International Journal of Grid and Distributed Computing
Vol.7, No.1 (2014), pp.135-148
http://dx.doi.org/10.14257/ijgdc.2014.7.1.13

DSRTrust: A Dynamic Trust Model of Distinguishing Service and Recommendation for Internet-based Virtual Computing Environment

Tong Qin[1] and Xinran Liu[2]

[1]*Information Security Center*
Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]*National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC), 100029 Beijing, China*
qintongbupt@163.com, lxr@cert.org.cn

Abstract

Internet-based virtual computing environments (iVCE) are open, anonymous and dynamic in nature. Such characteristics bring about threats and vulnerabilities in providing trusted services and improving resource utilization. Therefore, a dynamic trust model for distinguishing service and recommendation is proposed. In this paper, we analyze multidimensional decision factors related to the evaluation of autonomous node, such as user satisfaction, reward function, punishment function and time decay function. According to the network connection degree of node, our model assigns a new trust weight that specifically describes the relationship between network and trust in iVCE. We then propose a dynamic quantitative model for measuring different kinds of trust. Simulation results indicate that our model can effectively cope with malicious behavior and exhibits evident advantages in resource utilization compared with existing models.

Keywords: *trust model, trust management, iVCE, distinguish service and recommendation*

1. Introduction

With the rapid development of network and computer technology, large-scale Internet-oriented distributed systems have been emerging. Such systems include P2P computing, grid computing, cloud computing and virtual computing. Virtual computing relies on the self-organization of autonomous resources to achieve synergies and efficient aggregation has become an important distributed computing model. Internet-based virtual computing environment (iVCE) is built on an open Internet infrastructure by integrating and utilizing distributed autonomous resources to provide a harmonious, secure and transparent environment for end-users or application systems and ultimately transform the Internet from a "possible computing platform" to a "credible computing platform" [1]. However, numerous deceptive and unreliable services which often lead to the decline of resource utilization and service quality can be found in dynamic distributed applications. We look into some of the most popular and classic works on the trust model for literature review. Researchers have long been studying trust management [2], mathematical theories and social networks to construct trust models for suppressing malicious behavior.

Most models have been extensively discussed in previous literature. In recent study, a similar research confused the relationships of trust [3, 5]. They assume that a good

ISSN: 2005-4262 IJGDC

service provider is an honest resource recommender [4]. In other words, a resource recommender which provides reliable evaluation of nodes can provide good service quality [6, 7]. In contrast, the reality often fails expectations. Service trust (ST) is different from recommendation trust (RT). A node that provides good service is likely to provide malicious evaluation [8, 9, 11], which reduces service trust. To describe trust attributes objectively, some works are oriented to describe the dynamic trust factors which can affect the objectivity and accuracy of trust quantitative model [10, 12]. For this, existing models [11-13] propose much more evaluated factors. Subsequently, literatures [14-16] focus on the quantification weights. This observation indicates that the system is short of adaptability [15, 17]. Moreover, once the weight is defined, the system has difficulty adjusting this value [18, 19].

It is important to note that, most models mentioned above ignore the significant relationship between trust and distributed network. In this paper, we present a dynamic trust model separating service and recommendation in Internet-based virtual computing environments (iVCE). The major contributions are detailed as follows:

(1) The relationships of trust are analyzed in detail, and divided into service trust and recommendation trust for providing good service quality and higher resource utilization.

(2) To describe trust attributes objectively, some trust factors are discussed in DSRTrust, such as user satisfaction, time attenuation, reward and punishment function and network path length.

(3) The quantification weights are considered as the network complexity and social network to make an objective and accurate measure.

(4) DSRTrust can resist major attacks, such as simple attack, collusion attack and strategy attack to show better adaptability.

The structure of the paper is organized as follows. In section 2, we review the most recent related works. Section 3 describes the basic evaluation process in iVCE. In section 4, we introduce the dynamic trust computation model in detail. To show the performance of our model, the experiments and comparison are discussed in section 5. Finally, we draw the conclusion of the paper in section 6.

2. Related Work

Resource sharing in the Internet environment has been one of the most important areas of security research. Blaze *et al.*, [2] firstly propose trust management to solve the security problem of network service. Wang *et al.*, [1] discuss and explore the solution of trusted software. They put forward a trusted system which is combined with identity, ability and behavior. The characteristics of autonomous node bring issues in resource utilization. Many researchers study on the behavior trust in grid computing, P2P and other distributed computing.

