Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):1103-1108

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

The research of P2P network security model based on group trust relationship

Xue Ming

Henan University of Technology, Henan, Zhengzhou, China

ABSTRACT

At present, it is lack effective mechanism to improve the security of the system in the P2P network. There is a lot of malicious behaviors. Network security model has become an important subject of P2P application research. This paper will study P2P network based on group trust relationship. Set up different groups according to the node interests. The overall trust is compounded by direct trust between nodes, trust between groups and nodes, trust between groups and multiple parameters. Through the simulation experiment, this model is verified to have high ratio of successful download, and the peer load can be controlled in a admissible range. The performance of this model is studied through simulation experiment. The results show that the model can identify malicious nodes effectively. According to the trust value of the responder select the download source. In the P2P network, cooperative nodes have the high request rate of success and node degree of satisfaction in different malicious nodes attack mode.

Key words: Peer-to-peer, Reputation, Trust model, Security

INTRODUCTION

P2P network obtain a rapid development because of its resource sharing, node peer-to-peer communications and network flexible self-organizing characteristics. But due to the essential characteristics of P2P network anonymity, there are a large number of fraud and other malicious behavior in the system. Therefore, establishing an effective, safe trust mechanism is particularly important. It can be the next definition. Trust model is establishing a set of quantitative evaluation system through some kind of strategy. It can give the trust evaluation of the trading node and inform the evaluation to the other nodes in a network. At present, there are a lot of related researches at home and abroad [1-5]. More famous algorithm is P2P network users Eigen Trust put forward by Kamvar at Stanford university.

It is published services and e-commerce community, Peer Trust trust model based on reputation as well as the literature [6,7] trust model in 2003. The several most influential organizations and companies in world computer field, such as ACM, IEEE, Microsoft, IBM, HP are engaged in the research of this area. Domestic, Chen Guihai of nanjing university professor, Dou Wen of national university of defense technology also done a lot of research work in this field. Refer to human social management way, man is not a single individual, they are social. They always form a group according to certain strategy. Then these groups constitute the human society again. Each person has a trust in his own group. They will evaluate each other's trust between groups and groups. Based on this kind of management mode of human society, we propose a trust model GBTM based on group in this paper [8]. They can establish different groups according to interest hobby of the node. The overall trust is compounded by direct trust between nodes, trust between groups and nodes, trust between groups and multiple parameters.

P2P NETWORK SECURITY MODEL BASED ON GROUP

In Trust Frame, all the nodes divided into groups according to certain rules in the network. Node information collection is limited to within the group. Assume that the communication between the nodes and groups is safe, reliable. The whole of the model should include the following several parts: group divisions, nodes trusted computing within the same group, nodes trusted computing between different groups. Finally, the implementation strategy is given and the model is used to supplement and analyze.

The Group Divisions. In Trust Frame, the nodes form a group according to certain rules. Groups constitute the whole P2P network. The group mark with GID. The nodes are marked with the PID identification. {GID, PID} mark the only node in a group.

Trusted Computing of the Same Group Node.

a. The node trust value. After a transaction, node i makes satisfaction evaluation to node j services. We use r_{ij}^{n} to show. Where n is the nth trade. The method of probability possibility is used to distinguish nodes to provide different quality of service. $r_{ij}^{n} \in [0,1]$, 0 means node i to node j is entirely unsatisfactory. The critical value of 0.5 is satisfied and unsatisfied. 1 shows node i to node j is fully satisfied. The larger the value is, the higher the satisfaction is. Node i to node j is expressed as an evaluation information. It is$< r_{ij}^{n}, t^{n}, m >$. The t^{n} as ageing time that seems to node i for the nth transactions. The initial value is t. It decreases with time. When the duty is 0, $< r_{ij}^{n}, t^{n}, m >$ is deleted. N nodes said i and j are the maximum effective transaction serial number. If the evaluation information be deleted because of the aging time expires. Then the rest of the serial number of evaluations information automatically adjust. m shows trading relevant other information. t^{n} can be shown by the following.

$$t^{n} = \begin{cases} t \\ t^{n} - 1 \end{cases} \tag{1}$$

Direct trust value of node i to node j can be said by R_{ij}.

