Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2013, 5(12):738-744

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

Research overview of trust model in distributed systems

Tong Qin

Information Security Center, Beijing University of Posts and Telecommunications

---

ABSTRACT

In order to solve the problem of reliable evaluation in distributed system under Internet environment, we study on trust model which is an effect method of trust and robust in distributed system. Based on historic interactive information between entities, we define and value the behavior trust, and provide a reference data for the establishment of the trust model. In the paper, we introduce the basic concept and the research status of trust models, and deeply analyze the key problems and solutions on trust model. Through the study of some classic trust model, we discuss the existing issues in the present research.

Keywords: trust, trust attribute, trust model, trust management

---

INTRODUCTION

With the rapid development of network and computer technology, the traditional computing model is hard to meet new application needs. For this reason, there has been a new type of distributed computing models, such as grid computing, peer-to-peer (P2P) computing, virtual computing and cloud computing. However, when these distributed autonomous resources join in the system, they also bring about security hazard. Distributed systems which are composed by decentralized resources and variety of applications, is difficult to manage resources under the previous centralized approach. In addition, such as free-riding, oscillating service and malicious evaluation, these dishonest behaviors reduce the trust between resources and also create the risk of system operation. One important way is to build up trust model and management mechanism in solving the trust problem in distributed system. In 1996, Blaze et al. [1] firstly proposed the concept of "Trust Management". The basic idea is to admit incompleteness of security information in open systems, to add safety information in security decisions and to introduce trust management in distributed systems for security issues. In recent years, many researchers study the dynamics of trust relationships in distributed systems, use different mathematical theories and mathematical methods to propose plenty of excellent trust models in various application environments. In this paper, we review the status and progress of trust models and discuss the key problems and solutions to provide better guidance for future research.

The structure of rest part is organized as follows. Firstly, we analyze and introduce the basic concept of trust in detail. Secondly, we review classic trust models and compares different parameters. Finally, we discusses and concludes main problems of next research.

Key issues of trust model

In the network environment, traditional trust management mechanism based on Public Key Infrastructure (PKI) cannot adapt to the security requirement. So, researchers construct trust models for studying on dynamic trust relationship between user nodes. For this, the key issues of trust model are described as follows.

- The definition of trust explains the basic trust relationships between resources, and it is also important to divide trust relationships.
- Trust attributes are objective description of trust features. Moreover, this is a feasible way to construct accurate trust models.

● On the basis of multidimensional trust attributes, trust quantification utilizes mathematical theory and other methods to calculate trust value.
● Researchers are focus on risk factors which hides in the process of trust relationships. For instance, when trust model obtains service feedback to resource provider, it should take into account the identification and containment of malicious evaluation.

Definition of trust
Trust is one of the most primitive human emotions. In early theory, trust mainly involves aspects of psychology, sociology, politics and economics. With the continuous development of industrialized information, trust extends to business management, e-commerce, computer science and other areas. In a distributed system, trust is built on the interaction between resources. That is, trust which describes trust degree between resources is associated with resources and application environment. However, trust relationships can change with resources in dynamic context. This phenomenon also changes with time, assumption, expectation and environment factors. It is hard to quantify and predict [2]. So far, academics in the computer field still do not have a uniform definition of trust. TCG uses expected behavior of an entity and defines as, "If an entity's behavior is always in the expected manner to achieve the target, the entity is credible [3]." Various definitions of trust have been comparatively and comprehensively analyzed by Grandison and Sloman [4]. They define trust as "the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context (assuming dependability covers reliability and timeliness)."

In summary, we define trust as, "trust is on the basis of identity verification, through historical transactions between resources, and is also an authenticity and reliability evaluation which is integrated with identity, service, ability and behavior." In the existing trust models, the relationships of trust are mainly divided into the following categories.

● Intra-domain trust and inter-domain trust
In accordance with geographical information, organization and application type, trust correspondingly classifies into intra-domain trust and inter-domain trust. The method manages resources by domain. Moreover, the entire network is divided into several relatively independent sub-domains which have their own evaluation system and management strategy. It forms a hierarchical trust model for inter-domain autonomy. In general, the transactions between inter-domain resources and intro-domain resources on behalf of their respective domains. This approach solves autonomy, heterogeneity and scalability issues.

● Direct trust and indirect trust
In some trust models, trust evaluates historical transactions among resources. When the transaction time between A and B becomes more and more, trust degree changes. As is shown in figure 1, resource A and B is direct trust when resource B provides service to A.

