Research on the Trust Evaluation Mechanism in P2P E-commerce

Bingwen Yan, Rongrui Yu

Department of Management, Yango University, Fuzhou City, Fujian Province, China

sunshineybw@163.com; 13277844@qq.com

Keywords: P2P; E-commerce; Hash function; trust model; evaluation mechanism

Abstract: To solve the P2P E-commerce security problem effectively, on the basis of researching the trust model deeply in the P2P E-commerce, a method based on hash function is proposed to put the node from the trust group into the sub-group in a random. It reduces the risk of collusion attack. When a node provides a malicious service occasionally, it cannot be proved to be a malicious node, and it only needs to be given a warning. Transaction time factors, transaction scales, and transactions number are introduced to calculate the trust value. Penalty item is used to limit node to provide malicious service. It is more accurate to estimate the trust value. The model relies heavily on nodes from the group connected with outside group and the nodes from the same group, and it ensures the performance of the network.

1. Introduction

Compared with the traditional e-commerce model, P2P e-commerce has the following features. the risk of transactions is large, the transaction parties are mostly anonymous, there is no central certification administration rely on, and each individual has uncertainty and highly dynamics (Guha, 2004. The lack of trust and constraint mechanism between the transaction nodes is the main reason for restricting developments of P2P e-commerce (Can, 2010). Therefore, solving the transaction security in the P2P environment has become an urgent task for the development of e-commerce. Yao Wang proposed a trust model based on Bayesian network, which consists of two parts: trust mechanism and reputation mechanism (Yao, 2003. The trust mechanism deals with direct trust, and reputation mechanism is used to deal with recommendation trust. Because the trust model is too dependent on experience and has high reliability to experience requirements, the subjectivity is strong. In the daily e-commerce service, expert experience is generally difficult to obtain, and its accuracy can not be ensured as well. Therefore, the model based on Bayesian network is limited in practical applications. Qiaozhi Xu proposed Trust Group trust model (TGTM), separating the network into 3 groups: Good, Φ and bad (Qiaozhi, 2006). However, this model might causes collusion attack in practice. In addition, if a node occasionally provides malicious services, it can not prove that the node is a malicious node, but may be the fault of the node, and then it is not appropriate to do any transaction with the node.

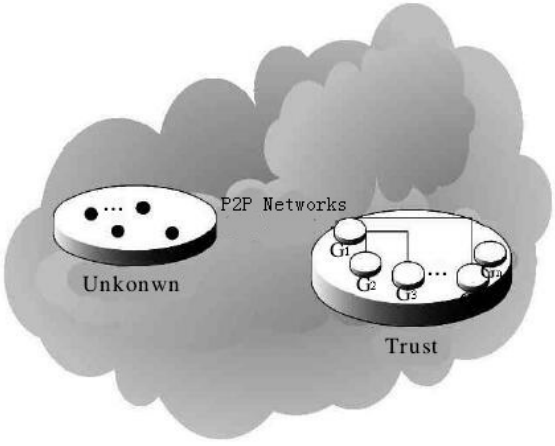

Figure 1 Unknown-trust network model

Aiming at the collusion attack problem, the network model is utilized as shown in Figure 1, and the Hash function is used to select the group that the nodes need to join. In e-commerce transactions, a node providing a malicious service can re trade after a period of time. However, once the node provides multiple malicious services, the node can not deal with the nodes in the trust group.

The P2P network is divided into two sets: Trust and Unknown sets. Here, NETWORK=Trust∪ Unknown, and Trust∩Unknown=Φ. The trust group can be subdivided into n subgroups G_1-G_n. Inner connection refers to the connection among nodes in a group, and outer connection refers to the connection between different groups. Group size refers to the maximum number of nodes that a group can hold, and is represented by G. Outer connection number means the maximum number of external connections that a group can maintain, and is represented by K.

The group size of the subgroups G_1-G_n is G, and each node maintains an inner connection to each other, as shown in Figure 2.

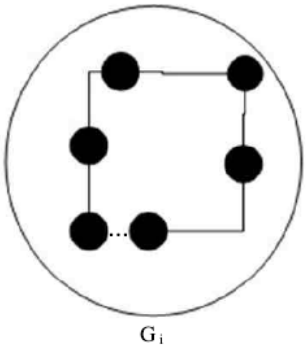

Figure 2 The structure of Gi in trust group

Each subgroup has a super node, and the super node maintains the inner connection between each node in the subgroup and maintains the K outer connections. The super node can allow and deny other nodes to join the group, and notify the current network environment to the newly added nodes, and notify the remaining nodes in the group and update the transaction information table when the node leaves the group. The super node stores a transaction information table, as shown in Table 1. Nid refers to the node in subgroups, Tid refers to the transaction information of nodes, Tsize refers to the transaction date, and Ttime refers to the transaction time.

Table 1 The transaction information table

Gid	Gsize	Nid	Tid	Tsize	Ttime

The ID of nodes in the group is unique. Each node maintains a node information table, as shown in Table 2. Where Tid is used to store the already traded node information, TrustData is used to store the trust value of the transaction node, and UnTrust is used to store the malicious node information.

