Send Orders for Reprints to reprints@benthamscience.ae

Research of Trust Model based on Interest Group and Similarity Recommendation

Hao Yan*

Software Engineering Institute, Jinling Institute of Technology, NanJing, No. 99 Hongjing Road Jiangning District Nanjing JiangSu, China

Abstract: Trust should be substantially based on evidences including historical behaviors and recommendations in p2p. But experiments show that nodes usually just focus on the services they are interested in. For others they may ignore or feedback at will. So in most cases the system suffers a lot from dishonest feedbacks and strategically cheating behaviors of malicious nodes. Paper proposes a new trust model based on interest group and similarity recommendation, in which nodes belong to their interesting groups, give feedback only to the service supplied by the same group for improving the accuracy of the feedback and recommendations. By this way nodes trust are divided into two parts: trust intra-group and trust inter-group according to their relations. Experiment results show that our trust model can help nodes effectively select appropriate interaction partners.

Keywords: p2p, trust model, interest group, similarity recommendation, inter-group trust.

1. INTRUDUCTION

P2P (Peer to Peer) is a distributed network, in which nodes are keeping equivalent relations, connecting with each other directly to exchange data and service. Because of the open, flexible, and dynamic characteristics, P2P network is used widely in fields of file-sharing, collaborative processing, and real-time communication etc. But its anonymity easily leads to the malicious nodes and hitchhike nodes existing in the network, and affecting the overall performance of the system. To solve the problems, based on the concept of trust management proposed by Blaze [1], the trust model in P2P has appeared, whose central idea is: by analyzing the data such as the historical behaviors of the interactions among nodes, and the recommendations of neighbor nodes etc, to determine whether the node is trustworthy or not, thus avoiding the interactions with malicious nodes or untrustworthy nodes and further improve network security.

Trust model is a measurable system to evaluate the trustful level of a node. Trust usually derives from two channels, first is for the service quality, the second is for the evaluations to other nodes. But different nodes may have different interests when participating in network, for example, in file-sharing applications, some nodes are only interested in music files, some nodes are interested in video, so different interest may lead to different evaluation standards, and resulting in error assessments. To resolve these problems, this paper proposes a trust model based on interest group and similarity recommendation. In one group, nodes have the same interest, so they are more active and giving accurate evaluation. Simulation results show that this model can improve the service quality effectively.

2. RELATED WORK

A lot of research work has been carried out on trust models, such as Altman gave a global trust model based on PKI [2], in which many leader nodes were set for managing and supervising other nodes, so this model had a high reliability, but the expansibility was bad and the problem of single point of failure existed; Paper [3] raised a trust model based on Bayesian network to denote different performance of different facet of the trust, but in fact this idea is essentially based on the user's own subjective judgments, which could be with prejudiced; Paper [4] gave a global trust model—EigenTrust, which gave every node a global trust value based on historical transaction records and according to the value to decide the transaction can be done or not. But the model presented a sub trust set as the basis, which may be not reasonable and hard to be used in the real world; Paper [5] proposed a new trust model—PowerTrust, which is based on the EigenTrust model and has improved performance and ability of resisting malicious behavior, but still is has not considered the transaction amount and doesn't facilitate the punish policy against the malicious nodes. Paper [6] proposed PeerTrust model based on feedback mechanism, which considered multiple trusted evaluation factors, gave a comprehensive trust value based on all the factors, but this algorithm did not consider the convergence problem of the large-scale network and punishment of the malicious nodes; In addition there are also many trust models based on node roles, fuzzy theory, cloud and so on [7-10]. While these models have their distinct method to solve the problem of nodes for abusing of P2P

1874-4443/14

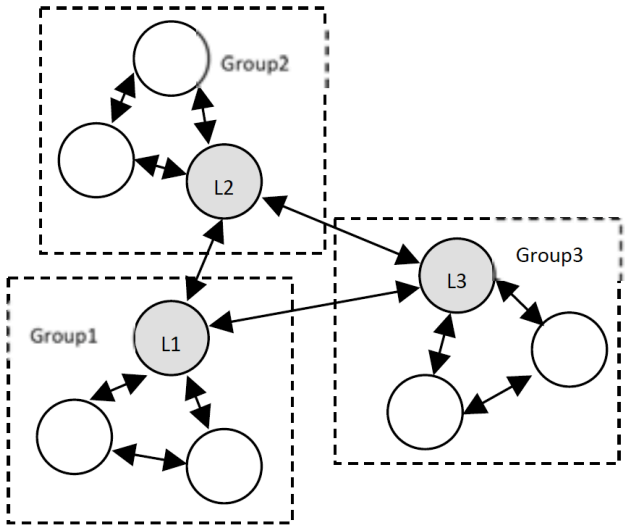

Fig. (1). Interest Groups.