In this section, we look into the prevalent research works focused on the trust model. To reduce dishonest file download, EigenTrust [3] assigns a globally unique value of the trust model based on historical transactions individually. According to the transaction, users make two kinds of evaluation which can hardly describe the trust degree. When the trust of a node is calculated, all the nodes in the network need to determine the final value of global trust by performing a specific algorithm. EigenTrust introduces some pre-trusted nodes which are not readily available. Once these nodes have malicious behaviors, their resource provider nodes will get inconsistent evaluation and launch large-scale malicious attacks. This situation will result in the failure of EigenTrust model.

Li XY *et al.*, [9-10] propose a sliding window to reduce the hidden calculated risks of network nodes. And according to them, the smaller risk window will get more accurate calculations. In contrast, the accuracy of the calculation reduces the efficiency and availability of network resources. The trust model represented by Xiong L *et al.*, [7] is similar. PeerTrust [7] designs five parameters to compute the trust degree of nodes, including the amount of trust satisfaction, trading volume, feedback credibility, transaction content and community content. Xiong's model is combined with self-similarity and satisfaction to calculate the trust degree of network nodes. In the model, trust evaluation of network nodes is provided by the neighboring network nodes. In the recent time window, PeerTrust model retrieves all the transactions to compute the trust degree. However, the calculation accuracy in large number of applications make network overhead serious. The limitation of this approach is that the computation convergence rate in large-scale P2P systems is not easy to achieve. Furthermore, each transaction has the same weight in time window. Actually, recent transactions should be given higher weight than historical transactions.

The above researches are based on the assumption that good service quality of the node has higher trust degree. In iVCE, the behavior of node is separated into service and recommendation. These models only consider one-sided factor to quantify the evaluation of node, which is difficult to resist malicious attacks. If this malicious behavior is not punished, such behavior will affect the service quality and even cause the failure of task scheduling. In the paper, we propose a dynamic trust model in iVCE based on previous research. DSRTrust model considers multiple decision factors, including time attenuation, reward and punishment mechanism and network complexity. In addition, the model emphasizes the decrease in historical trust over time and the important relationship between trust and network. Thus, the model has higher practical value. Finally, a simulation experiment on this model is analyzed and compared with that on other classical models. The experiment proves that the model has dynamic adaptability, better robustness and security.

3. Trust Evaluation Model

Trust is one of the most primitive and complex human emotions and in the Internet, trust also has its own special features, such as uncertainty, asymmetry, antisense, partial transitivity, asynchronous and complex nature. In this section, we present the basic process of trust evaluation and introduce the measure of trust.

3.1. Basic Framework

In Figure 1, the roles of trust mainly consist of the service requester (SR), resource provider (RP) and resource recommender (RR). Moreover, trust is divided into service trust (ST) and recommendation trust (RT) based on the type of trust relationship. Service trust is given by SR based on the service satisfaction of RP, whereas recommended trust is given by RR which RP services. We assume that all the SRs will provide RP service satisfaction (SSat) and at the same time provide RP recommended satisfaction (RSat) to other nodes.

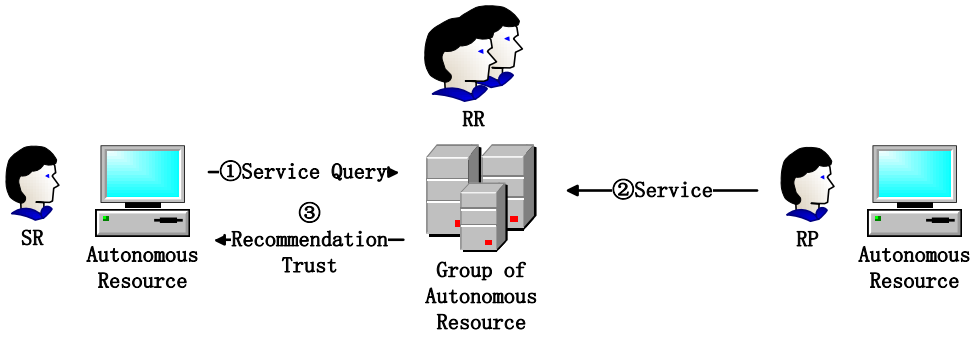


Figure 1. Trust Evaluation Process

An honest node always offers reliable service and recommendation. However, a malicious node will change its behavior. In the process of established relationship, trust is mainly divided into direct trust and indirect trust. Direct trust is given by the interaction of nodes, whereas indirect trust is generated by a third party that can be seen in Table 1. To describe services and recommended actions objectively and accurately, we propose that service and recommendation be distinguished in a quantitative trust model.