$$R_{ij} = \begin{cases} \sum_{k-1}^{n} \left(\dfrac{r_{ij}^{k} t^{k}}{\sum_{l=1}^{n} t^{l}} \right) & n \neq 0 \\ \\ R_{initial} & n = 0 \end{cases} \tag{2}$$

In the type, $R_{initial}$ is initial trust value for the new node.

b. The similarity degree of node. The node i and j trust evaluation similarity is expressed by S_{ij}. The higher similarity degree of i and j, it shows the view of i and j to other nodes is consistent in the network. Calculate the similarity of the i and j using the modified cosine similarity.

$$S_{ij} = \sum_{c \in I_{ij}} (R_{ic} - R_{i})(R_{jc} - R_{j}) / [\sqrt{\sum_{c \in I_{ij}} (R_{ic} - R_{i}^{2})} \sqrt{\sum_{c \in I_{ij}} (R_{jc} - R_{j}^{2})}] \tag{3}$$

In the formula, I_{i} shows node set with i direct trust relationship. I_{j} shows node set with j direct trust relationship. I_{ij} shows node set with i and j direct trust relationship. R_{ic} shows direct trust for node i to node c. R_{i} and R_{j} respectively mean direct trust arithmetic mean value about node i and j to other nodes.

c. The reputation values of the node. In group G_{i}, from the node i, the reputation values of node j expresses in T_{ij}.

$$T_{ij} = \sum_{k \in G_{i} \cap k \neq i \cap k \neq j} S_{ik} R_{kj} / (|G_{i}| - 2) \tag{4}$$

d. The reliability of the node. In group G_{i}, the reliability evaluation of node i to node j is R_{Aij}. Its calculation is as follows.

$$R_{Aij} = \begin{cases} \frac{\alpha R_{ij}}{\alpha+\beta}(\alpha\neq 0 \,\text{or}\, \beta\neq 0) \\ \\ 0(\alpha=0\, and\, \beta=0) \end{cases} \qquad (5)$$

α and β respectively mean the weight of direct trust and indirect trust in the nodes. The value of α and β are changing. They are affected by the factors such as transaction number, transaction amount. We define that the transaction efficiency is the ratio of transaction amount and transaction number in order to quantify α and β . The higher the transaction efficiency, the greater the understanding between the nodes.

$$\alpha = \begin{cases} (\frac{S_{Qij}}{T_{Nij}}) \quad (Have\ \ atransaction\ \ record) \\ \\ 0 \quad (No\ \ transaction\ \ record) \end{cases} \qquad (6)$$

$$\beta = \begin{cases} \sum_{K\in T\,(\mathrm{i})\cap k=j} S_{Qik} / \sum_{K\in T\,(\mathrm{i})\cap k=j} T_{Nik} \ \ \text{(Have atransaction record)} \\ \\ 0 \quad (No\ \ transaction\ \ record) \end{cases} \qquad (7)$$

T_{Nij} means "effective" transaction number between node i and j. S_{Qij} means "effective" transaction amount between node i and j. Each transaction amount is stored in the m field of satisfaction evaluation. T(i) means "efficient" node set deal with node i. The meaning of "effective" refers to S_{Qij} . T(i) and other relevant information, they are not deleted because of the aging time expires.

Nodes trusted computing between different groups.

a. Direct trust between the groups. The direct trust group G_i to group G_j shows with $R_{G_iG_j}$ $R_{G_iG_j} = \sum_{i,j} R_{ij} / [|G_i|\times|G_j|]$.

$$R_{G_iG_j} = \sum_{i,j} R_{ij} / [|G_i|\times|G_j|] \qquad \mathrm{i}\in G_i\,,\ \mathrm{j}\in G_j \qquad (8)$$

b. The reputation of nodes in the groups. Reputation value of node j in their group expresses in $R_j^{G_j}$.

$$R_j^{G_j} = \sum_{k\in G_j\cap k\neq j} R_{kj} / [|G_i|-1] \qquad (9)$$

c. Reliability of nodes in the group. Reliability evaluation is shown by R_{Aij} .

