Trust Evaluation Model based on Service Satisfaction

Ruizhong Du[1,2]
1.Computer School of Wuhan University, Hubei Wuhan, China
2.College of Mathematics and Computer Science of Hebei University, Hebei Baoding, China
durz@mail.hbu.cn

Xiaoxue Ma
Computing Center of Hebei University, Hebei Baoding, China
snow@hbu.cn

***Abstract*—In most of the current trust model, the evaluation of whether an entity is trust is different to different judger. The reason of this phenomenon is that different judger use the different standard in its opinion. So the evaluation lack of convincing, are not well describe the relationship between two parties. In response to these issues, drawing on the trust relationship between human societies, the introduction of the domain and domain trust, building the trust evaluation model based on service satisfaction. In every domain according to the service of the node itself, abstracting representative multiple service attributes from the trusted relationship of the node service, service requester comprehensive evaluates multiple service attributes provided by service provider based on personal interest, and combines with the trust value, decide whether to trade finally; after the transaction, service request calculates QoS(quality of service) difference degree according to actual QoS and service provider' own QoS claimed to judge the credibility of service provider, then gives corresponding rewards and punishment and trust update. The simulation results show that the model can more accurate assessment of the trust entity, to some extent effective against malicious attacks, which proves the validity and accuracy of the model.**

***Index Terms*—trust evaluation model, trust degree, trust domain, service attributes**

I. INTRODUCTION

With the computer technology and communication technology continues to evolve, the network environment has became into a public accessible, a large number of dynamic user-oriented and open network from the relatively static network. The face of massive resources and services, as there is a lot of fraud and unreliable service quality, customer choice, while the increase of how to identify and select efficient and secure resources or services, issues[1]. An effective solution is trust evaluation system[2-6]. Trust evaluation system collect, analyze historical behavior of entities in the future information to predict their likely behavior of transactions in which a trust for the user to select entities to trade higher, thus reducing the risk of transaction failure to avoid losses. Thus, the essence of trust evaluation system is to conduct the entity score, then score is calculated in accordance with a certain algorithm to obtain the trust value of the behavior of the entity for the reference of parties to the transaction.

II. RELATED WORK

Trust is a very subjective and complex concept [7],in 1996, M. Blaze and others the first times put forward the "trust management " concept [8], and the corresponding trust management system developed on this basis. With the large variety of widely distributed application systems, dynamic trust management and evaluation field of information security has become one of the focuses.

EigenTrust model puts forward the distributed computing method based on DHT[9], using the trust algorithm that calculates global trust value by direct trust value with trust transfer characteristics, but this model exists convergence problem, and have the higher communication cost and relative value of global reputation, it makes cannot directly judge whether the node is credible from the global reputation value. Zhou etc. [10] improve the EigenTrust model for the aspects of determination of credible peers and the speed of trust iteration convergence, and puts forward the PowerTrust model. In resistance of the malicious peers aspect, this model stronger than EigenTrust algorithm, but in the calculation of trust value, it doesn't consider the influence of the trust value on trading volume, and has not to make punishment for malicious behavior. PeerTrust model[11,12] uses the confidence factor to synthesize local reputation and global reputation, allow for many factors which could influence measurement of trust, and can deal with false evaluation very well, but PeerTrust model does not give measure method of trust factor and method for determining confidence factor. Asnar Y etc. [13] add trust factor to the risk evaluation, and then get a trust relations division according to trust relationship state, and have a more accurate evaluation of the risk value. Y. Wang etc.[14] first settle service

doi:10.4304/jsw.6.10.2001-2008

recommender roles in the trust recommendation factor, put forward a role-based trust evaluation and recommendation model, but don't give an organization and storage method of specific field "role". TianChunQi etc.[15] propose trust model based on reputation for P2P networks, introduce the risk factor, put forward to use information entropy theory to quantify risk, this model has significant improvement compared with some existing trust model on safety issues. Tien etc.[16] put forward a preliminary infrastructure for P2P-based marketplaces which can identify unfair evaluation, but the infrastructure is quite simple, and need further improvement. Jøsang etc. propose the concept of multiple-valued logic[17,18] based on the subjective logic, with Dirichlet multidimensional probability distribution [19] as the foundation, allowing to have different grades evaluation, which can be used for the calculation of reputation value, provide more flexible platform for design of reputation system. But the model only uses direct evaluation result to calculate trust degree, without considering recommendation trust ,and how to identify malicious evaluation and give it punishment. HuaiJinPeng etc.[20] give a dynamic trust management model facing network computing, define trust formula between subjects based on formalization of faith formula, and regard the trust transfer characteristics as a nature. Literatures [21,22] through the comprehensive analysis of the dynamic trust model related concepts and main problems, research methods, select some new, typical dynamic trust model and algorithm used to evaluate and compare.

