A Group-Based Trust Model in Peer-to-Peer Environment

Fen Xu, Yajun Guo,Qin Wang
Department of Computer Science, Huazhong Normal University, Wuhan 430079, Hubei,China, xufen5460@tom.com

Abstract. The open and anonymous nature of peer-to-peer system makes it easy to be attacked and abused by some malicious nodes, so it is very important to establish a perfect trust mechanism in peer-to-peer environment. In this paper, we propose a novel group-based trust model in which the trust relationships between entities are divided into trust relationship in group and trust relationship between groups. This model deals with these two kinds of trust relationships in the different way and improves trust value calculation method. The model can get more real trust value at the small price, and the advantages of the model are simple structure and high reliability.

1 Introduction

With the continuous development of peer-to-peer technology, distributed computing, electronic commerce, file sharing and instant messaging have been widely used. Peer-to-peer users directly establish interconnection and share resources. Peer-to-peer has been a new focus in Internet application.

At present, peer-to-peer can be classified into three categories according to the network structure. The first category is a purely decentralized peer-to-peer system, such as Gnutella [1] and Freenet [2] and so on. All nodes must play the role of searching resource and downloading. The second category is a hybrid peer-to-peer system, such as Napster, MSN, and BT file sharing and so on. Its searching function can be implemented in the centralized directory server, but downloading is still in peer-to-peer way. The third category is a super-node network architecture system, such as KaZaa (one of the most popular file sharing system currently). It is the organic combination of the purely decentralized peer-to-peer system and the hybrid peer-to-peer system. These super-nodes unlike the server in the hybrid peer-to-peer are transparent in function. Even if some fail, the whole network will not be affected.

Please use the following format when citing this chapter:

Xu, F., Guo, Y., Wang, Q., 2007, in IFIP International Federation for Information Processing, Volume 251, Integration and Innovation Orient to E-Society Volume1, Wang, W. (Eds), (Boston: Springer), pp. 44-50.

Although peer-to-peer network structure is with dynamic property and convenience, there are serious security issues. Good trust model is the key to assuring high quality service which is provided by the network. At present, there are a lot of research on the trust model based on peer-to-peer environment and mainly can be divided into the following categories [3, 4]: Digital signature model. This method doesn't pursue the credibility of nodes, but emphasizes the credibility of the data. Take file sharing application for example, when downloading is completed every time, the user judges the authenticity of the data. If the user trusts the authenticity of the data, makes a signature for the data. The data obtains the more signatures, the authenticity is higher. However, this method can only be applied for data sharing application, and can't prevent mass fraud, namely, malicious group of nodes all make signatures for inauthentic data. Currently popular file sharing applications are using this method [5]. PKI-based [6] trust model. There exist a small number of central nodes which are responsible for the supervision of the entire network and announce illegal nodes in the regular time. The legitimacy of central nodes is guaranteed by certificates issued by the CA. This kind of system usually relies on the center and has scalability and single node failure etc. issues, such as many servers [7] of eDonkey. Global credibility model. This kind of model obtains the global credibility of nodes by using mutual satisfaction iteration among the neighbor nodes. Local recommendation-based trust model [8, 9]. A node obtains the credibility of a certain node by asking for limited other nodes in this kind of system.

These models respectively have their advantages and disadvantages. In this paper, the basic idea of constructing the model is based on the local recommendation trust model. Trust value calculation method is improved in this model, so we can get more real trust value at the small price.

2 A group-based trust model

In this paper, we propose a novel group-based trust model based on the third categories super-node network structure (as shown in figure 1). This model can be used to deal with trust relationship between the entities in peer-to-peer environment and help peer-to-peer entities make trust choice. Select a node whose performance is the optimal as a super-node in each group of nodes. Some information of nodes in this group is stored in super-nodes. There is a lot of this kind of groups in the whole peer-to-peer structure, and super-nodes in each group are connected in the form of the pure peer-to-peer structure in the overall structure. This model divides the trust relationships between entities into trust relationship in group and trust relationship between groups which are dealt with in a different way. This model can evaluate the trust relationship between the entities more accurately, thus can solve security issues more effectively in peer-to-peer environment.