$$R_{Aij} = \min\left\{R_{G_iG_j}, R_{\mathrm{j}}^{G_j}\right\} \qquad (10)$$

A supplement of the model robustness.

a. The management of the group. The trusted computing involves in nodes trust within the same group and the different groups of nodes. In order to facilitate the node reputation maintenance in the group and trust information interaction between the groups, we set up three high reputation nodes as a group manager. Group manager is responsible for maintaining the node reputation and the trust information between groups. Their content exactly consistent, so as to prevent the happening of the "single point of failure".

b. The process of the new nodes. The anonymity of P2P network makes it hard to distinguish the normal new nodes and Whitewashing nodes. In this paper, we dynamically adjust the initial trust evaluation of a new node. Set the silent time t, encourage the good behavior of the normal new node, and restrict malicious behavior of Whitewashing node. At the same time, the node Whitewashing behavior is limited within the group, so it reduces the overall cost. In the t time of new node just joined, the node can only provide services, do not request service. Then the group manager respectively collect the satisfaction evaluation of a new node. Calculate the reputation of the nodes according to the type (3) and (4). We can obtain the new node reputation from the three managers. It can be denoted by T_{new}^{1}, T_{new}^{2} , T_{new}^{3}.At the same time, according to the type (10) to calculate the average value of group nodes reputation. It can be denoted by R_{ave}. In the silent time, the new node reputation values are all greater than the R_{ave}, a new node initial trust value $R_{in} = \max(0.5, R_{ave})$ .Otherwise, $R_{in} = \mathrm{m\,in}(0.5, \mathrm{T}_{new}^{1}, \mathrm{T}_{new}^{2}, \mathrm{T}_{new}^{3})$ after the silence time, group managers will put initial trust of the new node broadcasted to the members of the group. Each node updates the related trust information to the new node. c. The service control strategy. The higher reliability evaluation a node obtains, the better corresponding service quality they obtain. When R_{Aij} respectively belong to [0,0.2), [0.2, 0.4), [0.4, 0.6) ,[0.6, 0.8), [0.8, 1.0), the service quality obtained by nodes is "denial of service", "low-level service", "general service", "good service", "best service". At the same time, group managers will take a different strategy to punishment according to monitoring nodes' behavior and reputation in the group. When $R_{i}^{G_i}$ respectively belong to [0, $R_{ave}/3$],[$R_{ave}/3, 2R_{ave}/3$],[$2R_{ave}/3, 1$], for node punishment strategy, they are respectively "clear the node out of the group", "set silent time t, node can only provide services, do not request service", "no punitive actions".

The analysis of model versatility and expansibility.

a. A satisfaction evaluation r_{ij}^{n} and transaction amount S_{Qij} are associated with specific application. Evaluating a file download service in the file sharing, selecting the file quality, downloading bandwidth and popularity are evaluation standard. In e-commerce systems, we mainly consider the transaction duration, transaction costs, transaction important degree. We extract the different satisfaction evaluation factors in different P2P application and calculate r_{ij}^{n}, S_{Qij} is defined as the size of the transaction.

b. In the $< r_{ij}^{n}, t^{n}, m >$ evaluation information, the content of the m field is the extended trust data. With the unceasing change of P2P application requirements, record the related factors of new trust evaluation in the m field. Finally, the model has certain extensibility.

THE RESULTS OF SIMULATION AND ANALYSIS

The simulation environment. In this paper, the application of scenarios is file sharing. Based on the P2P research group in Stanford, Query Cycle Simulator has accomplished some classical trust model. Such as: Eigen Trus; Cup-pens; Trust Frame. In the network nodes are divided into three categories: good nodes, evil and bad meaning node. Goodwill node refers to the services or the evaluation of other nodes is reliable. Malicious nodes behavior mainly include: provide low level service; offer unreal evaluation; vilified goodwill node and exaggerate the same node. Whitewashing and Freeriding node is divided into bad behavior.

The results of simulation and analysis. a. Request success rate. Request success rate is the number of successful download goodwill node ratio of all downloads. It reflects the trust models application effect intuitively. Trust Frame, Cuppens model、Eigen Trust、Random successful request rate comparison is shown in figure 1.