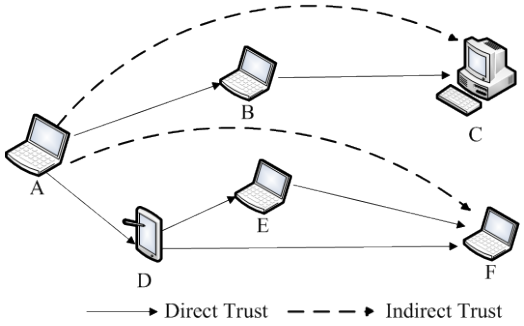

Fig.1: Direct trust and indirect trust

When there is direct interaction between resources, resources assess each other through their own experiences. However, as no direct transaction, resources evaluate the feedback of a third party. In figure 1, there is no direct dealing among E, F and A, but E and F provide direct services to D. Theoretically, D and E provide resource recommendation of F to A. For the scope of recommendation, there are two methods. Resource A only trusts the resources that have indirect services. Another is to collect all the resources interact with F. As can be seen, B, C and F have no interaction, so that there is no effect on its indirect trust. In the first method, although the scope of collection is very broad, it can lead to malicious recommendation. In contrast, the second method is much more suitable for trust mechanism in the human society.

Trust attributes

Trust attributes is one of the key researches of trust model and the basis of excellent trust model. It is complex to describe all the attributes. Integrated with previous studies, we introduce main trust attributes in this paper.

(1) Trust subjectivity

Trust is the authenticity and reliability of expected evaluation, is also to establish a subjective judgment in the historical transactions. Different factors can affect the result of trust which includes context, time and behavior and so on.

(2) Trust dynamics

The nature of trust relationships decides trust dynamics. In a distributed system, trust degree of resource is composed by condition of hardware and software (e.g., CPU, hard disk, memory, etc.), application environment (e.g., network, power supply, etc.) and human factors (e.g., psychology, behavior, etc.). Although trust dynamics is difficult to judge and predict, trust model can utilize external phenomena to quantify and manage trust.

(3) Trust variety

Trust relationships and standard are numerous, even for the same resource, different standard cause different result of trust evaluation. In addition, trust relationships can divided into four types from amount of resources as follows. Figure 2 explains these trust relationships.

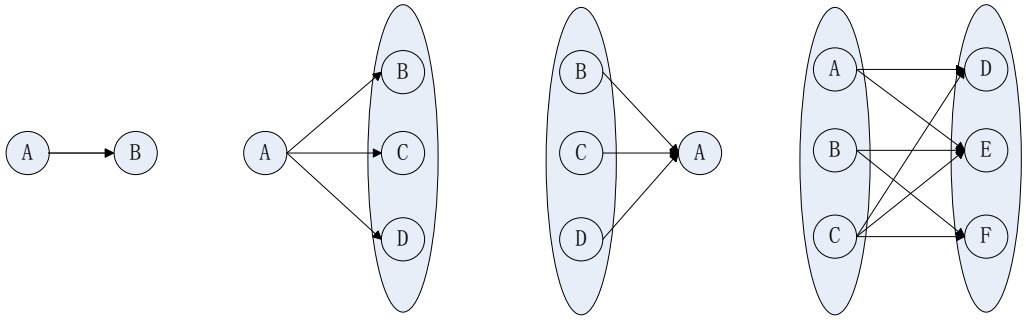

Fig.2: Trust relationships

(4) Trust asymmetry

When resource A trusts resource B, it is not equivalent that B trust A. That is, trust cannot be identical. To some extent, if resource B trusts resource A, the trust degree between them is limited.

(5) Trust transitivity

In the process of interaction between resources, they based on historical interaction evaluate each other. Trust relationship which is built up by direct transaction is called direct trust. In contrast, indirect trust means recommendation by trusted third party. During the trust transfer process, if A trusts B, and B trusts C, A may be a certain degree of trust in C. Therefore, trust has the nature of transitivity.

(6) Antonym of context

In the definition of trust, trust is composed by identity, service, ability and behavior. For example, service and recommendation are two kinds of trust relations, like economic relations buy and sell. In the case, trust attributes have changed. Resource A can provide good service, which does not represent an honest recommendation provider.

(7) Time attenuation

Trust degree changes over time. In a period of time, trust degree is limited to transaction frequency. If there is no interaction between resource A and B in a long time, trust degree will be decline. According with society mechanism, recent transaction has better able to reflect trust degree.