Table 1. Description of Trust

Description	Direct Trust	Indirect Trust
Service Trust (ST)	Direct Service Trust (DST)	Indirect Service Trust (IST)
Recommendation Trust (RT)	Direct Recommendation Trust (DRT)	Indirect Recommendation Trust (IRT)

The main title (on the first page) should begin 1 3/16 inches (7 picas) from the top edge of the page, centered, and in Times New Roman 14-point, boldface type. Capitalize the first letter of nouns, pronouns, verbs, adjectives, and adverbs; do not capitalize articles, coordinate conjunctions, or prepositions (unless the title begins with such a word). Please initially capitalize only the first word in other titles, including section titles and first, second, and third-order headings (for example, “Titles and headings” — as in these guidelines). Leave two blank lines after the title.

3.2. Trust Evaluation

In DSRTrust model, the trust degree is calculated based on three aspects: service trust, recommendation trust and overall trust. Each part of trust evaluation is computed by user satisfaction. As shown in Table 2, the satisfaction grades represent different degrees of evaluation. The grades are divided into four levels. ED_1 indicates that the nodes can provide good service or honest recommendation and that the trust degree of nodes should improve. ED_2 shows that the nodes have the common capability of service and recommendation, so the trust value will slightly rise. ED_3 denotes that network nodes provide malicious service and dishonest recommendation. The system will punish such nodes and trust will fall sharply. ED_4 indicates that the network nodes exhibit malicious behavior, such as the spread of malicious code or virus, and the trust value of this type of malicious node will sharply decline.

Table 2. Satisfaction Grades

Satisfaction Grades	*SSat(i,j)*	*RSat(i,j)*	Description
SD_1	(0.8,1]	(0.8,1]	Good
SD_2	(0.6,0.8]	(0.6,0.8]	Common
SD_3	(0.2,0.6]	(0.2,0.6]	Malicious
SD_4	[0,0.2]	[0,0.2]	Bad

The details of calculating the trust will be discussed in Section 4. The overall trust measures the node of trust degree in iVCE. The weight of service and recommendation trust is associated with network complexity.

4. DSRTrust Model

In this section, we present a dynamic trust model which distinguishes service and recommendation in detail. DSRTrust model introduces multidimensional factors to calculate three kinds of trust degree.

4.1. Multidimensional Factors

Trust is influenced by numerous factors. In this section, we consider three important factors to calculate trust degree. These factors include network, time, and incentive mechanisms. In the distributed system, network topology is the precondition of node behaviour. When nodes are connected on the physical layer, the interactive nodes can establish a trust relationship. At the initial conditions, trading nodes obey the principle of proximity, and the initial value of each node is zero.

Service trust indicates that the autonomous node *i* acts as RP to provide n times the services within trading time t, and node i obtains the ratings sequence $\{SSat_1, SSat_2, \ldots, SSat_n\}$. In all service transactions, trust is divided into direct service trust (DST) and indirect service trust (IST). According to a certain proportion, service trust is calculated through accumulation and is combined with the time attenuation function and reward and punishment function.

The time attenuation function (TF_n) denotes that trust is gradually reduced over time. When an autonomous node is idle for a long period of time, the trust degree should gradually decline. Here, λ is the decay constant and it controls the speed that the value declines to zero. As time interval Δt from the moment of last service t_{last} to the present t_{now} is larger, its trust degree is smaller. TF_n is computed as follows:

$$TF_n = e^{-\lambda \Delta t} = e^{-\lambda (t_{now} - t_{last})} \qquad (1)$$

To encourage honest services, the DSRTrust model introduces reward and punishment function (RPF_n) which is divided into reward function (RF_n) and punishment function (PF_n) to describe the trust degree. They are separately calculated by the adjacent satisfaction difference ΔSat_n, which is calculated as follows:

$$\Delta Sat_n = Sat_n(i,j) - Sat_{n-1}(i,j) \qquad (2)$$

In the incentive mechanism, we define the accumulated trust value on the basis of reward constant r_1, r_2, and r_3, which should meet the condition $r_1 < r_2 < r_3$. RF_n encourages and rewards good behavior, which results in the following equation:

