Trust Management in Peer-to-Peer Networks

Zhen Yu, Jie Zhu, Guicheng Shen
School of Information, Beijing Wuzi University, Beijing, China
Email: yuzhenhappy@163.com

Haiyan Liu
Department of Computer Engineering, Beijing Information Technology College, Beijing, China
Email: 48801343@qq.com

***Abstract*—In recent years, various applications of Peer-to-Peer (P2P) computing have been widely used because of its unique advantages, which have played an important role in commerce, communications and other fields. The P2P system is essentially a distributed system, without central servers. Each peer is both client and server, who have the same status. However, some features of P2P networks, such as autonomy, dynamic, and heterogeneity lead to an important problem, namely unreliable quality of service. Unreliable quality of service is usually presented as providing false or unreliable service, impacting customer satisfaction. The establishment of trust models which evaluates capabilities of peers can measure the service capacity of a peer, and identify malicious behavior, thereby reducing the risk of interaction and being an effective technique to ensure the overall availability of P2P networks. A trust model named METrust in P2P networks based on the recommendation is proposed. In METrust, a peer selects recommendation peers whose evaluation criteria are similar, and evaluation criteria of peers are determined through the AHP method (Analytic Hierarchy Process). Each peer in the network has a unique credibility of recommendation, and two trust parameters for updating the credibility of recommendation are introduced, namely updating range and updating strength. METrust proposes algorithms to compute the trust of peers. Simulations show that, the trust model METrust can identify malicious peers, and improve the quality of service in P2P networks effectively.**

***Index Terms*—Peer-to-Peer; trust; recommendation; evaluation criteria**

I. INTRODUCTION

In recent years, P2P (Peer-to-Peer) technologies [1] have been widely used in the vast field for its unique advantages, for example, file sharing, collaboration, instant messaging, communication, e-commerce systems, etc. P2P overlay networks can be divided into structured systems, unstructured systems and other systems with new structures to improve the efficiency of searching in the P2P network [2, 3]. P2P technologies allow people to interact with each other directly via the Internet, which makes it easier to communicate on the network. However, some disadvantages of P2P systems, such as anonymity, autonomy, and other characteristics have also led to some security issues affecting the quality of service of P2P networks. For example, some users suffered because of the malicious deception from illegal seller and no longer do online shopping; online bank accounts of some users were stolen and suffered heavy losses; some users cannot buy desirable commodity due to the lack of experience. Some researches on the trust model [4-6] in P2P systems show that using trust model can identify malicious peers effectively. Trust models can measure the credibility of the peer in various aspects, which has significance in improving the quality of service in P2P systems.

Trust models have been widely used in e-commerce, distributed computing, recommender systems [5]. Trust models compute the trust value in the peer mainly through the quantitative evaluation system, to forecast the capability of providing service in this peer. A peer's trust value can be the gist of other peers to decide whether they will get service from this peer, and after interactions other peers can update their opinions on the peer providing the service, such as eBay. Currently trust models based on recommendation [6-9] in P2P systems mainly compute the trust value of the service provider from its own interactive experience and recommendations from other peers. Some characteristics of P2P network such as heterogeneity, autonomy increase the complexity of the trust evaluation, and some researches [5, 6, 7, 9] put forward their trust models to solve certain security problems. However, trust evaluations in these trust models don't consider this condition refers to different preferences exist in different peers. Different peers getting the same service from the same peer will have different views to the peer providing the service who will receive unfair judges, which impacts the quality of service in P2P network.

To be able to get recommendation effectively, this paper proposes a trust model based on recommendation in P2P networks. In the trust model each peer has a unique credibility of recommendation. Experiments and simulation results show that the trust model proposed in this paper can identify malicious peers in P2P networks, and can improve the quality of service effectively.

The rest of this paper is organized as follows: section Ⅱ discusses related work on trust models. Section Ⅲ introduces our trust model based on preference and algorithms for computing the trust value. Simulation-based experiments are showed in section Ⅳ. In the last section, we present conclusions.