Curve of 4 Random refers to the model does not use any trust mechanism. Each node selected download resources randomly. Figure 4 illustrates when the malicious nodes up to 50%,TrustFrame still has high success rate of requests. This is due to Trust Frame's aging time、the degree of similarity node enhanced the accuracy of the trusted computing. At the same time the implementation of service control strategy for penalizing and motivation node.

b. The inhibition of bad nodes. The dynamic adjustment of new node initial trust must be a cost for Whitewashing nodes in the replacement of identity to join the network. At the same time, we limit the impact in the group. The node is punished by service control strategy for Freeriding. They have been reduced for the quality of the service or removed groups. The cooperation level of bad node is the ratio between the successful upload file size of all bad nodes and the successful download file size. The proportion of bad nodes is 40%. The simulation results are shown in figure 2.

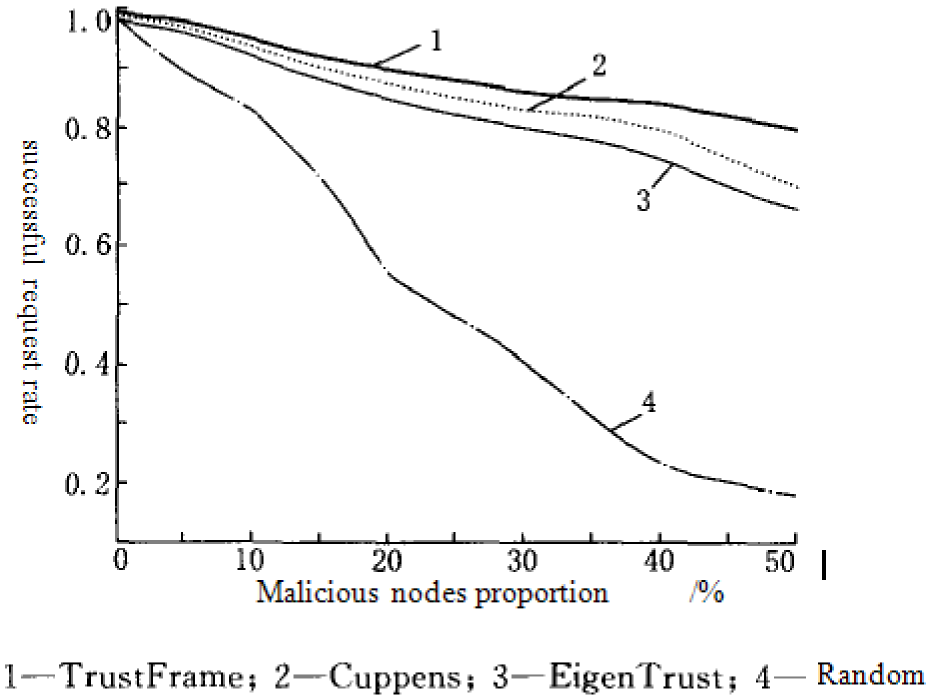

Figure 1: The successful request rate of the different size malicious nodes

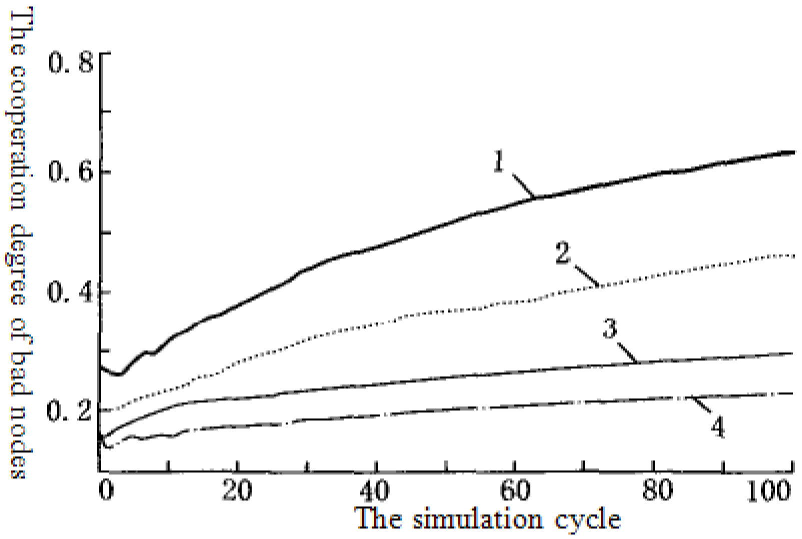

Figure 2: The inhibition of bad nodes

The inhibitory effect is more obvious for bad nodes in Trust Frame, the cooperation degree tend to be more reasonable.