When the most trusted models evaluate level of trust about service entities at present, the credibility of the service attributes whether the two sides trading result is credible is rather ambiguous, which makes the evaluation model lack of persuasion, and not very good depict the complexity and uncertainty of trust relationship between the two sides. In the human society, when people choose and buy a commodity, the first concern is whether the function of the goods to meet their needs, and then consider other properties of the goods, such as price, the brand value, appearance, usability, after-sale service and so on, finally purchase the items according to preferences oneself and comprehensive evaluation of each property. Purchased items, if the properties of the goods is consistent with vendors claimed, the seller is considered as trustworthy. Similarly, in the computer network system, the service requester for his services they need, have different needs, interests , preferences and decision attribute, if two request entities A and B ask for a same movie at the same time, entity A needs high-definition movie, however, entity B requires high speed download, this two cases leads to entities disagree on the QoS. It is trustworthy for A when the entity can provide the service of the high quality data resource, but if this entity can not provide high download speed, it is incredible for B, resulting in the disunity of trust definition. Likewise, the service provided by the service provider consists of multiple attributes, the each entities provides different quality of the service attributes.

In view of the above questions, learning trust relationship from human society, according to the service of the node itself, abstracting representative multiple service attributes from the trusted relationship of the node service, service requester comprehensive evaluates multiple service attributes provided by service provider based on personal interest, and combines with the trust value, decide whether to trade finally; after the transaction, service request calculates QoS(quality of service) difference degree according to actual QoS and service provider' own QoS claimed to judge the credibility of service provider, then gives corresponding rewards and punishment and trust update.

III. TRUST MANAGEMENT MODEL

A. SSTEM modle framework

With the increase of network entities, the size and complexity of the network will be increased, the system will become difficult to manage, in this situation fully distributed management overhead will be significantly increased; and modern networks require extensive connectivity application of different entities involved, users create a wide range of effective security mechanisms, and security policies while achieving consistent, so for the convenience of network security management and maintenance, standard research environment, this product information in accordance with the characteristics of the natural properties of a hierarchical classification, the entities in accordance with their respective areas of operation classification of goods in different areas (some entities may belong to multiple domains), the introduction of agents mechanism will be abstracted as shown in Figure 1 network-based field-level trust model as an entity can be measure the relationship between faith and trust in the framework of mechanisms to ensure the credibility of management.

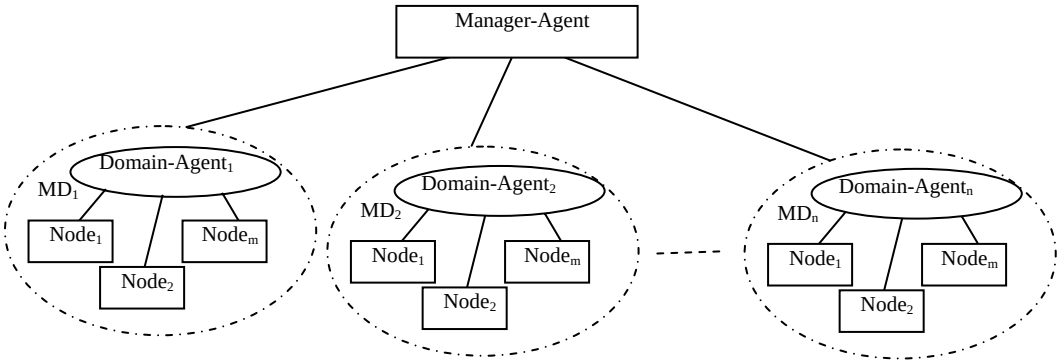

Fig 1 The framework of SSTEM Model

It can be seen from the figure, the model management framework divided into two levels, respectively, by the management domain deputy Manager-Agent and management entity domain information Domain-Agent composed of specific functions:

1) manager-agent is a global trust relationship manager, who manages all domain-agent. It is the root of trust, responsible for the collection and management of domain-agent of the credibility information, maintenance of global trust relationship. The information managed by MA is: ID of domain-agent, domain trust, calculation of global trust and domain model.
2) Domain-Agent is the manager of trust relationship, responsible for the collection and management of all entities within the credibility of information, maintenance of local trust. DA is responsible for the information is: domain entity search, reliability calculations, reliability of storage.
3) MD is the domain.