doi:10.4304/jsw.9.5.1062-1070

II. Related Work

Recommendation-based trust models are now widely used in business companies like eBay [10] and the Amazon [11]. According to the different calculation methods it can be classified into two kinds of models: global trust models and local trust models [12]. In global trust models, a peer can gain other peers' credibility from a view of the network that is wider than his own experience; while in local trust model, a peer gets other peers' credibility by querying some peers providing recommendation. EigenTrust [6] assigns each peer a unique global trust value based on the peer's history of uploads, and presents a distributed and secure method to compute global trust values based on power iteration. But EigenTrust suffers a flaw that it has some pre-trusted peers which are difficult to predefine a default collection of fixed sub-trusted peer in practice. The basic idea of Dou [9] is similar to EigenTrust, but without using pre-trusted peers. Dou's model reduces iteration cost and punishes malicious behavior, but doesn't consider the punishment to dishonest recommendation peers. The paper [9] cancels that default peer set and brings punishment rules for some bad behavior, in this way it reduced the iteration overhead, however, it did not take the difference between peer evaluations into consideration and didn't punish any dishonest recommending peer. Based on the global trust value, SWRTrust [13] added the similar factor of peer scoring behavior to express the peers' recommendation ability, keeps down peers' joint fraud behavior to some extent. SWRTrust computes the global trust value using the similarity of evaluation behavior, but doesn't consider the difference of preferences between two peers. The paper [14] gives a multi-granularity trust model. The paper [15] considers the peer's direct experience and other peers' recommendation together and calculate them with weighted average method, it would brings unfair because it's difficult to determine each peer's weight, which affects the judge of service quality. The paper [16] proposed a trust model aimed to malicious recommendation, the evaluation aimed at the documents provided by the service peer. The paper [17] defined suspicious trading to identify the false feedback. The paper [18] proposed a trust model which is based on probability statistics. The paper [19] evaluated the recommendation trust vector using two-stage fuzzy comprehensive evaluation of fuzzy theory in P2P networks. In local trust model, the Bayesian network-based trust model [7] believes that trust is multi-faceted and peers need to develop differentiated trust in different aspects of other peers' capability. But in this model, the way of computing the credibility of recommendation peer is based on user's subjective view which is unilateral. PeerTrust [8] brings more trust evaluation factors, construct trust from many angles but it also brings high calculation cost. In paper [20], a peer classification method based on the thought of maximal tree is proposed, which can effectively classify recommendation peers according to their trusted level. AgentTMS is proposed in paper [21] to improve the traditional trust models based on Agent's reputation and activity by leveraging the agent social relationships.

III. Trust Model in P2P Networks

In P2P network, each peer not only can provide services, but also can obtain services, besides they also can give recommendation of some peers. This paper takes the P2P file-sharing network as an example, and describes the trust relation.

A. Definition of Evaluation Criteria

Inconsistency of peer evaluation criteria will lead to unfair assessment of the service provider, the trust model proposed in this paper take evaluation criteria differences into consideration to solve this problem. Peers need to determine their own evaluation criteria, and provide to the other peers as the interaction reference. The evaluation criteria of the peer weights are realized with n-tuple.

Preferences of various peers in P2P network are different and evaluation criteria in service are also inconsistent. Declaration of preference is proposed in this paper to help interactions. However, weights of preferences of peers are difficult to assign with accuracy sometimes because of some subjective factors. To improve the accuracy in assigning weights of preference for each peer, the Analytic Hierarchy Process (AHP) [22] is used in this paper.

The AHP is a structured technique for helping people deal with complex decisions. Rather than prescribing a "correct" decision, the AHP helps people to determine one. An AHP hierarchy is a structured means of describing the problem at hand. It consists of an overall goal, a group of options or alternatives for reaching the goal, and a group of factors or criteria that relate the alternatives to the goal. The AHP hierarchy for preference is showed in Fig. 1.

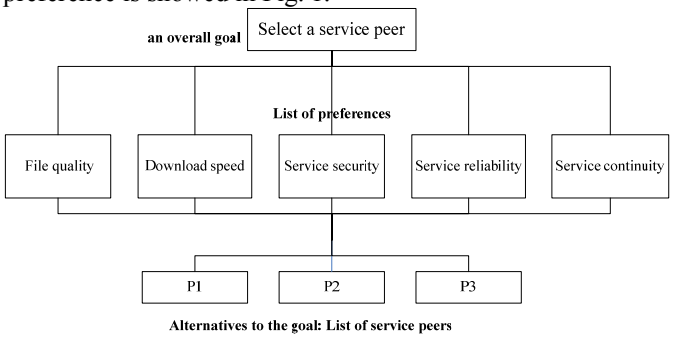

Figure 1. The AHP hierarchy for preference

Definition 1. Declaration of preference: after computation by AHP, each peer has a N-tuple for weights of his preference which will be declared in P2P network: $(W_{i1}, W_{i2}, \cdots W_{in})$, $W_{im} \in [0,1]$, $m \in [1,n]$, $\sum_{m=1}^{n} W_{im} = 1$, Where i represents the peer ID; n represents the total number of preference categories in P2P network; W_{im} represents the weight that peer i places in the m^{th}

preference. A peer can declare his weights in accordance with his preference freely.

B. Trust Computation

In Peer-to-Peer (P2P) networks, each peer can be used as the service provider and the visitor, and also can provide recommendations at the same time.

Generally, the trust computation in P2P networks is as follows, which was also referred in other paper [23]:

$$T_{ij} = \lambda \times D_{ij} + (1-\lambda) \times r_{ij}, \quad \lambda \in [0,1] \qquad (1)$$

T_{ij} denotes the total evaluation of the capability of providing service in the peer j from peer i's view; D_{ij} denotes peer i's direct experience of interactions with peer j; r_{ij} denotes the recommendation from corresponding recommendation peers; λ is the weight to indicate how the peer i values the importance of his own experiences and other recommendations. The trust model in P2P systems uses the formula (1) to compute the trust value.