2.1 Implementing process of the model

Group is a set of node members which have certain relationships, and can be organized according to different principles. The principle of organizing group in this model is the set of members which transact frequently, so there are transaction histories among all members of the group. In this process, when node u requests for

transaction with node v, it is necessary to know the trust value of node v at first. Two cases are discussed here.

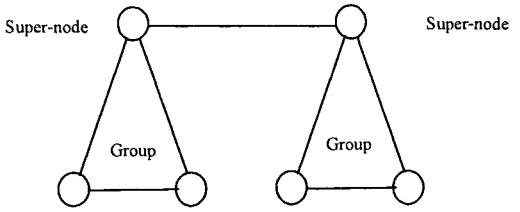

Fig. 1. Group-based peer-to-peer structure

(1) If node u and node v belong to the same group, the trust value of node v is calculated by node u using trust value calculation method in group. According to the trust value, node u judges whether transacts with node v. Update local records according to the results of the transaction at last.

(2) If node u and node v belong to the different group, the trust value of node v is calculated by node u using trust value calculation method between groups. According to the trust value, node u judges whether transacts with node v. Update records in the super-node according to the results of the transaction at last.

Implementing process of the whole model is shown in figure 2.

2.2 Trust value calculation

The trust value calculation of the model is divided into calculation in group and calculation between groups. The trust value of node v calculated by node u is $TV_{u,v}$ which is a discrete value between 0 and 1. The results of evaluation are more near to 1, namely, the node obtains the more satisfactory services, or the opposite.

- **Trust value calculation in group**

The trust value in group is calculated by using time based past transaction as well as peer recommendations.

The time based past transaction value of node v calculated at node u is denoted as $PT_{u,v}$ which is defined as follows:

$$PT_{u,v} = 1 - \frac{1}{\max[\{\mu_s ST_{u,v} - \mu_u UT_{u,v}\}, 0] + 1} \quad \ldots (1)$$

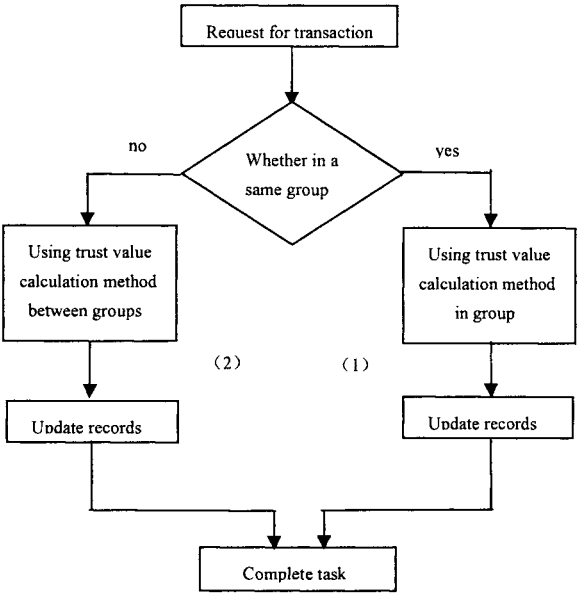

Fig. 2. Implementing process of the model

Where $PT_{u,v}$ is the past transaction value of node v calculated by node u based on past transactions, $ST_{u,v}$ is the successful transaction between node u and node v, $UT_{u,v}$ is the unsuccessful transaction between node u and node v. Both μ_s and μ_u are positive numbers depending on the time, and respectively represent the corresponding weights of $ST_{u,v}$ and $UT_{u,v}$. The weight μ_s is defined as:

$$\mu_s = \begin{cases} h & t_s \leqslant 1 \\ m & 1 < t_s \leqslant 2 \\ l & t_s > 2 \end{cases} \quad \ldots (2)$$

μ_u is defined similarly. This mapping function assigns low, medium, or high weights based on the last transaction time. The time t_s and t_u are defined as:

$$t_s = \frac{t - st_{u,v}}{\Delta t} \qquad t_u = \frac{t - ut_{u,v}}{\Delta t} \qquad \ldots (3)$$

Where t is the current time, $st_{u,v}$ ($ut_{u,v}$) is the time of last successful (unsuccessful) transaction, $\triangle t$ is the threshold time.