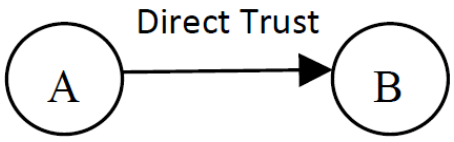

Fig. (2). Direct Trust.

resources and restrain the malicious behaviors of nodes, but meanwhile they ignored an important fact, that, like human society, nodes usually do not seriously evaluate a field which is uninteresting to them, which results error assessments. Therefore, this paper presents a trust model based on interest group and similarity recommendation which improves the effectiveness of feedback and recommendations.

3. NEW TRUST MODEL

3.1. Basic Definition

Interest group: We divide the whole network to N groups according to different file types, such as movie group, mp3 group, computer science group etc. Every group has a leader node, whose responsibilities are to maintain the information and global reputations of all nodes in his group, and all the basic information of other groups including their leader nodes, their network address etc. Usually the leader node is the one who has the best performance. The remaining are general nodes, which can freely submit their information to the leader node and choose to join the interest group that they are interested in as shown in Fig. (**1**).

Direct trust: the value is calculated based on direct transactions between the nodes Fig. (**2**).

Reputation inner group: is the global trust inner group, which reflects the node ability and trust of supplying services to other nodes in one group.

Recommendation trust inter-group: The recommendation trust to nodes in different groups is the direct trust value

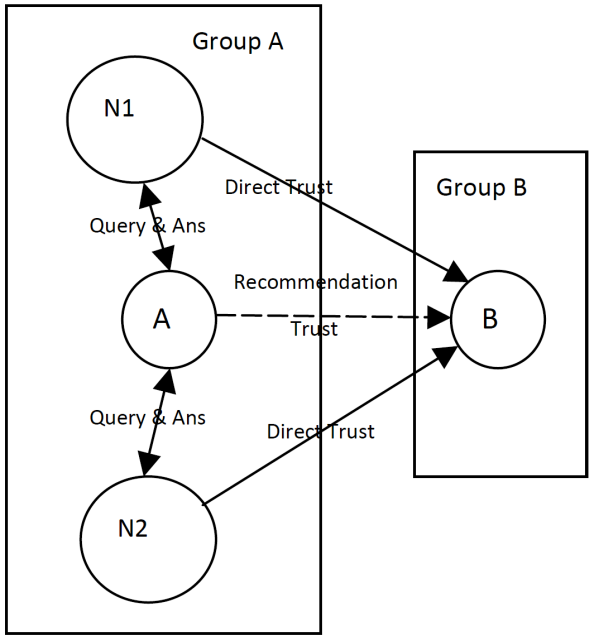

Fig. (3). Recommendation trust inter-group.

of neighbor nodes, with higher similarity in this group as shown in Fig. (**3**).

Decay of trust: Similar to the human society, both trust value and reputation will decay with the passage of time, which should be considered when constructing the trust model. Assuming the valid time period is T, evenly split to M_T time periods, so the span of each period is:

$$T_p = \frac{T}{M_T} \tag{1}$$

and the decay function can be defined to:

$$f(t) = \rho^{M_T - \frac{T_c - t}{T_p}}, \tag{2}$$

in which, T_c denotes the current time, t denotes the time when the historical transactions happened, parameter σ ρ is the adjustment factor, which can be used to adjust the rate of decay.

3.2. Implements

Direct Trust denoted by DTr_T is the subject evaluated trust value based on the historical direct interactions between nodes. Assuming node N_a applied $Tran_T$ count service requests to node N_b in time period t, using $Tran_S$ to denote successful transaction times, $Tran_F$ to denote fail transaction times. So the direct trust of N_a to N_b in this period is

$$DTr_{(a->b)\Delta t} = \frac{Tran_S}{Tran_S + Tran_F} * f(\Delta t) \tag{3}$$

So in the whole valid time span, the direct trust of N_a to N_b is

$$DTr_{(a->b)T} = \frac{\sum_{i=1}^{n} DTr_{\Delta ti}}{n} * \omega^{\frac{\sum Tran_F}{\sum (Tran_F + Tran_S)}} \tag{4}$$

And ω is the rewards and punishments adjustment factor, whose value range is between 0 and 1.