Definition 2. The degree of satisfaction with an interaction: $S_{ij} = \sum_{n} W_{in} S_{ijn}$, where S_{ij} represents the total degree of the satisfaction that peer i places in the interaction with peer j; S_{ijn} represents the part degree of the satisfaction in the n^{th} preference that peer i places in the interaction with peer j. If $S_{ij} \geq \alpha$, the interaction can be considered successful, else failing, α represents the threshold of the degree of satisfaction, $\alpha \in [0,1]$.

Definition 3. The similarity of preferences between peer i and peer j: $Sim_{ij} = \dfrac{\sum_{m=1}^{n} W_{im} \times W_{jm}}{\sqrt{\sum_{m=1}^{n} W_{im}^{\ 2}} \times \sqrt{\sum_{m=1}^{n} W_{jm}^{\ 2}}}$, where uses a function based on cosine similarity to describe the degree of similarity between two peers comparing difference of peers' weights.

Definition 4. The direct trust can be computed as follows:

$$D_{ij} = \frac{G_{ij}}{G_{ij} + B_{ij}} \qquad (2)$$

where G_{ij} represents the number of successful interactions with peer j from peer i's view, B_{ij} represents the number of failing interactions with peer j from peer i's view, D_{ij} represents the summary of peer i from the direct interactions with peer j and reflects the view that peer i places on peer j directly. If there is no direct interactions between two peers, G_{ij}, B_{ij} will be 0, and D_{ij} will be 0.

Definition 5. The recommendation trust value for peer j can be computed using equation below:

$$r_{ij} = \frac{1}{\sum_{r \in I(j)} Sim_{ir}} \sum_{r \in I(j)} D_{rj} \times R_r \times Sim_{ir} \qquad (3)$$

where $I(j)$ represents the set of peers which have bought commodities from peer j which can provide recommendations for service peer j, D_{rj} represents the direct trust value that peer r places on peer j which is came from peer r's direct experience of interactions with peer j, R_r represents the credibility of recommendation of peer r to measure whether peer r can provide a credible recommendation which has a global value in P2P network. If $\sum_{r \in I(j)} (R_r \times Sim_{ir}) = 0$, then $r_{ij} = 0$, which represents there is no recommendation available.

Definition 6. The updating ranges of peer i:

$$U_c^i = \sqrt{2}^{\,5(c-Max_c)/Max_c}, \quad U_c^i \in (0,1] \qquad (4)$$

After interactions, peers need to update the recommendation credibility of the other recommended peer. The model proposed in the paper determines the update range based on the current number of interactions, the update range has slow growth with the increase of the interactive experience. c represents the current number of interactions.

Definition 7. The updating strength of peer i:

Aiming at service provider S, visitor i update the updating strength of recommend peer after success transaction:

$$P_i^s = \frac{\sum_{k \in I(s)} G_{ks}}{\sum_{k \in I(s)} G_{ks} + \sum_{k \in I(s)} B_{ks}} \times R_i \qquad (5)$$

Aiming at service provider S, visitor i update the updating strength of recommend peer after success transaction:

$$P_i^s = \frac{\sum_{k \in I(s)} B_{ks}}{\sum_{k \in I(s)} G_{ks} + \sum_{k \in I(s)} B_{ks}} \times R_i \qquad (6)$$

C. Algorithm to Update the Credibility of Recommendation

Each peer in the trust model METrust has the unique credibility of recommendation, reflecting the credibility of a peer in the P2P system, and embodying the peers' "reputation" in providing recommendation. In the trust model, malicious peer can be identified by updating credibility of recommendation, which can ensure the security of P2P systems. Firstly, we give some related primitives and corresponding semantics as below:

$I(i)$: set of peers who have transactions from peer i;

GetVal (ID_r, D_{rj}, R_r): Get D_{rj} for peer j and get the corresponding R_r ;

CalSim (ID_i , ID_r , Sim_{ir}): Get weights of recommendation peer *r* for peer *j* and compute Sim_{ir} according to Definition 3;

CalDiff(ID_i , ID_r , D_{ij} , D_{rj} , Sim_{ir}): Compute the evaluation difference of peer *i* and peer *r*;

CalFactor(U_c^i , P_i^j): compute the updating range and updating strength of visitor *i* to and recommend peers of service provider *j*;

CalRecm($diff_{ir}^j$, θ , R_r): compare $diff_{ir}^j$ and θ ,and update R_r .

1）The trust evaluation algorithm that Peer *i* compute the totol turst of response peer *j* is as follows:

Procedure ComputeTrust(ID_i , ID_j)

GetDirectTrust(ID_i , ID_j , D_{ij});

GetRecmTrust(ID_i , ID_j , r_{ij} , CalRecmTrust);

GetTrustVal(ID_i , ID_j , D_{ij} , r_{ij} , T_{ij});

End

Procedure CalRecmTrust(ID_i , ID_j , r_{ij})

for (any $r \in I(j)$!= i)

GetVal(ID_r , D_{rj} , R_r);

CalSim(ID_i , ID_r , Sim_{ir});

endfor

$$r_{ij} = \frac{1}{\sum_{r \in I(j)} Sim_{ir}} \sum_{r \in I(j)} D_{rj} \times R_r \times Sim_{ir} ;$$

End

With the algorithm, peer *i* can compute the total turst value of all response peers.