(8) Trust quantifiability

Although the evolution of trust is difficult to measure, trust model can quantify resource trust by external phenomenon. Through mathematical theory and social mechanism, trust model can quantify and evaluate the degree of trust in resources. Moreover, it can be combined reward incentive mechanism to promote resource utilization.

Trust value representation

Trust quantification describes the trust degree by mathematical method. At present, the main expression methods are discrete value, probability, fuzzy value, gray value and trust cloud, etc. All the methods reflect different trust degree besides discrete value.

(1) Discrete value

Trust model [5-12] uses the discrete value which represents different kinds of trust. In general, they introduce two discrete values 0 and 1. In literature [10], authors employ four discrete values {G, L, N, B} which are mapped to four levels of service quality. This method is easy to implement. But the discrete classification is hard to accurately describe trust degree.

(2) Probability value

Trust models [13-20] choose this method to express trust value, and the general value interval [0,1]. Moreover, 0 represents complete distrust, 1 indicates totally trust. For example, the expression of trust degree between resource p and q is $Trust(p,q) \in [0,1]$. Although the method describes trust degree, it brings randomness and ignores subjectivity.

(3) Fuzzy value

Some literatures [21-26] utilize fuzzy theory to construct trust model which use eigenvector, grade of membership and other concepts to infer trust degree. Literature [19] defines various trust degree through fuzzy sets $T_i \in £(X)$ (i=1,2,…,n). Trust value representation method based on fuzzy theory is well to solve the dynamic nature of trust.

(4) Gray value

This method is on the basis of gray system theory. Through weight function, gray system theory quantifies the key attributes which is hardly described by value and defines gray correlation degree of trust value. In [27-30], researchers take advantage of gray theory to establish trust model. Compared with fuzzy theory, gray theory is more suitable for solving sparse data in distributed systems.

(5) Trust cloud

Trust cloud [31-36] references cloud model to express trust degree by a triple elements (E_x, E_n, H_e). In the model, E_x describes trust degree between entities, E_n is entropy which expresses trust dynamics and H_e is ultra entropy which represents uncertain of E_n. The method can well describe trust dynamics.

Risk factor

To establish excellent trust model, the important issue is risk factor which can lead to trust model failure. Plenty of computing models which includes P2P, cloud computing and virtual computing are focus on risk factor to improve the adaptability of trust model. Most models propose feasible program to avoid potential risk. Due to historical transactions, they promote honest evaluation to service provider. In section 3, we review classic trust model and draw the comparison in detail.

DISSCUSSION

Comparison of classic trust model

In this part, we review the classic trust model under different computing environment. In P2P, there are many excellent trust models which consider the risk factor to resist attacks. Here, three trust models are illustrated as follow.

Trust model in Peer-to-Peer environment

● EigenTrust

DK Sepandar et al. [5] propose EigenTrust. Based on history of uploading files, system individually assigns a globally unique value. When EigenTrust computes trust value of a user node, all nodes in the network determine the final value of global trust by performing a specific algorithm. But EigenTrust sets pre-trust node, once this type of nodes has malicious behavior that service provides get inconsistent with the actual evaluation, these nodes will result in EigenTrust failure.

● PeerTrust

X Li et al. [14-15] present PeerTrsut to mange reputation. In PeerTrsut, there are five trust references which are the amount of satisfaction feedback, the number of transaction, transaction content and community content. And it calculates trust degree of node by self-similarity and satisfaction. Moreover, trust degree of node is determined by neighbor nodes. On account of these five references, its disadvantage is network overhead serious in large-scale P2P.

● R^2Trust

In recent research, R^2Trust is proposed by Tian Chunqi et al. [19]. It divides trust degree of network node into direct trust degree, recommendation trust degree and risk factor. And it computes risk factor by information entropy in information theory. This model can resist some malicious attacks, such as simple attack, collusion attack and strategy attack. But it cannot resist relatively complex sybil attack.

Trust model in distributed systems

Besides P2P, trust model is widely used to promote resource utilization in other computing environment. For Internet-based virtual computing environment (iVCE), trust management is a feasible way to resist operation risk.

● CRep

CRep model [8] introduces the concept of autonomous element group and group topology. Autonomous element i evaluates service of autonomous element j which is marked as E_{ij}, and the value range is {(1,0), (0,1)}, where (1,0) represents satisfactory service, (0,1) is unsatisfactory service. Group service evaluation between group C_A and C_B ($A \neq B$) represents all the service of group C_B in a period of time. And it improves resource services through incentive mechanisms.