$$RF_n = \begin{cases} e^{-r_1*|0.4-\Delta Sat_n|}, \\ \quad 0.6 < Sat_{n-1}(i,j) \le 1, 0.6 < Sat_n(i,j) \le 1 \text{ and } 0 \le \Delta Sat_n < 0.4 \\ e^{-r_2*|1-\Delta Sat_n|}, \\ \quad 0 \le Sat_{n-1}(i,j) \le 0.6, 0.6 < Sat_n(i,j) \le 1 \text{ and } 0 < \Delta Sat_n \le 1 \\ e^{-r_3*|0.6-\Delta Sat_n|}, \\ \quad 0 \le Sat_{n-1}(i,j) \le 0.6, 0 \le Sat_n(i,j) \le 0.6 \text{ and } 0 \le \Delta Sat_n < 0.6 \end{cases} \quad (3)$$

In the punishment mechanism, the situation that causes the decline of service or recommen dation satisfaction is given a different degree of punishment. Here, p_1, p_2, and p_3 are defined a s punishment constants, which should meet the condition $p_1 < p_2 < p_3$. The expression of PF_n becomes:

$$PF_n = \begin{cases} -e^{-p_1*|1+\Delta Sat_n|}, \\ \quad 0.6 < Sat_{n-1}(i,j) \le 1, 0 \le Sat_n(i,j) \le 0.6 \text{ and } -1 \le \Delta Sat_n < 0 \\ -e^{-p_2*|0.6+\Delta Sat_n|}, \\ \quad 0 \le Sat_{n-1}(i,j) \le 0.6, 0 \le Sat_n(i,j) \le 0.6 \text{ and } -0.6 \le \Delta Sat_n \le 0 \\ -e^{-p_3*|0.4+\Delta Sat_n|}, \\ \quad 0.6 < Sat_{n-1}(i,j) \le 1, 0.6 < Sat_{n-1}(i,j) \le 1 \text{ and } -0.4 \le \Delta Sat_n < 0 \end{cases} \quad (4)$$

4.2. Service Trust Degree

DST is given by SR on the basis of its own transaction experience. $DST_n(i, j)$ means the DST degree between SR i and RP j. Through Formula (5), the value is calculated as follows:

$$DST_p(i,j) = SSat_p(i,j) + \left[1 - SSat_p(i,j)\right] \cdot RPF_p(i,j) \quad (5)$$

IST is computed on the basis of the recommendation of the third node k. $IST_n(i, j)$ is computed as follows:

$$IST_q(i,j) = RT_q(i,k) \cdot DST_q(k,j) \quad (6)$$

We assume that SR i has n transactions with RP j in the current time cycle t. A$DST_m(i, j)$ denotes m direct service trust, which is accumulated as follows:

$$ADST_m(i,j) = \sum_{p=1}^{m} [DST_p(i,j) \cdot TF_p] \quad (7)$$

$AIST_{n\text{-}m}(i, j)$ represents (n-m) indirect service trust degree, we get:

$$AIST_{n-m}(i,j) = \sum_{q=1}^{n-m} IST_q(i,j) \quad (8)$$

Here, we propose trust factor α, which is decided by the user, and $\alpha \in [0,1]$. In general, the SR is inclined to trust its own trading experience. That is, α meets the condition $0.5<\alpha<1$. Service trust degree $ST_n(i, j)$ is defined as follows:

$$ST_n(i,j) = \alpha \cdot ADST_m(i,j)/m + (1-\alpha) \cdot AIST_{n-m}(i,j)/n-m \quad (9)$$

4.3. Recommendation Trust Degree

RT describes the degree on the basis of RR and RP. RT refers to the feedback evaluation given by SR. The network path length (NPL_{ik}) between SR and RR is one of the most

important factors. When two autonomous nodes are close, we believe that the service or recommendation evaluation has significantly more reference value. When NPL_{ik}=1, the recommendation trust degree is called direct recommendation trust and defined as $DRT(i, k)$. When $NPL_{ik} > 1$, RT degree is called indirect recommendation trust and defined as $IRT(i, k)$. $DRT_n(i, k)$ denotes the nth recommended evaluation between i (SR) and k (RR), and computation formula is computed as follows:

$$DRT_n(i,k) = RSat_n(i,k) + [1 - RSat_n(i,k)] \cdot RPF_p(i,k) \quad (10)$$

$IRT_n(i, k)$ denotes the indirect recommendation trust of SR i and RR k, for this, we get:

$$IRT_n(i,k) = \frac{RSat_n(i,k) + [1 - RSat_n(i,k)] \cdot RPF_n(i,k)}{NPL_{ik}} \quad (11)$$