2）After calculation, peer *i* take the interaction with responder peer *j* with the maximum trust value and need to perform the evaluation process, evaluation and update algorithm is as follows:

Procedure EvalDown(ID_i , ID_j)

Download(ID_i , ID_j);

if (Download(ID_i , ID_j)=good) then

$G_{ij} = G_{ij} + 1$;

else

$B_{ij} = B_{ij} + 1$;

endif

UpdateLocal(ID_i , ID_j , S_{ij} , G_{ij} , B_{ij} , $B(i)$);

UpdateRecommend(ID_i , ID_j , S_{ij} , G_{ij} , B_{ij} , $A(j)$);

UpdateRecmTrust(ID_i , ID_j);

End

3）The algorithm which vistor *i* update credibility of recommendation of recommended peers of the service provider *j* is as follows:

Procedure UpdateRecmTrust(ID_i , ID_j)

for (any $r \in I(j)$!= *i*)

GetVal(ID_r , D_{rj} , R_r);

CalSim(ID_i , ID_r , Sim_{ir});

CalDiff(ID_i , ID_r , D_{ij} , D_{rj} , Sim_{ir});

CalFactor(U_c , P_i^j);

With probability P_i^j , CalRecm($diff_{ir}^j$, θ , R_r);

endfor

End

Each peer of METrust trust model in the network has only credibility of recommendation, which is the comprehensive result of previous recommendations regardless of the ability of providing services. Peers consider criteria differences between themselves and recommend peers when selecting recommendations. The algorithm to update the credibility of recommendation in METrust trust model can identify malicious recommend peer effectively.

Procedure UpdateRecmTrust(ID_i , ID_j)

for (any $r \in I(j)$!= *i*)

GetVal(ID_r , D_{rj} , R_r);

CalSim(ID_i , ID_r , Sim_{ir});

CalDiff(ID_i , ID_r , D_{ij} , D_{rj} , Sim_{ir});

CalFactor(U_c^i , P_i^j);

With probability P_i^j , CalRecm($diff_{ir}^j$, θ , R_r);

endfor

End

IV. SIMULATION AND RESULTS

A. Simulation Environment

In this paper, the query cycle model [24, 25] is used as the simulator, which constructs a P2P system. Each simulation consists of some simulation cycles. In each simulation cycle, the peer in the system can initiate transaction queries and response to queries; queries are broadcast like Gnutella, via TTL control the size of the query. Peers initiating the query will wait to receive responses and select the peer with the highest trust value

from the response list to complete the transaction. In the simulation, peers in the system are divided into two categories: good peers and malicious peers, good peers provide reliable services, and malicious peers provide unreliable services, and have reputation speculation behavior [26]. Basic settings that apply for the experiments are summarized in Table I.

Simulation realized EigenTrust model, PeerTrust model used PSM algorithm, and the model proposed in this paper called METrust, and Random model.

1) EigenTrust model is a global trust model, computing the trust using the global credibility.

2) PeerTrust model is a local trust model Based on PSM algorithm. The same responding peers have different trust value for different peers.

3) METrust trust model is a local trust model. Peer in the network has a unique credibility of recommendation. Each peer determines the extent of adoption of recommended peers according to the difference of the evaluation criteria, and update recommended credibility after the interaction.

4) In random model peer randomly select the service peer for download.

The criterion of effects in our experiments is the success ratio of transactions, which is the percentage of the number of successful transactions versus the number of total downloads in a query cycle.

1) Simple malicious peer (IM): responding to queries actively and providing false services;

2) Malicious peer group (CM): malicious peers form a group to carry out joint fraud. Peers in this class have the function as IM class, and also exaggerate the members of the same group and denigrate other good peers;

3) Swing peer group (DM class): In addition to constitute CM class, the malicious peer can provide other peers with trusted transactions and normal feedback by probability f in order to accumulate trust to do some malicious acts;

4) Camouflage peer group (EM class): In addition to constitute CM class, some malicious peers in EM class acts as good peers so as to get high credibility of recommendation, and give high trust to other malicious peers in CM class.

TABLE I.
SIMULATION SETTINGS

Network	topology		Power-law
	total number of peers		100
	proportion of malicious peer		[0-50%]
	minimum number of neighbors		3
	TTL		4
Service	evaluation criteria		download speeds
			document quality
Peer	good peer	Active	100%
		Queries	100%
		Responds	match
		Request	random
	malicious peer	Active	100%
		Queries	100%
		Responds	Malicious
		Request	random
Content	content categories		20
	content distribution		Zipf
	file distribution in content		random
Simulation	query cycles		500

B. *Peers of IM Class*

Firstly, the credibility of recommendation of each peer with existing IM class peers is showed in Figure 2. As can be seen from Figure 2, because IM class peers provide honest recommendation, the credibility of recommendation of each peer does not reduce in METrust model.