B. Related definitions

Definition 1 setting X as a system entity domain, $X = \{ x_1, x_2, ..., x_N \}$, $N \in (1, 2, 3, \cdots)$, therein, $x_1, x_2, ..., x_N$ show N entities in the system. In an interactive, each entity may play one of three kinds of roles: Service Requester (SReq), Service Provider (Sp), and Service Recommender (SRec).

Trust is a multidisciplinary concept, which has yet to form a unified definition at present .TCG uses the expected behavior of entities to define credible: an entity is credible, if it always achieve the desired goals by expected behavior way [23]. This paper refer [23-25] the definition about credibility, setting x_i, x_j as any two entities in the system, and $i, j \in N, i \neq j$, after a trade, the definition of evaluating entities whether is credible as follows:

Definition 2 trust: that is a kind of subjective judgment built on the existing knowledge, which is measure based on a timestamp, the service requester, according to the environment about the provision of the specified services of the service provider x_j in accordance with the will of x_i.

In this paper, trust is divided into three types: direct trust, recommended trust and global trust. To direct trust and recommended trust there is a certain degree of subjectivity and one-sidedness, while the global trust can more objectively reflect the overall behavior characteristics of users. Global trust is caluculated from direct trust and recommended trust through a certain method.

Definition 3 direct trust degree: the system entity x_i and entity x_j through direct interactive history and achieve the trust value of the entity x_i, shown by $DT(x_i, x_j)$

Definition 4 recommend trust degree: the system entity x_i achieves the trust value which is comprehensive calculated by direct trust degree of multiple entities acting on the entity x_j, shown by $RT(x_i, x_j)$.

Definition 5 domains of trust: it is a comprehensive trust in a domain which calculated of direct trust degree and recommended trust degree.

Definition 6 global trust degree: It is quantitative expression of trust, refer to comprehensive trust value which synthesizes the direct trust and recommend trust, shown by $T(x_i, x_j)$.

Definition 7 service attributes: before every transaction, the service requester needs to conduct this provider from various sides, such as resource running speed, reliability, easily use etc, which makes a request for various service attributes, and establishes attribute set of resource service, showed by $ATTR = \{attr_1, attr_2, ..., attr_M\}$, and $attr_i$ represents i-kind attribute of the resource provider.

Definition 8 QoS attribute value oneself: the value of QoS which service provider claims according to their ability in t time, showed by $Q_{ATTR}^{x_j} = \{q_{attr_1}^{x_j}, q_{attr_2}^{x_j}, ..., q_{attr_M}^{x_j}\}$, and $0 \le q_{attr_m}^{x_j} \le 1$ represents QoS oneself of m-kind service attribute of the service provider . In order to accurately depict QoS oneself, we suppose that service providers can update QoS attribute value themselves according to their immediate service performance and the feedback of the service requester.

Definition 9 trade QoS satisfaction evaluation: after every trade , for each service attribute, quality index is defined as $\{q_{attr_1}^{x_i,x_j}, q_{attr_2}^{x_i,x_j}, \ldots, q_{attr_M}^{x_i,x_j}\}$, which gets from service provider entity $x_j (x_j \in X)$ providing actual trade to service requester entity $x_i (x_i \in X)$, showed by $Q_{ATTR}^{x_i,x_j} = \{q_{attr_1}^{x_i,x_j}, q_{attr_2}^{x_i,x_j}, \ldots, q_{attr_M}^{x_i,x_j}\}$, and $0 \le q_{attr_m}^{x_i,x_j} \le 1 (m = 1, 2, \ldots..M)$ represents evaluation value of m-kind service attribute from the service requester x_i to the service provider x_j.

Definition 10 Services Evaluation Factor (SEF): each entities have own preference for every service attribute in selecting the service object. Establishing that $\tilde{\omega}_m$ represents importance degree of m-kind service attribute relative to other service evaluate factor, and meets:

$$0 \le \tilde{\omega}_m \le 1, \quad \sum_{m=1}^{M} \tilde{\omega}_m = 1 \tag{1}$$

then $\tilde{\omega}_m$ is called for the evaluate factor of m-kind attribute.

Definition 11 Transaction request vector: it is defined as the five-group , in which id is the entity number; type is the domain for the requested goods; for the entity's self-confidence factor, is the minimum confidence threshold; flag is a flag, 0 or 1.