Reputation in group denoted by G_{Rp} is the global trust inner group, which reflects the node's ability and trust for supplying services to other nodes in one group. Within the group, every direct trust value between nodes after each of their transactions should be sent to the leader node and stored there. Therefore if m nodes in one group, the leader node should hold a $m \times m$ matrix for storing the direct values like this:

$$DTr_{all} = \begin{bmatrix} DTr_{11} & DTr_{12} & \cdots & DTr_{1m} \\ DTr_{21} & \ddots & \ddots & DTr_{2m} \\ \vdots & \ddots & \ddots & \vdots \\ DTr_{m1} & DTr_{m2} & \cdots & DTr_{mm} \end{bmatrix},$$

Where DTr_{ab} denotes the direct trust of N_a to N_b. Then we can get the group reputation of node N_i:

$$G_{Rp}{}^{i} = \frac{\sum_{n=1}^{m-1} DTr_{ni}}{m-1}, n \neq i \tag{5}$$

Recommendation trust inter-group is denoted by RTr. Experiences show that recommendation trusts from nodes with similar interests are more reliable which should be given higher weight. So in our model, when evaluating nodes trust in other groups, we choose recommendations from the neighbor nodes with the similar trust. This model uses the cosine similarity function to measure trust similarity between two nodes:

$$S_{ij} = \frac{\sum_{k=1}^{m-2} DTr_{ik} DTr_{jk}}{\sqrt{\sum_{k=1}^{m-2} (DTr_{ik})^2} \sqrt{\sum_{k=1}^{m-2} (DTr_{jk})^2}}, \quad k \neq i, j \tag{6}$$

And N_k is one node in the same group with N_i and N_j.

Setting the similarity threshold, is δ, choosing p neighbor nodes with bigger similarity than δ, we can get the recommendation trust:

$$Rtr_{uv} = \frac{\sum_{i=1}^{p} S_{ui} * DTr_{iv}}{\sum_{i=1}^{p} S_{ui}} \tag{7}$$

So, the final trust to one node is:

$$Tr_{a->b} = \begin{cases} \alpha DTr_{a->b} + (1-\alpha) G_{Rp}^{b} & In\ the\ same\ group \\ \beta DTr_{a->b} + \gamma Rtr_{a->b} + (1-\beta-\gamma) G_{Rp}^{b} & In\ different\ group \end{cases} \tag{8}$$

In which α, β, γ are weight adjust factors, and $0 < \alpha < 1$, $\beta + \gamma < 1$.

3.3. Transaction Process

Assuming node N_a intend to download files from N_b. Firstly, N_a has to estimate if N_b is trustworthy or not.

So, there are two scenarios, the first one is:

※ N_a and N_b in one group, then N_a should do the work as following steps:

1、Get the direct trust of N_b by their direct transaction records. If there are no records in the database, set the trust value to the initial value.

2、Send query request to the leader node in their group for asking the N_b's group reputation.

3. Get the final trust by the equation 8, if the trust value less than trust threshold, refuse the transaction, otherwise start the transaction.

4. After finishing the transaction, store the new transaction result with current time into its own database, and also send the new trust value (by step 3) to the leader node to update the global reputation of N_b.

The second scenario is:

※ N_a and N_b in different group, then N_a should do the work as the following steps:

1. Get the direct trust of N_b by their direct transaction records. If there is no record in the database, set the trust value to the initial value.

2. Search neighbor nodes with the larger similarity than threshold in their group.

3. Get the recommendation trust of N_b through the selected neighbors.

4. Send query request to the leader node of N_b, and get the N_b's global reputation.

5. Get the final trust by equation 8, if the trust value less than trust threshold, refuse the transaction, otherwise start the transaction.

6. Store the new transaction result with current time in its own database.

4. EXPERIMENTS

In order to evaluate this approach, we've made several simulation experiments with PeerSim(V1.0). PeerSim is a

Table 1. Simulation Parameters.

Parameter Name	Value
initial trust value	0.65
trust threshold η	0.65
valid time T	10 min
time period T_p	30 sec
time period count M_T	20
adjustment factor ρ	0.8
weight α	0.7
weight β	0.5
weight γ	0.3
reward & punishment ω	0.8

network simulation software for P2P network, supporting structured and unstructured P2P network simulation. We add codes for implementing our trust model into the software and set 2000 nodes in the network, 50 groups with 40 nodes in each group.