The graph of the past transaction evaluation against successful and unsuccessful transactions is shown in the figure 3. 'h', 'm' and 'l' are given the values 3, 2, and 1 respectively, and μ_s and μ_u are randomly assigned one of these values in every calculation of $PT_{u,v}$. The graph shows fluctuations when $ST_{u,v}$ and $UT_{u,v}$ have

roughly the same values, but when $ST_{u,v}$ is considerably larger than $UT_{u,v}$, $PT_{u,v}$ approximates to 1.

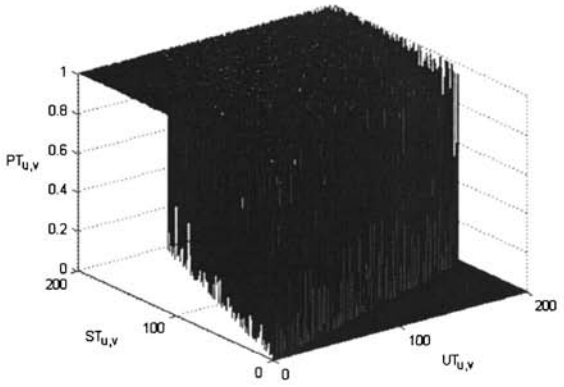

Fig. 3. Time based past transaction evaluation

Suppose the number of nodes is n in the group. Each node owns a trust value of any other nodes it transacts with before. When any node obtains peer recommendations, the trust value of the node is calculated by using the following formula.

$$PR_{u,v} = \frac{\sum_{k=1}^{n-1}[TV_{u,k} * TV_{k,v}]}{n-1} \quad \ldots (4)$$

Where $PR_{u,v}$ is the peer recommendations trust value of node v calculated by node u, $TV_{u,k}$ is the trust value of node k calculated by node u, and $TV_{k,v}$ is the trust value of node v sent by node k.

Suppose that node u wants to calculate the trust value of node v, then $TV_{u,v}$ is calculated by the following equation:

$$TV_{u,v} = (1-\lambda) * PT_{u,v} + \lambda * PR_{u,v} \quad \ldots (5)$$

Where λ is a constant which is between 0 and 1. For nodes just joining the peer-to-peer network or without any thought, users are more willing to believe that the recommendation information of the other nodes, so the value of λ can be set larger. For some opinionated nodes, they prefer to trust their own judgment, so the value of λ can be set smaller, generally we can set λ 0.5.

Update the local records based on the results of the transaction at last.

- **Trust value calculation between groups**

Suppose that there are n nodes in the group in which the performance of super-node is optimal. Super-node has higher power and memory compared to other nodes in the group. Taking storage efficiency into account, the size of group should be

small. For the calculation of trust, super-node cyclically broadcasts a request in a group. In response, all group member nodes forward their $\overrightarrow{TV_{sn}}$ trust value of other member nodes to super-node. The trust vector of super-node is defined as:

$$\overrightarrow{TV_{sn}} = (TV_{sn,1}, TV_{sn,2}, \ldots, TV_{sn,n}) \quad \ldots (6)$$

Where $TV_{sn,k}$ is the trust value of node k. It is calculated by the following equation:

$$TV_{sn,1} = \frac{\sum_{k=2}^{n} TV_{k,1}}{n-1}, \ldots, TV_{sn,n} = \frac{\sum_{k=1}^{n-1} TV_{k,n}}{n-1} \quad \ldots (7)$$

This trust vector is saved in the super-node and updated in the cyclical time.

When node u requests for transaction with node v, and node u and node v belong to the different group, the trust value $TV_{u,v}$ is calculated by the following formula:

$$TV_{u,v} = TV_{sn_v,v} * \theta_{sn_v,sn_u} \quad \ldots (8)$$

Where sn_u is the super-node of node u, sn_v is the super-node of node v, θ_{sn_v,sn_u} is the trust weight between super-node sn_v and super-node sn_u.