C. Trading Process

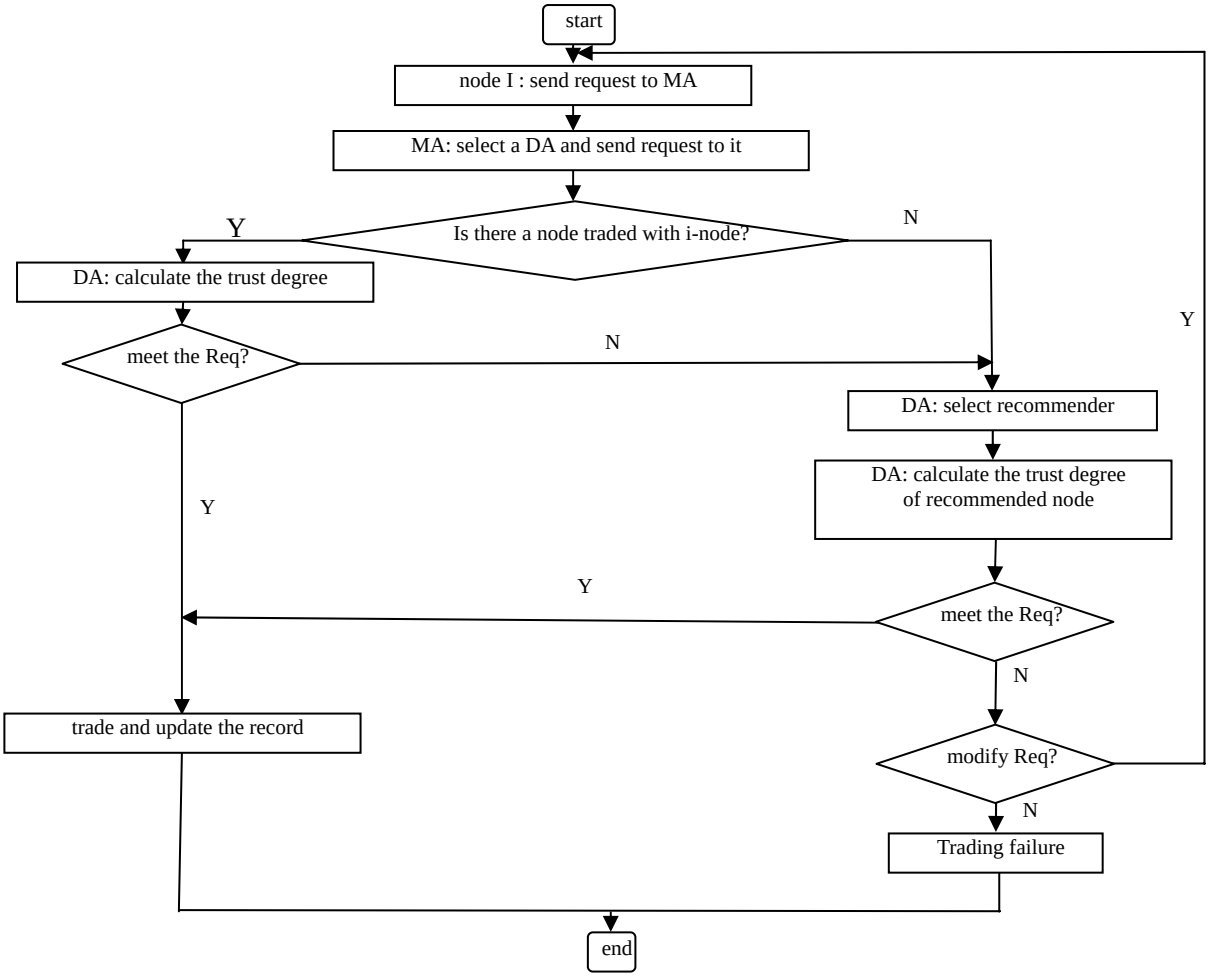

Fig 2. The Process of the trust model

1) Requester send transaction request Req to MA, and then based on the type of Req MA will select DA and sent Req to DA.
2) DA check the entities in its domain, if there are entities traded with requester DA bring up the historical record and calculate the trust degree in accordance with the formula.
3) According to the trust degree set the entities sequence in order, and judge whether the entities meet the trading conditions, if so, trading.
4) If the domain does not meet the trading conditions for all entities or no entities traded before, MA will select entities in other domain.
5) DA calculates the trust degree of the recommended entity.
6) View the flag bit, if it is 1 MA calculate the global

trust degree, else does not calculate.