In this simulation environment, we preset two types of nodes:

a). normal node. All of these nodes supply real services, and give real evaluations.

b). malicious node. Who will give false information and do not give true files for download.

For the sake of simplicity, each node in our system plays only one role at a time, either the role of file provider or the role of a downloader.

Meanwhile, we assume the network is an ideal model, every node has the right to search all files no matter which node they belong to. Then the node selects a more trustful node it considered after evaluation judgment and downloads the file it needed.

Simulation parameters are shown in the Table **1**.

At the same time, for comparing the performance, we develop the EigenTrust in experiment too

5. RESULTS

The goal of the first experiment is to see if the trust model can judge the trustful nodes, rightly, in order to get the successful transaction. We set 20% malicious nodes in the network, who will supply bad services, after 5000 cycles, the fluctuation ratio of successful transactions is shown as the Fig. (**4**).

From the Fig. (**4**) we can see that with the same initial trust values, if there is no trust evaluation mechanism in the network, the successful transaction rate decreases very fast and finally fluctuates around 40%. But if we add trust models (EigenTrust or our model) to the network, the successful transaction rate increases with the cycle. The reason is that all these two trust models can effectively evaluate whether the node is trustful or not. So the node can select the most trustful node for its downloading and prevents it from the malicious nodes. From Fig. (**4**), we can also conclude that with the constant malicious ratio, our trust model has a better successful transaction ratio than Eigentrust increasing with the cycles and finally arriving at a steady state.

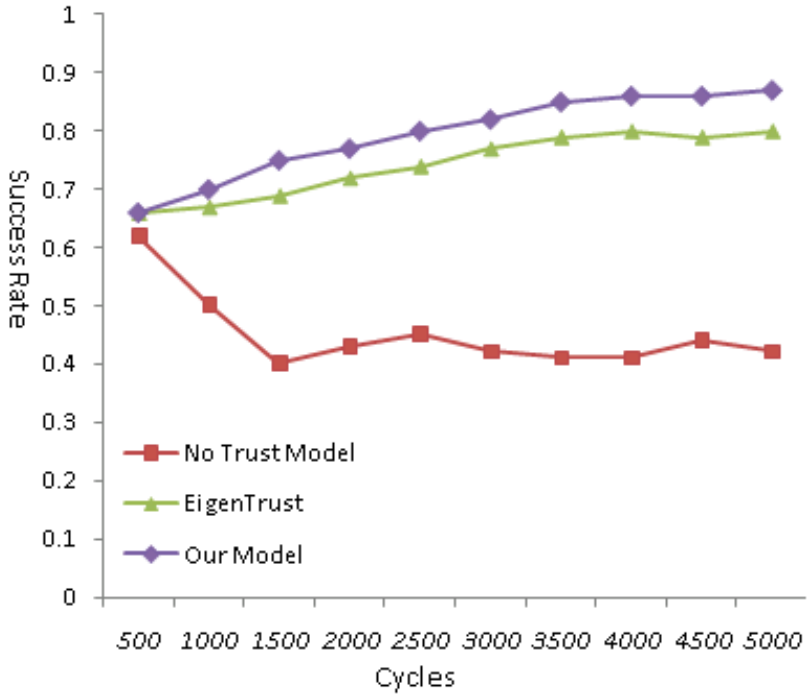

Fig. (4). First experiment.