● Trust model based on Bayesian

In theory of Bayesian, trust model uses probability to express uncertainty in the trust relationship. And trust degree also obtains from probabilistic reasoning. Some researchers introduce Bayesian probability to construct trust models. For example, trust model proposed by Y Wang and J Vassileva [13] consider multidimensional parameters to evaluate trust degree. However, it ignores the authenticity of feedback and various construction of network. Besides, Bayesian theory does not describe trust subjectivity.

● Trust model based on fuzzy theory

Fuzzy theory can be well represented trust uncertainty and subjective of trust relationships. Literatures [21-23] investigate the fuzziness of trust subjective and construct subjective trust management model on the basis of fuzzy set theory. Yet, when subordinating degree function is defined, it is hard to change special subordination degree. In a sense, the model is lack of flexibility.

● Trust model based on gray theory

To solve trust evaluation in distributed systems, literature [27] uses gray number to represent trust evaluation between entities. According with clustering method, trust model divides attributive class of entities. Grey theory and fuzzy theory are an effective way to describe dynamics of trust relationship.

● Trust cloud model

In literature [33], L Deyi et al. propose the concept of subjection cloud. On the basis of this, researchers are focus on trust model to solve decision making problem in cloud computing. Trust cloud model designed by M Xiangyi et al. [34] well express the dynamics and uncertainty of trust. According to trust cloud, it achieves direct and indirect trust recommendation between entities.

Parameter comparison

Table 1 is combined with previous studies on trust, it primarily divides trust model by five parameters. Application environment describes the major requirement of trust. Furthermore, value representation and mathematical theory are important approach to study trust model. Trust attributes in different environment are various. Similarly, risk is mainly associated with above parameters. Table 1 compares eight kinds of trust models with these five references as follow.

Table 1: Comparison of trust model

Trust model	Comparison of references				
	Application environment	Value representation	Mathematical theory	Trust attributes	Risk
EigenTrust	P2P	Discrete value	Vectors	subjectivity, dynamics, transitivity	Higher
PeerTrust	P2P	Probability value	Random mathematics	subjectivity, dynamics, asymmetry, transitivity, context, time attenuation	Lower
R^2Trust	P2P	Probability value	Information entropy	subjectivity, dynamics, asymmetry, transitivity, context, time attenuation	Lower
Bayesian	Bayesian network	Probability value	Bayesian probability	dynamics, asymmetry, transitivity,	High
CRep	iVCE	Discrete value	Vectors	subjectivity, dynamics, transitivity, time attenuation	Low
Fuzzy	Distributed system	Fuzzy value	Fuzzy theory	subjectivity dynamics asymmetry transitivity	Low
Gray	Distributed system	Gray value	Gray theory	subjectivity dynamics asymmetry transitivity	Low
Trust cloud	Cloud computing	Trust cloud	Random mathematics, fuzzy mathematics	subjectivity dynamics variety asymmetry transitivity	Low

CONCLUSION

Research on trust model aims to improve service quality and solve security problems in open internet environment. These provide a strong foundation for next exploration. However, most study is focus on behavior and identity trust. There are still plenty of issues that need further study as follow.

(1) In study of behavior trust, analysis of network behavior is the basis of trust classification. On account of various trust characteristics, it has great significance for establishing trust model.

(2) Most trust models only consider the relationship of intra-domain trust, while inter-domain trust is a lack of exploration. In the meantime, dividing trust domain is also urgent to solve.

(3) In the process of constructing trust model, value representation and mathematical theory can greatly affect the result of trust evaluation. Meanwhile, it should take into account the features of application environments and different trust purpose.

(4) With the rapid development of network application, more and more attacks appear in internet. How to resist numerous attacks is worth exploring. In addition, it should consider scalability, network overhead and other factors to establish more practical significant trust model.

Acknowledgements
This paper is supported by the National Basis Research Program of China (No.2011CB302605).

REFERENCES

[1] M Blaze; J Feigenbaum. *The 17th Symposium on Security and Privacy*, **1996**, 164-173.
[2] L Xiaoyong; G Xiaolin. *Journal of computers*, **2009**, 32(3), 405-416.