3 Performance analysis

The real-time performance of the trust value. When trust value is calculated in this model, time-based past transaction evaluations are considered. Time is set in order to give larger weights of the trust evaluation for recent transactions. For the historical trust value, the recent behavior is more concerned, because the recent behavior can reflect the credit records of the node in the most recent period, thus real-time performance of the trust value is guaranteed. And adding the time factor can also reflect the easy-destruction-hard-construction performance [10] of the credit.

The accuracy of the trust value. When the node calculates the trust value, it not only considers transaction histories of the local records, but also asks for recommendations of members in the group. If small numbers of nodes fail, it doesn't have too much effect on the entire trust value calculation, so the reliability of the model is greatly improved. Because the local stores are only transaction records participated in by their own, and recommending to other nodes is more reliable, thus making the accurate judgment to the trust value is guaranteed.

The integrity of the trust value. Trust values are stored in the node itself in this model and need not other nodes participate in the management, so it prevents the trust value from being altered, forged or deleted by malicious nodes, thus the integrity of the trust value is guaranteed.

The calculation efficiency of the trust value. Selecting a set of nodes among which transactions are very frequent constitutes a group in this model. The advantages are that these nodes are worth trusting at first which can be drawn based

on transaction experience, otherwise, it will not frequently transact with them. And these members whose relationships are close are easier to provide effective information. A node only needs to access to the set of nodes in the group, it can better judge the trust value of the node which wants to transact, so the communication is less and the efficiency is higher.

4 Conclusions

In this paper, we propose a novel group-based trust model based on the super-node network architecture. The structure of this model is very simple. The model is very easy to be accepted by users and can suit for many kinds of peer-to-peer application environment. The trust relationships between entities are divided into trust relationship in group and trust relationship between groups in the model. For the different trust relationship, we use the different calculation method to assure the real-time performance, accuracy, integrity and calculation efficiency of the trust value. In future, we will make much more specific definition and description for this model such as updating strategy of the trust value and so on. We will also incorporate intrusion tolerant intelligence in this model, so that nodes are able to detect false information sent by any malicious node.

References

1. Distributed System for Information storage and Searching Model Description, http://www.gnutella.co.uk/liberary/pdf/paper final gnutella english.pdf.

2. I. Clark, O. Sandberg, B. Wiley, T. Freenet Hong, A distributed anonymous information storage and retrieval system, *Proc. of the Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, July 2000,311-320.

3. W. Dou, H.M. Wang, Y. Jia, A recommendation-based peer-to-peer trust model , *Journal of Software*, 2004, 15 (4), 571-583.

4. F. Cornelli, E. Damiani, S. D. C. Vimercati, *Choosing reputable servents in a P2P network*, in: Proc. of the 11th International World Wide Web Conference Hawaii, ACM Press, May 2002, 376-386.

5. K. Albrecht, AR. Clippee Ruedi, *A large-scale client/peer system, Technical Report,* TR-410, Swiss Federal Institute of Technology, 2003.

6. SD. Kamvar, MT. EigenRep Schlosser, Reputation management in P2P networks, Proc. of the 12th Int'l World Wide Web Conf Budapest, ACM Press, 123-134.

7. J. Altman, PKI Security for JXTA overlay networks, Technical Report, TR-I2-03-06, Palo Alto: *Sun Microsystem*, 2003.

8. A. Abdul-Rahman, S. Hailes, A distributed trust model, *Proc. of the 1997 New Security Paradigms Workshop*, ACM, September 1997, 48-60.

9. M. Blaze, J. Feigenbaum, J. Ioannidis, The role of trust management in distributed systems security , *Secure Internet Programming: Issues in Distributed and Mobile Object Systems*, volume 1603 of Lecture Notes in Computer Science, July 1999, 183-210.

10. Y. Zhong, Y. Yu, *Dynamic Trust Production Based on Interaction Sequence Technical Report*, CSD-TR 03-006, Dept. of Computer Science, Pudure University, 2003.