We assume that RR k has r transactions with RP j in the current time cycle t. $ADRT_r(i, j)$ denotes r direct RT, and the equation becomes:

$$ADRT_r(i,k) = \sum_r DRT_r(i,k) \quad (12)$$

In Formula (13), the accumulated value of indirect RT value $AIRT_{n-r}(i, j)$ is computed as follows:

$$AIRT_{n-r}(i,k) = \sum_{n-r} IRT_{n-r}(i,k) \quad (13)$$

As can be seen, $RT_n(i, k)$ is calculated as follows:

$$RT_n(i,k) = ADRT_r(i,k)/r + AIRT_{n-r}(i,k)/n - r \quad (14)$$

4.4. Overall Trust Degree

Overall trust degree is a combination of service trust and recommendation trust in a certain weight, which is generally a subjective distribution in most models. This method ignores network importance. In our model, we consider this key factor and propose that the weight distribution is confirmed by the network connection degree. By definition, network connection degree NC_i shows the connection number of node i. In iVCE, we assume that all autonomous nodes are marked as 1,2,…,n. Therefore, all network connection degrees can be marked as NC_1, NC_2,…, NC_n. Through Formula (15), the weight of node i based on the network connection degree is computed as follows:

$$RNet_i = NC_i \Big/ \sum_{i=1}^{n} NC_i \quad (15)$$

For this, the overall trust degree $OT(i, j)$ between SR i and RP j can be calculated as follows:

$$OT_n(i,j) = RNet_j \cdot ST_n(i,j) + RNet_i \cdot RT_n(i,j) \quad (16)$$

5. Experiments and Comparisons

In this section, we present the results of our experiments to prove the effectiveness of our trust model. First, we prove the computation accuracy in four types of peers. Second, we compare the proposed model with two classical models, EigenTrust and PeerTrust, and

evaluate its effectiveness in the presence of malicious peers.

5.1. Simulation Environment

According to the complex network theory, we construct a network based on the BA scale-free network model to approach the real-world networks using Matlab 2008. In the experiment, we suppose that 500 nodes are in the network. Other parameters in the experiments are in Table 3.

Table 3. Simulation Parameters Setting

Parameters	Description	Value
α	Weight of direct service trust degree	α=0.7
λ	Time attenuation factor	λ=2
(r_1, r_2, r_3)	Reward factors,$r_1<r_2<r_3$	(2,4,6)
(p_1, p_2, p_3)	Punishment factors, $p_1<p_2<p_3$	(3,6,9)

The four types of nodes are described as follows:

(1) Honest node always provides honest service and recommendation.

(2) Simple attack node provides poor service and false recommendation.

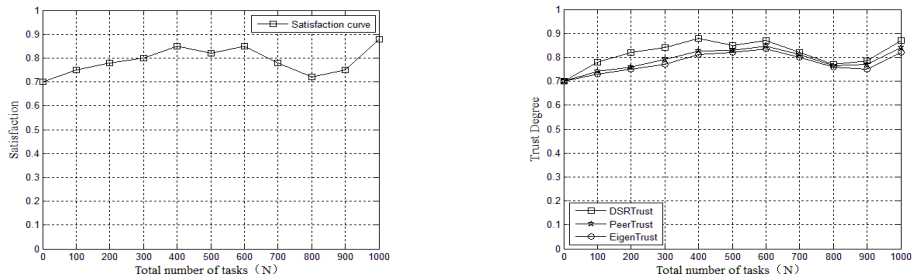
(3) Collusion node only provides good service to its members but provides malicious service to others.

(4) Strategy node, in the initial phase, hides its malicious purpose. When its trust degree becomes higher, this node begins to abuse its own trust and misleads other network nodes.

5.2. Calculation Accuracy

The satisfaction degrees of honest, simple attack, collusion, and strategy nodes differ. In DSRTrust, we compare the calculation accuracy with EigenTrust and PeerTrust.