D. Trust Evaluating of QoS

After the transactions between x_i and x_j, x_i will evaluate the QoS of x_j through the following expression, according to all attributes of service:

$$Q^t_{x_i,x_j} = Q(x_i, x_j, t) = \sum_{m=1}^{M} \tilde{\omega}_m q_m^{x_i,x_j} \tag{2}$$

After the end of a service, calculate the QoS evaluation Difference Degree according to the following equation:

$$D^{Q(xj)}_{Q(xi,xj)} = \frac{\left| Q^t_{x_i,x_j} - Q^{self,t}_{x_j} \right|}{Q^t_{x_i,x_j}} \tag{3}$$

$$V_k(x_i, x_j) = \begin{cases} 1, \text{ when } D^{Q(xj)}_{Q(xi,xj)} \le \varepsilon \\ 0.5, \text{ when } D^{Q(xj)}_{Q(xi,xj)} = null \\ 0, \text{ when } D^{Q(xj)}_{Q(xi,xj)} > \varepsilon \end{cases} \tag{4}$$

The $V_k(x_i, x_j)$ expresses trust evaluation value which be got after the end of the transactions between service requester x_i and service provider x_j, according to the QoS.

E. Trust Calculation

a. Direct Trust Calculation

In the calculation of direct trust introduce the following four factors:

1) the number of transactions: The more that transactions between two entities the higher the degree of mutual trust between entities, can prevent some malicious entity disguised as honest in the beginning of the entity, to a certain reputation in the accumulation of damage after the start.
2) Trading time: from evaluation of current transactions in recent times to better reflect the recent behavior of an entity, so the business from the current time evaluation of the credibility of the more recent impact should be greater.
3) Transaction Amount: evaluation of large transactions credibility of direct impact, so that small transactions can prevent users to access the integrity of large transactions in the deception.
4) Transaction Evaluation: After each transaction, the two sides of the product according to the quality of the transaction, the transaction process is smooth, the product on time and other factors are given in the transfer of the corresponding evaluation {excellent, good, and poor}, the evaluation value in [0,1].

The calculation of direct trust is following the equation (5):

$$DT(x_i, x_j) = \alpha \frac{\sum_{l=1}^{n} \Phi(t_l) \times \Phi(m_l) \times C_l}{n} (n > 0) \tag{5}$$

where $\alpha = \sqrt{n/(n+1)}$ is the function of the number of transactions, $\Phi(t_l) = e^{-\lceil (t_0 - t_l)/T \rceil}$ is the time decay quotient, t_0 is the time of this transaction, t_l is the time of the l times transaction, $\Phi(m_l) = e^{-1/m_l} (m_l > 0)$ is used to adjust the amount of the transaction on the impact of direct trust.

b. Recommended Trust Calculation

To calculate the recommended trust degree, this text shows that the x_i collects the direct trust degree that x_i communicate directly with other entities about x_j in this system. There is the recommended trust degree about x_j:

$$RT(x_i, x_j) = \sum_{k=1}^{N} DT(x_i, x_k) * DT(x_k, x_j) / N \tag{6}$$

N expresses the number of the recommended entities. $DT(x_i, x_k)$ expresses the direct trust degree, the x_i over the x_k, $DT(x_k, x_j)$ expresses the direct trust degree, the x_k over the x_j.Considering the decay of the recommended trust degree, this text uses the direct trust degree $DT(x_i, x_k)$ as the recommended trust degree factor of the x_k,this prevents individual entities to exaggerated or slander when making recommendations.

c. Domain and gloable Trust Calculation

The domain trust is calculated by equation (7):

$$T(X, x_i, x_j) = \lambda DT(x_i, x_j) + (1-\lambda) RT(x_i, x_j) \quad (0 \le \lambda \le 1) \tag{7}$$

It expresses the domain trust of entity in domain T

The global trust is:

$$T(x_i, x_j) = \frac{\sum_{j=1}^{n} T(Y, x_k, x_j)}{n} (T(Y, x_k, x_j) \ne 0, n > 0) \tag{8}$$

IV. SIMULATION

In order to verify the validity of the model, we use the simulation software querycycle simulator[26] developed by the Stanford University. We make simulation experiments for the model based on P2P file sharing network environment with the Windows XP and the JAVA development language.

Simulation Environment:1000 nodes, 50000 files, files are uniform and random distribution in each node. Every node downloads a file which it has not in a simulation cycle. Simulation factors and their values are as the table 1. The value of the simulation cycle is 100, that is every node finish 100 times transactions in a simulation cycle.