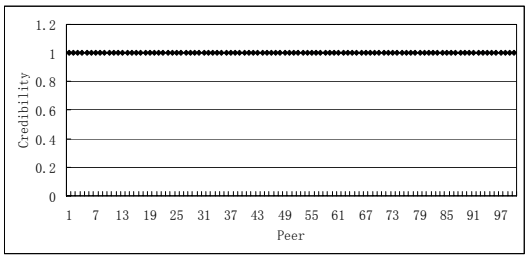

Figure 2. Credibility of recommendation of IM peers

Then the changing trend is given that incredible downloads of IM class peers over cycles of four models with 20% malicious peers. Incredible downloads of four models are declining slowly with increasing interaction cycles and approach a stable value. The incredible download of random model is the highest than other. The incredible download of EigenTrust model untrusted is higher than METrust model and PeerTrust model. The trend between METrust and PeerTrust is little differences. The incredible download number of METrust is slightly below PeerTrust model.

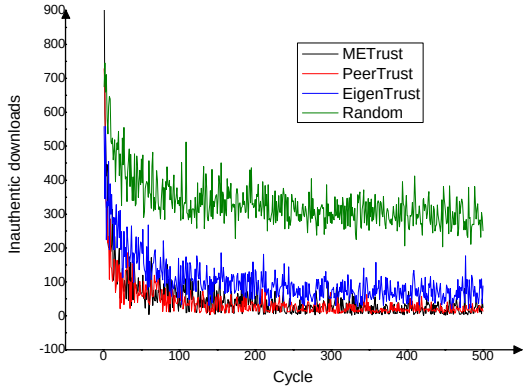

Figure 3. Inauthentic downloads of IM class peers

In the case of the presence of different scale IM class malicious peers, download success rates of four models are compared. Proportions of malicious peers in all peers are 0%, 10%, 20%, 30%, 40%, 50%. As Showed in Figure 4, METrust model, PeerTrust model and EigenTrust model are better than the Random model and can inhibit the IM class malicious peers. In Random model, the download success rate is reducing with increasing proportions of malicious peers. METrust model with IM class peers in network is little difference with PeerTrust model, and download success rates of these two models have a decreasing trend with increasing proportions of malicious peers. EigenTrust model have a certain number of high trusted peers, however this assumption in practice is unreasonable and difficult to operate, with the increasing proportions of malicious peers, and high trusted peers play the more important role, so that when the malicious peer reach the ratio of 30% and 40%, EigenTrust model is also able to achieve the higher download success rate. When malicious peers reach the half of all peers, that's 50% of the system, download success ratios of three models are all low. METrust model and PeerTrust model have little difference when IM class malicious peer exists, but METrust model has obvious advantages compared to other trust models when there are few more cunning malicious peers will be discussed below.

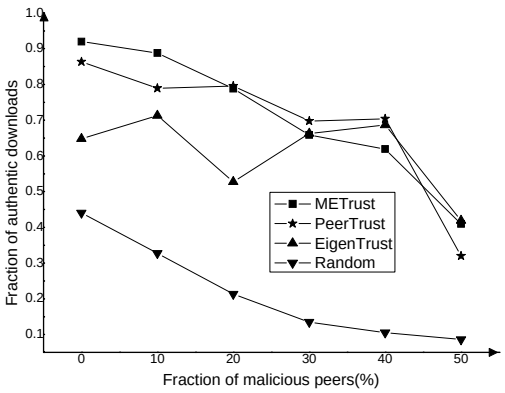

Figure 4. Download success rate of IM peers

In Figures 5, we compare the load of each peers in four models when the proportion of malicious peers is 40%, i.e. the number that providing unreliable service as a service peer. In all 100 peers, peer 1 to peer 60 are good peers in Figure 5, and peer 60 to peer 100 are peers in the IM class, and EigenTrust model selected peer 56 to peer 60 as high-trusted peers. As can be seen from Figure 5, IM class peers don't provide reliable services, and they will not become download sources, so the number of providing reliable services is 0. But In EigenTrust model, when malicious peers reach a certain size, the number of providing services from high trusted peer 56-peer 60 is far higher than normal peers. As In EigenTrust model, there are a certain number of pre-high trusted peers which cumulate their trust with increased interaction cycles and play a more and more important role in the interaction with the increasing scale of malicious peers. The more malicious peers and the less good peers exist in networks, the more dependence of high trust collective will happen, which cannot achieve the load balancing; the download success ratio of EigenTrust model is strongly dependent on high trust peers, which might make high trusted peer overload. While there aren't global trust values in METrust model and PeerTrust model, each peer selects the service peer based on their own preferences, and different peers will select different service peers due to their different evaluation criteria, which will not bring peer overload.