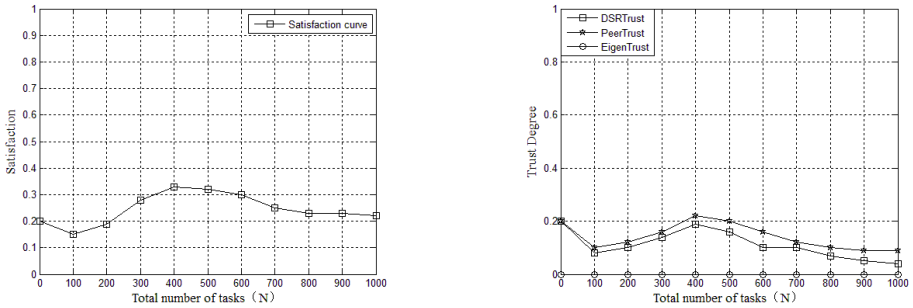
5.2.1. Honest Node: Figure 2(a) denotes the satisfaction of an honest node in 1000 transactions. The main characteristic of honest nodes is that they always provide good trading. When the satisfaction is up, the trust value is also increasing. Figure 2(b) shows that an honest node has a high trust degree, and differences among the three models are not evident. According to the incentive mechanism, the trust degree in DSRTrust is slightly higher.



(a) Satisfaction (b) Trust Degree

Figure 2. Satisfaction and Trust Degree of Honest Node

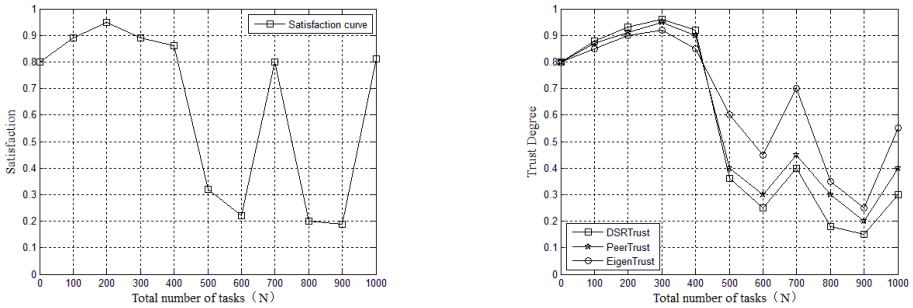
5.2.2. Simple Attack Node: Figure 3(a) depicts the satisfaction of a simple attack node in 1000 tasks. As can be seen, the satisfaction is very low, which leads to the decline of trust value. Figure 3(b) compares the trust value of a simple attack node in three models. The tendency of a simple attack node is always bad. EigenTrust trust value is zero because this model calculates trust degree on the basis of the value of satisfaction. In the other models, the value is nearly the same, because PeerTrust and DSRTrust use discrete values to represent trust.



(a) Satisfaction **(b) Trust Degree**

Figure 3. Satisfaction and Trust Degree of Simple Attack Node

5.2.3. Collusion Node: Figure 4 describes the satisfaction and trust degree of a collusion node in 1000 transactions. A collusion node provides good services to its members but offers malicious services to the others. For this, the satisfaction of a collusion node is unstable. From Figure 4(b), the trust degrees in different models obviously vary. EigenTrust defines the amount of satisfaction to calculate trust degree. Therefore, the trust degree remains high. However, PeerTrust and DSRTrust use discrete value to compute the trust degree. Moreover, DSRTrust considers reward and punishment functions to adjust the trust degree objectively. Thus, the trust degree in DSRTrust is lower.

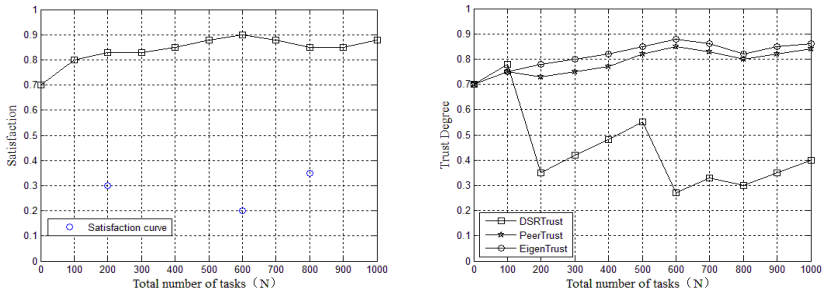


(a) Satisfaction **(b) Trust Degree**

Figure 4. Satisfaction and Trust Degree of Simple Collusion Node

5.2.4. Strategy Node: Figure 5(a) denotes the satisfaction of a strategy node in 1000 tasks. At the beginning of trade, a strategy node provides good services to achieve a higher trust degree. After a period of time, however, this node provides malicious services. Therefore, the satisfaction is almost high. As is shown in Figure 5(b), the tendency of a strategy node is significantly different. In EigenTrust and PeerTrust, the trust degree has similar trends. Because they do not discover this sudden malicious behaviour, and the DSRTrust model gives

the greatest punishment to this situation and sharply lowers the trust degree. Therefore, the trust degree in DSRTrust drops drastically.