c. The system overhead. The system overhead is measured by network traffic in the process of trust mechanism running. It includes all the query request, response message, connection information and so on. The network traffic is shown in figure 3 when well-meaning node successfully downloaded more than 90% in the different network scales.

Trust Frame, Cuppens and Eigen Trust network traffic difference is not big when network size is small. But as the network scale increase, Eigen Trust network traffic increase rapidly based on the global trust information collection. Compared with Cuppens model, Trust Frame node distribute in the group according to the interest of property. Considered the relationship between individuals and groups, groups and group, communication load are mainly distributed in smaller groups. Based on the aging time remove invalid information, it can effectively reduce the system overhead.

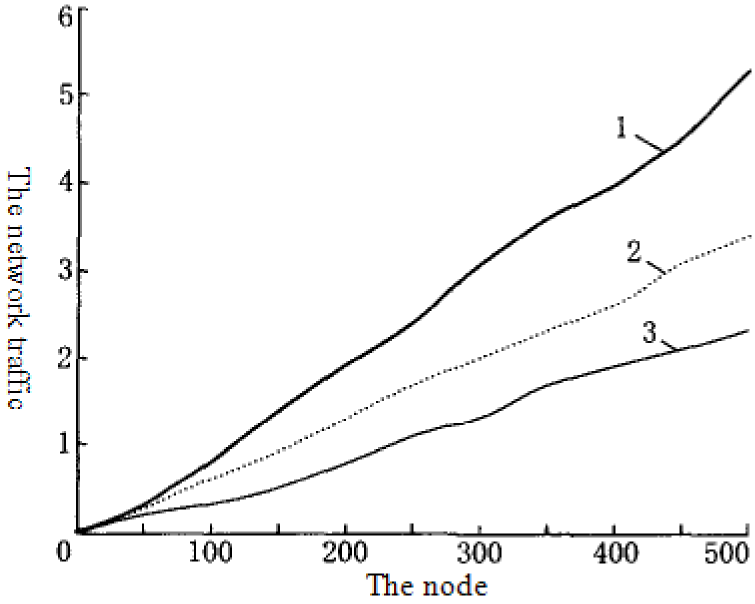

Figure 3: The network traffic contrast

CONCLUSION

This paper proposes a trust management model based on group. The calculation results of general trust in the model consider the node trust directly; trust in the group; trust between groups. And introduces the feedback credibility factor and multiple weighting factor to adjust trust. So the model can adapt to a variety of network environment. The simulation shows that this model can effectively inhibit a variety of malicious behavior, improve the success rate of interaction.

REFERENCES

[1]Liu Xiao-lan. *China Sport Science and Technology*. **1984**, 29(13), 46-49.
[2]Luo Yang-chun. *Journal of Shanghai Physical Education Institute*. **1994**, 23(12), 46-47.
[3]Wan Hua-zhe. *journal Of Nanchang Junior Colle*ge. **2010**, 3, 154-156.
[4]Li Ke. *Journal of Shenyang Sport University.* **2012**, 31(2), 111-113.
[5]Zhang Shu-xue. *Journal of Nanjing Institute of Physical Education*. **1995**, 31(2), 25-27.
[6]Pan Li. *Journal of nanjing institute of physical education(natural science).* **2004**, 19(1), 54-55.
[7]Li Yu-he; Ling Wen-tao. *Journal of Guangzhou Physical Education Institute*. **1997**, 17(3), 27-31.
[8] Xu Guo-qin. *Journal Of Hebei Institute Of Physical Education*. **2008**, 22(2), 70-72.