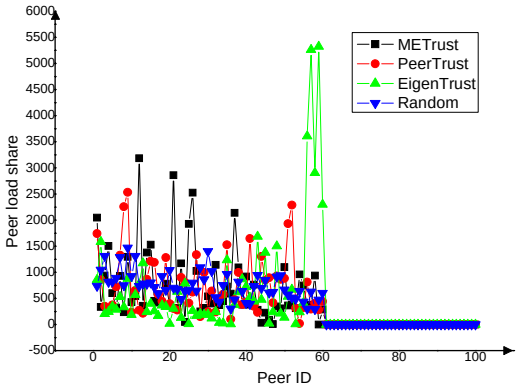

Figure 5. Peer load of IM peers

C. *Peers of CM Class*

Firstly, the credibility of recommendation of each peer with existing IM class peers is showed in Figure 6. As can be seen from Figure 6, in all 100 peers, peer 1 to peer 90 are good peers, and peer 91 to peer 100 are malicious peers, 50% among malicious peers(peer93、96、97、99、100)consist the CM class, and the remainder is IM class peers. In Figure 6, the credibility of recommendation of CM class peers is a bit low; while that's of other peers providing honest recommendation have no significant change.

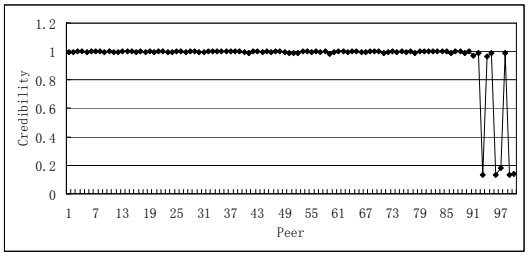

Figure 6. Credibility of recommendation of CM peers

Then the changing trend is given that incredible downloads of CM class peers over cycles of four models with 20% malicious peers. As can be seen from Figure 7, the trend is similar to the Figure 3, and not goes into details here.

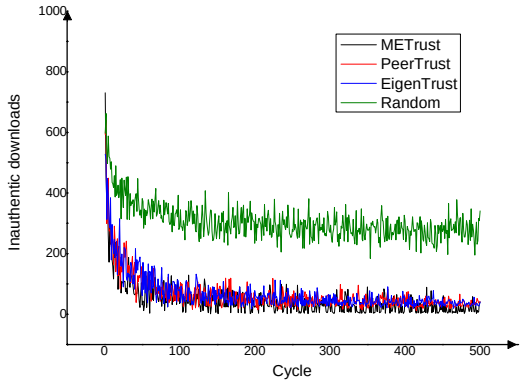

Figure 7. Inauthentic downloads of CM class peers

In the case of the presence of different scale CM class malicious peers, the download success rates of four models are compared. Proportions of malicious peers in all peers are 0%, 10%, 20%, 30%, 40%, 50%. As Showed in Figure 8, EigenTrust model has no action to CM class peers, and malicious peers in CM class will be easier to obtain higher credibility with the increasing of CM class peers; and EigenTrust model does not have punishment mechanism on this kind of false recommendation which causing good peer download success rates decrease significantly. PeerTrust model has little difference with EigenTrust model with CM class peers existing. METrust model can judge false recommendation and CM class malicious peers can be identified, so the result is better. In most cases, METrust model is superior to PeerTrust model and EigenTrust model, when the proportion of malicious peers reaches 30%, download success rates of good peers can reach more than 75%.

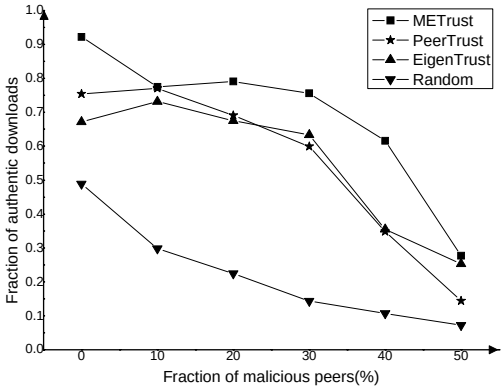

Figure 8. Download success rate of CM peers

With 40% malicious peers, loads of each peer in the four models are showed in Figure 9. The condition is similar to the above situation with IM class peers, and not repeats them here.

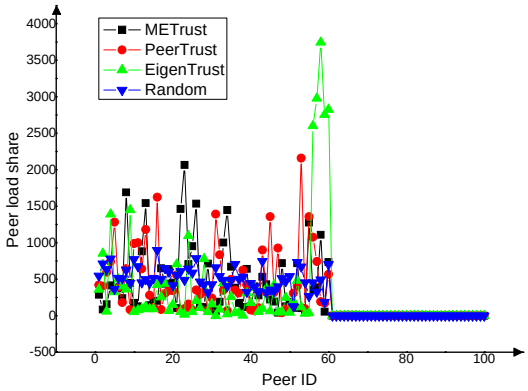

Figure 9. Peer load of CM peers

D. *Peers of DM Class*

Then Figure 10 shows success ratios when the probability f changing from 0 to 0.8 with 30% malicious peers. METrust, proposed in this paper, is superior to other trust models, which can deal with DM class peers.