TABLE I. SIMULATION FACTORS AND THE VALUES

factor	instruction	initial value
N	node number	1000
N_f	file number	50000
M	service attribute number	6
$q_{attr_1}^{x_j} \sim q_{attr_M}^{x_j}$	service attribute value	Random number in 0~1 and $\sum_{m=1}^{M} q_{attr_m}^{x_j} = 1$
$\tilde{\omega}_1 \sim \tilde{\omega}_M$	QoS value weight factor	Random number in 0~1 and $\sum_{m=1}^{M} \tilde{\omega}_m = 1$
ε	Threshold value	0.05
λ	Direct trust degree Regulators factor	0.6
∂	Historical factor	0.6
Ps	Percentage of sincere Peers	1~0
Pm	Percentage of Malicious Peers	0~1

A. Number of direct transactions impact on trust degree

Supposing ρ =0.6，Fig. 3 shows when the direct trust degree is small, the proportion of the recommendation trust degree is larger, with the increasing of the number of transactions, the impact of the direct trust degree on global trust degree is growing, that is to say, nodes believe their own judgment more and more, this can restrain Malicious Peer' malicious recommended to a certian extent. Also found in human society, with the deepening of communication, people believe heir own judgment more and more.

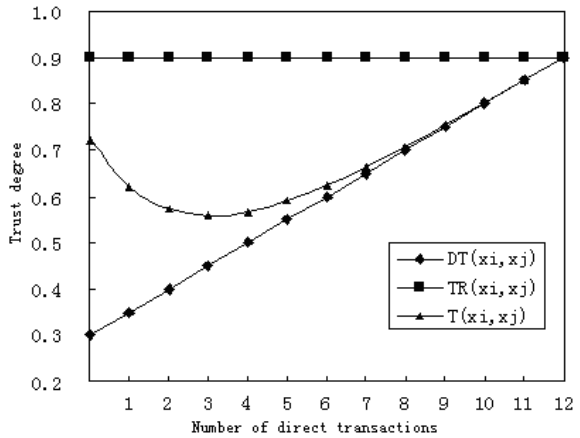

Figure 3 number of direct transactions impact on trust degree

B. MSATrust model restrains Malicious Peer of effective simulation experiment

In order to evaluate MSATrust model contain malicious attacks, in the simulation environment there is four types of nodes:

Sincere Peer: This node always provides other nodes with reliable services, and provides fair evaluation after trading.

Simply Malicious Peer: This node does not provide other nodes reliable service and feedback during trading.

Strategic Malicious Peer: Depending on the different circumstances this nodes with different probabilistic provide reliable service, when credit value is lower than a threshold value, this nodes provide other nodes authentic service for its accumulation of credit value; when credit value is higher than a threshold value, this nodes will provide unreliable service to seek their illegal profits, this nodes make their credit value always maintain in confidence level within the system.

Collusive Malicious Peer: Illegal node combined form malicious gangs, they conspire to slander good nodes and exaggerated the similar nodes, their aim is to deceive other nodes to believe the similar nodes and refuse to trade with legally nodes.

Successful Transaction Rate, that is to say, in this system, the proportion of successful trades in all trades. In order to facilitate comparison, there is achieving the transactions of the Eigen Trust model and No trust model.

a. Simply Malicious Peer

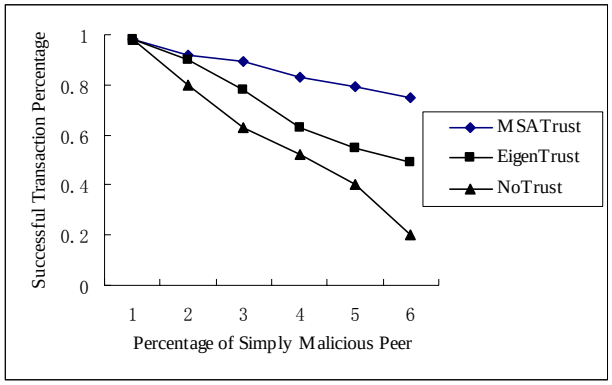

Figure 4. change of Successful Transaction Rate with number of Simply Malicious Peer

We can see from the Fig. 4, when there is no Malicious Peer, the Successful Transaction Rate could reach 100%. But with the increasing of the number of Malicious Peer, the Successful Transaction Rate rapidly descend in the system without No trust model, when the Malicious Peer reach to 50%, the Successful Transaction Rate is just 20%. There is no punishment in the EigenTrust, so the Successful Transaction Rate descends faster. In the MSATrust model, with the increasing of trades, when the Malicious Peer reach to 50%, the Successful Transaction Rate still reach to above 70%, because it can effectively identify and restrain the Malicious Peer.

b. Strategic Malicious Peer

In simulation experiment, when the trust of Strategic Malicious Peer is above 0.6, it offers authentic service with probability of 20%, on the opposite side, it offers authentic service with probability of 60%, the Fig. 4 shows the change of the models when they get attack of Strategic Malicious Peer. We can see from Fig.5, in the EigenTrust, without punishment, the Strategic Malicious Peer make Successful Transaction Rate down rapidly.

