. 5, (2009), pp. 10-13.
- [2] J. Gray, "Distributed computing economics", *Queue*, vol. 6, no. 3, (2008), pp. 63-68.
- [3] Y. Afek, N. Alon, O. Barad, *et al.*, "A biological solution to a fundamental distributed computing problem", *science*, vol. 331, no. 6014, (2011), pp. 183-185.
- [4] A. D. Kshemkalyani and M. Singhal, "Distributed computing: principles, algorithms, and systema", Cambridge University Press, (2008).
- [5] Y. Zhang, Q. Gao, L. Gao, *et al.*, "Imapreduce: A distributed computing framework for iterative computation", *Journal of Grid Computing*, vol. 10, no. 1, (2012), pp. 47-68.
- [6] B. P. Rimal, E. Choi and I. Lumb, "A taxonomy and survey of cloud computing systems", *INC, IMS and IDC, 2009. NCM'09. Fifth International Joint Conference on IEEE*, (2009), pp. 44-51.
- [7] H. Casanova, A. Legrand and Q. M. Simgrid, "A generic framework for large-scale distributed experiments", *Computer Modeling and Simulation, UKSIM 2008, Tenth International Conference on IEEE*, (2008), pp. 126-131.
- [8] X. Li, F. Zhou and X. Yang, "A multi-dimensional trust evaluation model for large-scale P2P computing", *Journal of Parallel and Distributed Computing*, vol. 71, no. 6, (2011), pp. 837-847.
- [9] L. Y. Tian, J. Zhan, W. Jiang, *et al.*, "Research on quantified cloud computing trust model", *Computer Engineering and Design*, vol. 34, no. 1, (2013), pp. 13-17.
- [10] Y. L. Sun, Z. Han and K. J. R. Liu, "Defense of trust management vulnerabilities in distributed networks", *Communications Magazine, IEEE*, vol. 46, no. 2, (2008), pp. 112-119.
- [11] R. Scandariato, Y. Ofek, P. Falcarin, *et al.*, "Application-oriented trust in distributed computing", *Availability, Reliability and Security, ARES 08, Third International Conference on. IEEE*, (2008), pp. 434-439.
- [12] F. G. Marmol and G. M. Pérez, "Security threats scenarios in trust and reputation models for distributed systems", *computers & security*, vol. 28, no. 7, (2009), pp. 545-556.
- [13] M. F. Gómez and P. G. Martínez, "Towards pre-standardization of trust and reputation models for distributed and heterogeneous systems", *Computer Standards & Interfaces*, vol. 32, no. 4, (2010), pp. 185-196.
- [14] M. Omar, Y. Challal and A. Bouabdallah, "Reliable and fully distributed trust model for mobile ad hoc networks", *Computers & Security*, vol. 28, no. 3, (2009), pp. 199-214.
- [15] G. Schryen, M. Volkamer, S. Ries, *et al.*, "A formal approach towards measuring trust in distributed systems", *Proceedings of the 2011 ACM Symposium on Applied Computing. ACM*, (2011), pp. 1739-1745.

- [16] Y. Ding, F. Liu and B. Tang, "Context-sensitive trust computing in distributed environments", *Knowledge-Based Systems*, vol. 28, (2012), pp. 105-114.
- [17] F. Messina, G. Pappalardo, D. Rosaci, *et al.*, "A trust-based approach for a competitive cloud/grid computing scenario", *Intelligent Distributed Computing VI*. Springer Berlin Heidelberg, (2013), pp. 129-138.
- [18] H. Zhao and X. Li, "H-trust: A robust and lightweight group reputation system for peer-to-peer desktop grid", *Distributed Computing Systems Workshops, ICDCS'08, 28th International Conference on IEEE*, (2008), pp. 235-240.
- [19] G. Da Costa, J. P. Gelas, Y. Georgiou, *et al.*, "The green-net framework: Energy efficiency in large scale distributed systems", *Parallel & Distributed Processing, 2009. IPDPS 2009. IEEE International Symposium on. IEEE*, (2009), pp. 1-8.
- [20] T. Eymann, S. König and R. Matros, "A framework for trust and reputation in grid environments", *Journal of Grid Computing*, vol. 6, no. 3, (2008), pp. 225-237.
- [21] Z. Shen, L. Li, F. Yan, *et al.*, "Cloud computing system based on trusted computing platform", *Intelligent Computation Technology and Automation (ICICTA), International Conference on IEEE*, vol. 1, (2010), pp. 942-945.
- [22] F. Feng, C. Lin, D. Peng, *et al.*, "A trust and context based access control model for distributed systems", *High Performance Computing and Communications, HPCC'08, 10th IEEE International Conference on IEEE*, (2008), pp. 629-634.
- [23] D. Peng, W. Chen and Q. Peng, "TrustVis: visualizing trust toward attack identification in distributed computing environments", *Security and Communication Networks*, vol. 6, no. 12, (2013), pp. 1445-1459.
- [24] A. Mohaisen, H. Tran, A. Chandra, *et al.*, "Trustworthy distributed computing on social networks", *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ACM*, (2013), pp. 155-160.
- [25] Z. Cao, K. Li, X. Li, *et al.*, "Guest Editors' Introduction: Special Issue on Trust, Security, and Privacy in Parallel and Distributed Systems", *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, (2014), pp. 0279-282.

## Authors

**Libin Wang**, Female, was born on March 14th, 1975, from Fuzhou City, Jiangxi province, China. She received her Bachelor's Degree in Computer Applications (2002) and Master's degree in Computer Application Technology (2010) From Nanchang University. Now she is lecturer of Fuzhou Medical College of Nanchang University. Her current research interests include computer application, algorithm design, computer teaching.

**Xiangjun Li**, Male, was born on January 3rd, 1972, from Pingxiang city in Jiangxi Province, China. He received his B.S. in Mathematics Education (1994) from Jiangxi Normal University, China and M. Eng. in Computer Application Technology (2004) from Nanchang University, China. Mr. Li is currently a professor and master's supervisor in Department of Computer Science and Technology of Nanchang University, China. His areas of research interest are artificial intelligence, knowledge discovery in database and network security, especially on rough sets and granular computing.

**Xinquan Yan**, Male, was born on August 13rd, 1970, from Fuzhou City, Jiangxi province, China. He received his Bachelor's Degree in Mathematics Education (1994) from Jiangxi Normal University. Now he is high school senior teacher of Linchuan No.1 middle school of Jiangxi Province, his current research interest include Senior Middle School Mathematics Education and Computer application.

**Song Qing**, Male, was born on November 10th, 1992, from Ganzhou city in Jiangxi Province, China. He received his Bachelor's Degree in Network Engineering (2014) from Nanchang University, China. Now he is a postgraduate student in Department of Computer Science and Technology of Nanchang University. His current research interests include big data mining, data anomaly detection.

**Yuanlu Chen**, Male, was born on December 5th, 1991, from Shangrao City, Jiangxi province, China. He received his Bachelor's Degree in Computer Science and Technology (2014) from Nanchang University. Now he is a postgraduate student in Department of Computer Science and Technology of Nanchang University. His current research interests include cryptography, data anomaly detection, computer application.