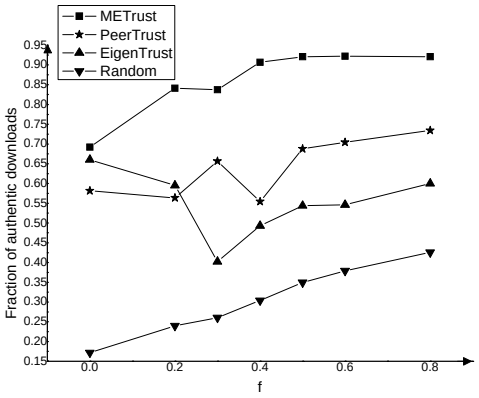

Figure 10. Download success rate of DM peers

E. Peers of EM Class

Firstly, the credibility of recommendation of each peer is showed in Figure 11. The number of peers is 100, and 1-80 acts as good peers, the other acts as malicious peers. 50% of malicious peers, that's 85,86,87,89,91,94,95, 96, and 98,100, compose EM class peers, and others are IM class peers. Figure 11 shows that the trust model can identify EM class peers.

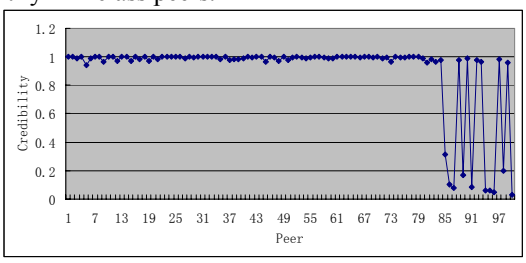

Figure 11. Credibility of recommendation of EM peers

Then Figure 12 compares success rates of four trust models with 30% malicious peers when the proportion of EM class peers changing from 0% to 50%. As showed in Figure 12, METrust, the trust model proposed in this paper, can better control this kind of malicious behavior.

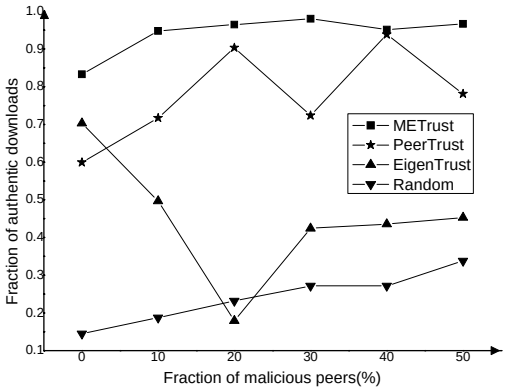

Figure 12. Download success rate of EM peers

V. CONCLUSION

This paper presents a trust model in Peer-to-peer networks. Each peer in the system has a unique credibility of recommendation. Analysis and simulation show that the trust model can evaluate the peer's trust value with the smaller overhead, and identify malicious peers in P2P networks, which improve the quality of service in P2P networks effectively.

ACKNOWLEDGMENT

The research is sponsored by Beijing key Laboratory of Intelligent Logistics System (NO: BZ0211), Beijing Wuzi University. This paper is supported by six projects including: Youth Research Funding Project of Beijing Wuzi University (2011XJQN003), Project for Beijing University Logistics Technology Engineering Research Center(BJLE2010), Funding Project for Academic Human Resources Development in Institutions of Higher Learning Under the Jurisdiction of Beijing Municipality(PHR200906210), Funding Project for Base Construction of Scientific Research of Beijing Municipal Commission of Education, Funding Project for Science and Technology Program of Beijing Municipal Commission of Education Under the grant number (KM200910037002), Special Funding Project for Education Quality Improvement of Beijing Wuzi University.

REFERENCES

[1] A Oram. Peer-to-Peer: Harnessing the Power of Disruptive Technologies [M]. USA: O'Reilly and Associates, 2001.

[2] Chen ZG, Liu JQ, Li D, Liu H. SOBIE: a novel supernode P2P overlay based on information exchange [J]. Journal of computers, 2009, 4 (9): 853-861.

[3] Meng FB, Ding L, Peng S, Yue GX. A P2P Network Model Based on Hierarchical Interest Clustering Algorithm [J]. Journal of software, 2013, 8 (5): 1262-1267.

[4] K Aberer, Z Despotovic. Managing Trust in a Peer-to-Peer Information System [A]. Proc.ACM Conf. Information and Knowledge Management (CIKM) [C]. USA: ACM Press, 2001. 310-317.

[5] F Cornelli, E Damiani, S D C di Vimercati, et al. Choosing Reputable Systems in a P2P Network [A]. Proc.11th Int'l World Wide Web Conf [C]. Hawaii: ACM Press, 2002. 441-449.

[6] S Kamvar, M Scholsser, H Garcia-Molina. The EigenTrust Algorithm for Reputation Management in P2P Networks [A]. Proc.12th Int'l World Wide Web Conf [C]. NewYork: ACM Press, 2003. 640-651.