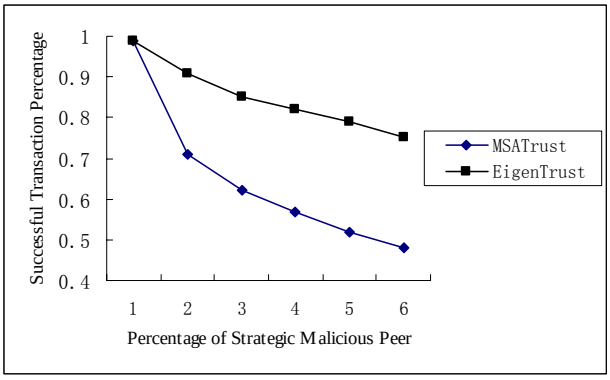

Figure 5 change of Successful Transaction Rate with percentage of Strategic Malicious Peer

c. Collusive Malicious Peer

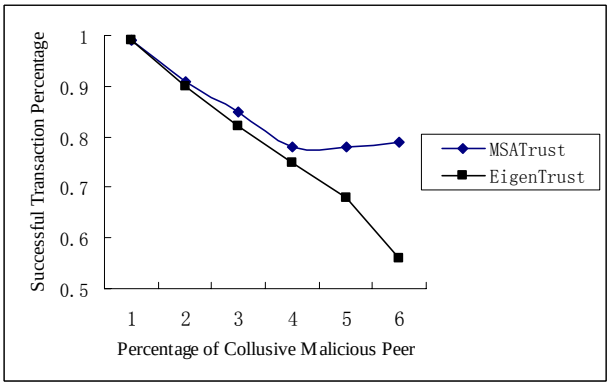

Figure 6 change of Successful Transaction Rate with number of Collusive Malicious Peer

Fig. 6 makes a comparison about Successful Transaction Rate between the EigenTrust and MSATrust under the condition of Collusive Malicious Peer. In simulation experiment, they conspire to slander good nodes and exaggerated the similar nodes, they provide good nodes unreliable service and credible service for similar nodes. Due to EigenTrust model made against cheating conspiracy, therefore, with the increase of the proportion of such node, malicious node exaggerate credibility with each other. They attract large of trades but no identification of the malicious peer, this makes the Successful Transaction Rate of system down. The MSATrust is similar to the EigenTrust，the Successful Transaction Rate falls down at the beginning, with the increasing of the number of transactions, the impact of the direct trust degree on global trust degree is growing, that is to say, nodes believe their own judgment more and more, this can restrain Malicious Peer' malicious recommended to a certain extent. Thus, the Successful Transaction Rate rise instead, this shows the robustness of the model against malicious attacks.

The result of the simulation experiment shows the MSATrust can effectively building trust relationship between nodes, the system with large scale malicious node can still provide higher success rate.

V. CONCLUSION

Based on entities characteristics of their services, we abstract representative multi-service attributes from trust relationships to represent a trust evaluation model. The service requester based on their own preferences of service to evaluate the multi-service properties of service provider, combined with the trust value that determines whether the transaction doing; closing of the transaction, the service requester based on the actual quality of services received and service claimed by the provider to calculate the Quality of Service different degrees, to judge the credibility of service providers, and the corresponding rewards and punishments and trust updates. Simulation results show that the model can more accurately assess the entity's trust, can effectively curb the types of malicious attacks entities when a higher proportion of malicious entities can still maintain a relatively high rate of successful transactions.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China (60873203), Natural Science Foundation of Hebei Province (F2010000313).