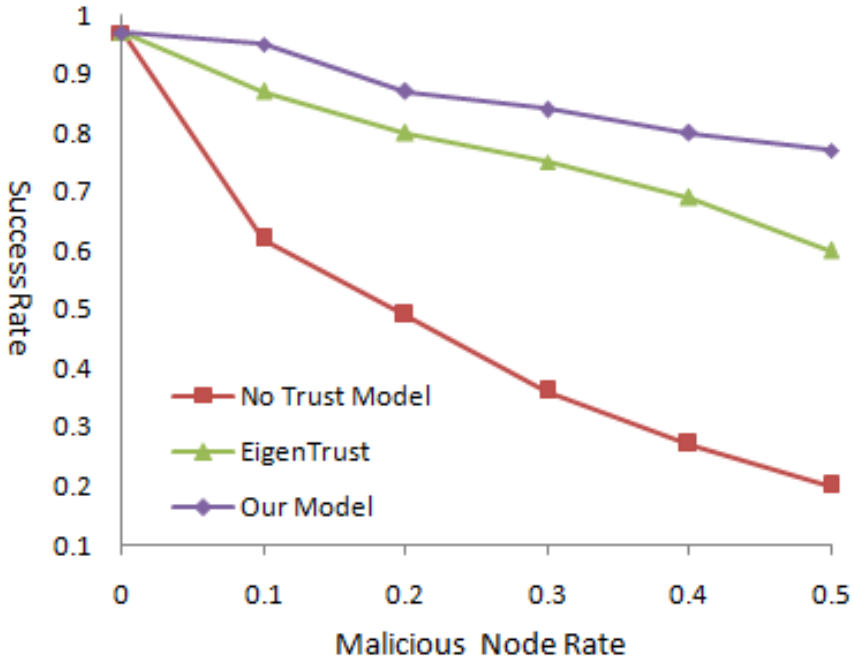

Fig. (5). Second experiment.

In the second experiment, we are increasing the rate of malicious node to inspect the effectiveness of the model. The result is shown in Fig. (**5**).

We can see that with the malicious nodes rate increasing, the entire successful transaction ratio under the three conditions is decreasing. But in no trust model condition, the ration decreases faster, in our trust model and EigenTrust the ratio can also keep in a higher level. Relatively speaking, our trust model still gets a best result.

CONCLUSION

To make nodes to develop trust and reputation among themselves is a popular issue in peer-to-peer system where many different resources are offered. Trust and reputation mechanisms can provide a way for protection of unreliable or malicious nodes. In this paper, we propose a new trust model in p2p based on interest group and similarity recommendation, which can improve accuracy of feedback and recommendations, restrain the influences of random evaluations. Simulations show that this trust model can help nodes make effective decision for judging trustful node and improve the security of the P2P network.

But frankly speaking, because of the complexity of the real network and the behaviors of nodes with random uncertainty, it is impossible to describe and identify all the characteristics and elements of node's behavior. Therefore, almost all the existing methods for analyzing the similarity of behavior have their own limitations and only suitable for certain environments in which the node behaviors has some fixed characteristics and easy to confirm. Our model also has some weakness, for example, it can judge the node trustful or not and punish it, but cannot deal with conspiracy cheating of multiple nodes, and at the beginning we assumed the leader node is trustful, but if it is not, our model does not resolve the scheme. So next we will continue our research around these two problems.

CONFLICT OF INTEREST

The author confirms that this article content has no conflict of interest.

ACKNOWLEGMENTS

Project supported by the College and University Natural Science Foundation of the Ministry of Education, Jiangsu (13KJD52000).

REFERENCES

[1] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," In: *Proceedings of the 1996 IEEE Symposium on Security and Privacy,* 1996, pp. 164-173.

[2] J. Altman, "PKI Security for JXTA overlay networks," Technical Report, TR-I2-03-06, Palo Alto: Sun Microsystem, 2003.

[3] Y. Wang, and J. Vassileva, "Bayesian network-based trust model," In: *Proceedings of IEEE/WIC International Conference on Web Intelligence,* Halifax: Canada, 2003, pp. 372-378.

[4] S. Kamvar, M. Scholsser, and H. Garcia-Molina, "The EigenTrust algorithm for reputation management in P2P networks," In: *Proceedings of 12th Int'l World Wide Web Conf.,* New York: ACM Press, 2003, pp. 640-651.

[5] R. Zhou, and K. Hwang, "A robust and scalable reputation system for trusted peer-to-peer computing," *IEEE Transactions on Parallel and Distributed Systems,* vol. 18, no. 4, pp. 460-473, 2007.

[6] 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, pp. 843-857, 2004.

[7] L. Yang, Y. Zhang, and C. Xing, "A node interest similarity based P2P trust model," In: *12th IEEE International Conference on Communication Technology (ICCT),* 2010, pp. 572-575.

[8] T. Wen, and C. Zhong, "Research of subjective trust management model based on the fuzzy set theory," *Journal of Software,* vol. 14, no. 8, pp. 1401-1408, 2003.

[9] W. Li, and L. Ping, "Trust model to enhance security and interoperability of cloud environment," *Cloud Computing,* Springer Berlin Heidelberg, 2009, pp. 69-79.

[10] J. Li, Y. Jing, and X. Xiao, "A trust model based on similarity-weighted recommendation for P2P environments," *Ruan Jian Xue Bao (Journal of Software),* vol. 18, no. 1, pp. 157-167, 2007.

Received: November 26, 2014 Revised: January 09, 2015 Accepted: January 20, 2015