[3] C Kaidi; C Jiannliang. *KSII Transactions on Internet and Information Systems*, **2012**, 6(1), 5-23.
[4] J Audun; I Roslan; B Colin. *Decision support systems*, **2007**, 43(2), 618-644.
[5] DK Sepandar; TS Mario; Hector GM. *Proceedings of the 12th Int'l Conf. on World Wide Web*, **2003**, 640-651.
[6] Z Qian; Z Xia; W Xuezhi; et al. *Journal of Software*, **2006**, 17(1), 96−107.
[7] D Wen; W Huaimin; J Yan; et al. *Journal of software*, **2004**, 15(4), 571-583.
[8] T Yangbin; W Huaimin; C Junsheng. *Journal of software*, **2007**, 18(8), 1968-1986.
[9] V Cahill; B Shand; E Gray; et al. *IEEE Pervasive Computing*, **2003**, 2(3), 52-61.
[10] L Zhengqiang; S Weisong. *Proc. of the 38th Annual Hawaii International Conference on System Sciences*, **2005**, 201-211.
[11] L Jingtao; J Yinan; Xiao xiaochun; et al. *Journal of software*, **2007**, 18(1), 157−167.
[12] Z Rufang; H Kai. *IEEE Transactions on parallel and distributed systems*, **2007**, 18(4), 460-473.
[13] Y Wang; J Vassileva. *Proceedings of IEEE/WIC Int'1 conference Web Intelligence*, **2003**. 372-378.
[14] X Li; L Ling. *Proceeding of Fourth ACM Conf. Electronic Commerce*, **2003**, 228-229.
[15] X Li; L Ling. *IEEE Transactions on knowledge data engineering*, **2004**, 16(7), 843-857.
[16] D Anupam; MM Islam. *IEEE Transactions on dependable and secure computing*, **2012**, 9(2), 261-274.
[17] J Shouxu; L Jianzhong. *Journal of software*, **2007**, 18(10), 2551−2563.
[18] T Jing; S Leping. *Journal of Harbin institute of technology*, **2010**, 42(7), 1172-1176.
[19] X Changyou; Y Li; Z Yusen; et al. *Journal of Southease University (Natural Science Edition)*, **2012**, 42(5), 803-807.
[20] T Chunqi;Y Baijian. *Future Generation Computer Systems*, **2011**, 27(8), 1135-1141.
[21] J Sabater; C Sierra. *Proc. of the 1st Int. Joint Conf. on Autonomous Agents and Multi-agent Systems*, **2002**, 475-482.
[22] Z Zhengzhen; L Yonglong; G Liangmin; et al. *Journal of computers*, **2011**, 6(8), 1634-1638.
[23] S Schmidt; R Steele; TS Dillon; et al. *Applied Soft Computing Journal*, **2007**, 7(2), 492-505.
[24] C Chao; W Ruchuan; Z Lin. *Acta Eletronica Sinica*, **2010**, 38(11), 2505-2509.
[25] M Shunan; H Jingsha; G Feng; et al. *Proc. of the 3rd international conference of security of information and networks*, **2010**, 27-31.
[26] C Zhigang; L Limiao; G Jingsong. *International journal of advancements in computing technology*, **2012**, 4(8), 67-74.
[27] X Lanfang; H Huaifei; S Zixia; et al. *Journal of software*, **2007**, 18(7), 1730-1737.
[28] W Pan; Z Shunyi; C Xuejiao. *International journal of advancements in computing technology*, **2011**, 3(10), 75-84.
[29] S Yu; W Ling. *Proc. of the 2nd international conf. on networks security; wireless communications and trusted computing*, **2010**, 513-516.
[30] X Lanfang; H Huaifei; W Aimin; et al. *Jouranl of Huazhong university of science and technology (natural science edition)*, **2007**, 35(11), 92-95.
[31] W Shouxin; Z Li; L Hesong. *Journal of software*, **2010**, 21(6), 1341-1352.
[32] H Haisheng; W Ruchuan. *Journal on communications*, **2008**, 29(4), 13-19.
[33] L Deyi; M Haijun; S Xuemei. *Journal of computer research and development*, **1995**, 32(6), 15-20.
[34] M Xiangyi; Z Guangwei; L Changyu; et al. *Journal of System Simulation*, **2007**, 19(14), 3310−3317.
[35] Y Dingguo; C Nan; T Chengxiang. *Information Technology Journal*, **2011**, 10(4), 759-768.
[36] D Min. *Advances in information sciences and service sciences*, **2012**, 4(19), 132-138.