REFERENCES

[1] Zhang Qian, Sun Yu, Liu Zheng, Zhang Xia, Wen Xuezhi. Design of a distributed P2P-based grid content management architecture. Proceedings of the 3rd Annual Communication Networks and Services Research Conference, 2005:339-344

[2] Hu Ning, Zou Peng, Zhu Pei-Dong. Reputation-Based Collaborative Management Method for Inter-Domain Routing Security. Journal of Software[J]，2010，21（3）：505-515

[3] Song Shanshan, Hwang Kai, Kwok Yu-Kwork. Trusted Grid computing with security binding and trust integration. Journal of Grid computing[J], 2005,3(1):53-73

[4] Audun J, Roslan I, Colin B. A survey of trust and reputation systems for online service provision. Decision Support Systems, 2007.43(2):618-644

[5] Hong Zhong，Haixin Duan，Wu Liu. RRM：A kind of incentive mechanism of trust model [J]. Science China Press.2008，38(10):1747-1759

[6] Xiaoyong Li,Xiaolin Gui. Trust Quantitative Model with Multiple Decision Factors in Trusted Network[J]. CHINESE JOURNAL OF COMPUTERS,2009,32(3):405-416

[7] Runlian Zhang,Xiaonian Wu,Shengyuan Zhou,Xiaoshe Dong. A Trust Model Based on Behaviors Risk Evaluation [J]. CHINESE JOURNAL OF COMPUTERS,2009,32(4): 688-698

[8] M. Blaze, J. Feigenbaum and J. Lacy. Decentralized trust management. In Proceedings of the 17th Symposium on Security and Privacy, 1996: 164-173

[9] Kamvar SD, Schlosser MT. EigenRep: Reputation management in P2P networks. In: Lawrence S, ed. Proc. of the 12th Int'l World Wide Web Conf. Budapest: ACM Press, 2003,,123~134.

[10] ZHOU RUNFANG,KAI H.PowerTrust:A robust and scalable reputation system for trusted peer-to-peer computing[J].IEEE Transactions on Parallel and Distributed Systems,2007,18(4):460-473.

[11] Xiong L and Liu L. A Reputation-Based Trust Model for Peer-to-Peer Ecommerce Communities[C], Proceedings of IEEE International Conference on Electronic Commerce, New York,2003, 228-229.

[12] Xiong L, Liu L. PeerTrust:Supporting reputation-based trust for peer-to-peer electronic communities[C], IEEE Transactions on Knowledge and Data Engineering, 2004,16(7), 843-857.

[13] Asnar Y, Giorgini P, Massacci F, et al. From trust to dependability through risk analysis. DIT-University of Trento : Technical Report DIT-06-079 , 2006

[14] Y. Wang, V. Varadharajan. Role-based recommendation and trust evaluation. The 9th IEEE International Conference on E-Commerce. Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services(CEC-EEE 2007). July 2007: 278-288.

[15] TIAN Chun-qi1, ZOU Shi-hong2, WANG Wen-dong2, CHENG Shi-duan2, Trust model based on reputation for peer-to-peer networks. Journal on Communications, 2008,29(4):63-70

[16] Tien Tuan Anh Dinh, Tom Chothia, Mark Ryan. A Trusted Infrastructure for P2P-Based Marketplaces. The 9th International Conference on Peer-to-Peer Computing. Seattle, USA, 2009:151-154

[17] A. Jøsang. Conditional Reasoning with Subjective Logic. Journal of Multiple-Valued Logic and Soft Computing, 2008,14(2–3):155–185

[18] A. Jøsang. Cumulative and Averaging Unfusion of Beliefs. The Proceedings of the International Conference on Information Processing and Management of Uncertainty (IPMU2008), Malaga, June 2008.

[19] A. Jøsang and Haller J. Dirichlet Reputation Systems. In In the Proceedings of the International Conference on Availability, Reliability and Security (ARES 2007), Vienna, Austria, April 2007.

[20] Jianxin Li,Jinpeng Huai,Xianxian Li. DTM:A Dynamic Trust Management Model for Internet Computing Environments[J]. CHINESE JOURNAL OF COMPUTERS,2009,32(3): 493-505

[21] Xiaoyong Li, Xiaolin Gui. Research on Dynamic Trust Model for Large Scale Distributed Environment[J]. JOURNAL OF SOFTWARE, 2007,18(4):460-473

[22] Yongjun Li, Yafei Dai. Research on Trust Mechanism for Peer-to-Peer Network[J]. CHINESE JOURNAL OF COMPUTERS，2010,33(3):390-405

[23] Trusted Computing Group. https: //www. Trustedcom putinggroup. org /

[24] Audun J, Roslan I, Colin B. A survey of trust and reputation systems for online service provision. Decision Support Systems,2007,43(2):618-644

[25] Artz D, Gil Y. A survey of trust in computer science and the semantic Web. Web Semantics,2007,5(2):58-71

[26] Stanford P2P Sociology Project，http://p2p.stanford. edu /www/download.htm

Ruizhong Du, born in 1975, master and associate professor. His main research interests include network technology and trusted computing

.

Xiaoxue Ma, born in 1974, master and associate professor. Her main research interests include network technology and trusted computing.