(a) Satisfaction **(b) Trust Degree**

Figure 5. Satisfaction and Trust Degree of Strategy Node

5.3. Successful Transaction Rate

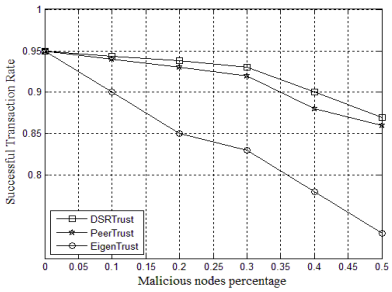


Figure 6. Simple Attack Node

Simple attack is a malicious behaviour that mainly provides malicious services or recommendations. The metrics, called the successful transaction rate, is the ratio of the number of successful transactions to the total. As is shown in Figure 6, when no malicious node is in the system, the successful transaction rate is 95%. As the ratio of malicious nodes increases, all three models of transaction success rate tend to decline. However, the success rate of the DSRTrust model falls to the slowest. EigenTrust does not distinguish the authenticity of the satisfaction, such that the transaction success rate sharply declines. When simple attack nodes reaches 50%, the success rate still remains above 85% in PeerTrust and DSRTrust.

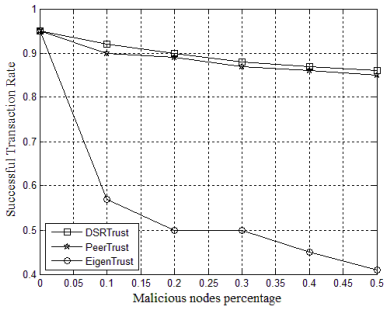


Figure 7. Collusion Node

Figure 7 simulates the results of successful transaction rate, when collusion nodes rise from 0% to 50%. As can be seen, EigenTrust model does not define malicious and honest evaluation, such that the successful transaction rate obviously declines. PeerTrust and DSRTrust, which are both considered the collusion attacks, have much higher successful transaction rates, even when the rate of collusion node is up to 50%. However, PeerTrust model does not take into account the change of satisfaction and different punishments. Yet, because the calculated model dynamically adjusts trust value through the reward and punishment function, DSRTrust has a higher successful transaction rate.

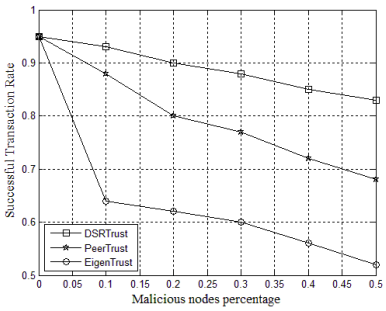


Figure 8. Strategy Node

Figure 8 denotes the simulation of successful transaction rate under the condition of strategy malicious behaviour. Compared with the two other models, DSRTrust model can still maintain high transaction success rate even when 50% of system nodes are malicious nodes. Although EigenTrust model uses the global trust calculation method, it does not consider the dynamic trend of strategy nodes and lacks a reward and punishment mechanism. Once the number of strategy nodes increases, the transaction success rate significantly decreases. Although PeerTrust model can effectively resist the attack strategy behaviour, its trust degree calculation method PSM algorithm, which is restricted by the sliding window, does not effectively reflect the dynamic change. Due to this, the successful transaction rate is higher than that in EigenTrust.

6. Conclusions

In iVCE, the characteristics of an autonomy node lead to various threats and crises. Research on the trust relationship between the autonomy node and mechanism provides an effective way to solve the problem. In this paper, we propose a dynamic trust model of distinguishing service and recommendation (DSRTrust) to solve some issues in existing trust models. Moreover, in combination with reward and punishment functions, the model can objectively and accurately calculate trust degree and resist malicious attack behaviour, such as simple, collusion, and strategy attacks. Analysis and experimental simulation prove that the proposed DSRTrust model retains high efficiency, even when malicious nodes appear at different ratios.

Acknowledgements

This paper is supported by the National Basis Research Program of China (No.2011CB302605), and the National Natural Science Foundation of China (No. 61121061).