[7] Y Wang, J Vassileva. Bayesian Network-Based Trust Model in Peer-to-Peer Networks [A]. Proceedings of the Workshop on "Deception, Fraud and Trust in Agent Societies" at the Autonomous Agents and Multi Agent Systems 2003(AAMAS-03). Berlin: Springer-Verlag, 2003. 23-34.

[8] Li Xiong, Ling Liu. PeerTrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities [J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 6(7): 843-857.

[9] Dou Wen, Wang Huai-Min, Jia Yan, et al. A Recommendation-Based Peer-to-Peer Trust Model [J]. Journal of Software, 2004, 15(4): 571-583. (in Chinese)

[10] eBay Web Site [OL]. http://www.ebay.com, 2009-03-10.

[11] Amazon.com [OL]. http://www.amazon.com, 2009-03-10.

[12] ZHANG Yu, CHEN Hua-jun, JIANG Xiao-hong, SHENG Hao, et al. A Survey of Trust Management for E-commerce Systems [J]. Acta Electronica Sinica, 2008, 36(10): 2011-2012. (in Chinese)

[13] LI Jing-tao, JING Yi-nan, XIAO Xiao-chun, WANG Xue-ping, et al. A trust model based on similarity-weighted recommendation for P2P environments [J]. JournalofSoftware, 2007, 18(1): 157-167. (in Chinese)

[14] Zhang Qian, Zhang Xia, WenXue-zhi, Liu Ji-ren, et al. Construction of peer-to-peer multiple-grain trust model [J]. Journal of Software, 2006, 17(1): 96-107. (in Chinese)

[15] A Abdul-Rahman, S Hailes. Supporting trust in virtual communities [A]. In Proc.of the 33rd Hawaii International Conference on System Sciences [C]. Los Alamitos: IEEE Computer Society Press, 2000. 132-141.

[16] S Y Lee, O H Kown, J Kim, S J Hong. Mitigating the Impact of Liars by Reflecting Peer's Credibility on P2P File Reputation Systems [A]. Lecture Notes in Computer Science, Agents and Peer-to-Peer Computing. Heidelberg: Springer, 2008. 111-122.

[17] L Mekouar, Y Iraqi, R Boutaba. Detecting malicious peers in a reputation-based peer-to-peer system [OL]. http://bcr2.uwaterloo.ca/~iraqi/Papers/Conferences/CCNC 2005.pdf, 2005-01-03.

[18] Xu Feng, Lü Jian, Zheng Wei, Cao Cun. Design of a trust valuation model in software service coordination [J]. Journal of Software, 2003, 14(6): 1043-1051. (in Chinese)

[19] Zhou Z Z, Luo Y L, Guo L M, Ji M J. A Trust Evaluation Model based on Fuzzy Theory in P2P Networks [J]. Journal of computers, 2011, 6 (8): 1634-1638.

[20] Guo LM, Luo YL, Zhou ZZ, Ji MJ. A Recommendation Trust Method Based on Fuzzy Clustering in P2P Networks [J]. Journal of software, 2013, 8 (2): 357-360.

[21] Peng M, Xu Z Q, Pan S M, Li R, Mao T Y. AgentTMS: A MAS Trust Model based on Agent Social Relationship. Journal of computers, 2012, 7 (6): 1535-1542.

[22] Analytic Hierarchy Process [OL]. http://en.wikipedia.org/wiki/Analytic_Hierarchy_Process, 2010-08-01.

[23] Yu Z, Zheng XF, Wang SJ, Li MX. A P2P trust model based on preference. The 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing.

[24] QueryCycleSimulator [OL]. http://p2p.stanford.edu/www/demos.htm, 2009-03-10.

[25] Schlosser M, Condie T, Kamvar S. Simulating a file-sharing P2P network. In: Proceedings of the 1st Workshop on Semantics in P2P and Grid Computing (SemPGRid2003), Budapest, 2003: 69-80.

[26] Tian G, Peng H, Sun C, Li Y J. Analysis of Reputation Speculation Behavior in China's C2C E-Commerce Market. Journal of computers, 2012, 7 (12): 2971-2978.

Zhen Yu was born in Shandong Province, P.R. China on autumn, 1983. Now she is a lecturer in school of Information, Beijing Wuzi University. Her major is computer application. Her research experiences focused on areas of trust computation and network security.

Jie Zhu is a professor in school of Information, Beijing Wuzi University. He was awarded the honored title of "outstanding young teacher in Beijing" in 1994. His major is computer science and technology. His research interests include system development, database application, etc.

Guicheng Shen was born in Jiangsu Province, P.R. China in 1966. Now he is a professor in school of Information, Beijing Wuzi University. His major is computer application. His research interests include information security, business intelligence, etc.

Haiyan Liu was born in Neimeng Province, P.R. China in 1978. Now she is a lecturer in Department of Computer Engineering, Beijing Information Technology College. She had done her postdoctoral research in State Key Laboratory of Hydro science and Engineering, Tsinghua University, Beijing, China. Her major is computer application.