References

[1] X. C. Lu, H. M. Wang and J. Wang, "Internet-based Virtual Computing Environment: Beyond the data center as a computer", Future generation computer system-the international journal of grid computing and science, vol. 29, no. 1, **(2013)**, pp. 309-322.
[2] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized trust management", Proceeding of the IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, **(1996)**, pp.164-173.
[3] S. D. Kamvar, M. T. Schlosser and H. G. Molina, "The EigenTrust algorithm for reputation management in P2P networks", Proceeding of the 12th Int'l World Wide Web Conference, New York, **(2003)**, pp. 640-651.
[4] X. Men, Y. Ding and Y. Gong, "Trust: A trust model based on feedback-arbitration in structured P2P network", Computer communications, vol. 35, no. 16, **(2012)**, pp. 2044-2053.
[5] D. Cao, Z. Xiao and W. Shao, "A Service-oriented Programming Platform for Internet-Based Virtual Computing Environment", Proceedings of the International Conference on Parallel and Distributed Systems, Beijing, **(2009)**, pp. 700-705.
[6] G. Q. Zhou and Q. K. Zeng, "Trust evaluation model based on role separation", Journal of Software, vol. 23, no. 12, **(2012)**, pp. 3187-3197.
[7] L. Xiong and L. Liu, "PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities", IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 7, **(2004)**, pp. 843-857.
[8] C. Q. Tian and B. J. Yang, "R^2Trust, a reputation and risk based trust management framework for large-scale, fully decentralized overlay networks", Future generation computer systems, vol. 27, no. 8, **(2011)**, pp. 1135-1141.
[9] X. Y. Li and X. L. Gui, "Trust quantative model with multiple decision factors in trusted network", Journal of Computers, vol. 32, no. 3, **(2009)**, pp. 405-416.
[10] X. Y. Li, F. Zhou and X. D. Yang, "A multidimensional trust evaluation model for large-scale P2P computing", Journal of Parallel and Distributed Computing, vol. 71, no. 6, **(2011)**, pp. 837-847.
[11] D. Anupam and MI. Mohammad, "SecuredTrust: A dynamic trust computation model for secured communication in mutiagent systems", IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, **(2012)**, pp. 261-274.
[12] J. Hu, Q. Wu and B. Zhou, "FCTrust: A robust and efficient feedback credibility-based distributed P2P trust model", Proceeding of IEEE 9th Int'l conference for Young Computer Scientists, Hunan, **(2008)**, pp.1963-1968.
[13] Y. J. Li and Y. F. Dai, "Research on trust mechanism for Peer-to-Peer network", Journal of computers, vol. 33, no. 3, **(2010)**, pp. 391-405.
[14] K. Shao, F. Luo, N. X. Mei and Z. T. Liu, "Normal distribution based dynamical recommendation trust model", Journal of Software, vol. 23, no. 12, **(2012)**, pp. 3130-3148.
[15] N. Iltaf, A. Ghafoor and U. Zia, "An attack resistant method for detecting dishonest recommendations in pervasive computing environment", Proceedings of the IEEE International Conference on Networks, Singapore, **(2012)**, pp. 173-178.
[16] Y. X. Feng and W. Q. Ying, "Adaptive dynamic trust evaluation model for P2P networks", Journal of South China University of Technology (Natural Science), vol. 40, no. 9, **(2012)**, pp. 56-61.
[17] S. X. Wang, L. Zhang and H. S. Li, "Evaluation approach of subject trust based on cloud model", Journal of Software, vol. 21, no. 6, **(2010)**, pp. 1341-1352.
[18] S. X. Wang, L. Zhang, S. Wang and X. Qiu, "A cloud-based trust model for evaluating quality of web services", Journal of Computer Science and Technology, vol. 25, no. 6, **(2010)**, pp. 1130-1142.
[19] H. S. Huang and R. C. Wang, "Subjective trust evaluation model based on membership cloud theory", Journal on Communications, vol. 29, no. 4, **(2008)**, pp. 13-19.

Authors

Tong Qin received her master degree in software engineering from Beijing University of Posts and Telecommunications (BUPT) in 2007. Currently, she is a Ph.D. candidate in Information Security Center at BUPT. Her research is mainly in the area of network security and distributed computing.

Xinran Liu received his Ph.D. in computer architecture from Harbin Institute of Technology in 1998. He is currently a researcher in National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and also a doctoral supervisor in Information Security Center at Beijing University of Posts and Telecommunications in Beijing, China. Professor Liu's research interests include distributed computing and information security.