Table 2 The transaction information table

Tid	TrustData	Gsize	Tsize	Ttime	Untrust

2. Participation and Elimination of Nodes

2.1 Participation of Nodes

When a new node has just been added to the P2P network, the trust value of this node is 0, and it is added to the Unknown set. At the same time, the node can improve its trust value by transaction (Mujtaba, 2004). When the trust value of the node reaches the threshold of trust, that is R_t, the node will be added to the trust group. If a node provides a malicious service, then the trust value of node

will be lower than the threshold, added to the unknown group (Qian, 2006). At this time, the node can only be traded with the nodes in the unknown group, When the node trust value again reaches the trust threshold R_t, it must wait $\triangle T$ before they can re-adding to the trust group, which can be a warning to malicious nodes. If the node provides malicious services n times, the node need to wait at least $\triangle T^n$ to re-join the trust group. For instance, the node A provides malicious services, $\triangle T=30d$. If A provides only one malicious service, the node can not trade with trust nodes within 30d. Obviously, if the node A provides malicious service n times, it cannot not trade with other nodes until 30^n day, which means the node A can no longer be traded with trust nodes. Each node in the group must maintain a node information table, which can be used to store transaction information and malicious node information.

For instance, initial condition: $A \in$ unknown. When $R_a \geq R_t$, A joins in the trust group, and conduct the following works.

(1) If hash(a)=i;

(2) A sends a join request to the G_i. If there are no other nodes, the node A is added to the G_i and is used as the super node of the group;

(3) If other nodes already exist in G_i, then calculate (G_i). if calculate(G_i)=G, turns step (4), otherwise turns step (5);

(4) If G_i refuses to join of A, A sends a join request to the G_{i+1}. If there are no other nodes, the node A is added to the G_{i+1} and is used as the super node of the group;

(5) If the super node allows A to join, the node A joins the group G_i, and compares the trust value with other nodes in the group, and then the node with high trust value is the super node of G_i; If the super node refuses the request information of A, turn step (6);

(6) A sends a join request to G_{i+1}, and calculate (G_{i+1}). If calculate(G_{i+1})=G, G_{i+1} refuses the join of A, turns step (8), otherwise turns step (7);

(7) If there are no nodes in G_{i+1}, the node A joins the group G_{i+1},and is used as the super node of the group; If the super node in G_{i+1} refuses the join of A, turns step (8);

(8) A sends a join request to G_{i+2}, and repeat the above steps;

(9) When the number of nodes reaches G in each group, no more nodes are allowed to jont;

(10) End.

In e-commerce activities, multiple nodes in the same group can easily perform joint fraud or dynamic swing. Through the hash function to determine the entrance of nodes, the dynamic swing and joint fraud can be effectively avoided to prevent the collusion phenomena.

2.2 Elimination of Groups

The elimination of group is based on the belief that there is no node in the group as the basis of elimination (Baoyu, 2013). When a node wants to quit the group at the end of the transaction, it sends the leave request to the super node to indicate its leaving determination. After receiving the request, the super node notifies other nodes in the group and updates the node information table. Once nodes conduct dishonest transactions and malicious service, the trust value of node will be reduced. when the trust values of nodes below the threshold, the node will be deported to the unknown group. In addition, the super node updates transaction information table, and the malicious node is added to the blacklist. At the same time, this information would be conveyed to other nodes using flood mode, and then each node updates its information table.

When the last nod exits the group, it means that the group is extinct.

3. Trust Evaluation Mechanism

Abhilash Gummadi defines trust values between [-1, +1]. This paper utilized this method, by which the trust value below 0 means incredible (Abhilash, 2004). In addition, the higher trust value, the more credible.

3.1 Calculation of Trust Value

For one node, the nodes related to it are mainly the nodes in the group and the nodes that are connected with the group. These nodes constitute the network topology T, as shown in Figure 3.

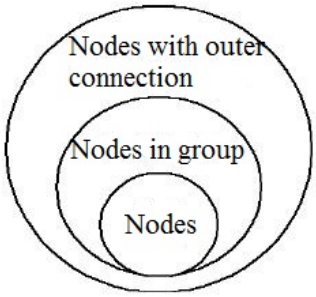

Figure 3 The network topology T of nodes

Before e-commerce, the more knowledge of the transaction entity, the greater the probability of success of the transaction. According to the characteristics of e-commerce, four parameters are introduced when calculating the trust value of node.

(1) Transaction time; (2) Transaction size; (3) Transaction number and (4) Penalty.

3.2 Measurement of Trust Value

For a node S, it first sets the trust threshold of its transaction, and when the trust value of target nodes reaches this threshold can carry out the transaction. In addition, S checks the history of its transaction. If it has ever been traded with the target node, the node checks and calculates whether the trust value of node d has reached the transaction threshold, and then deals with the transaction if the threshold is reached. If the threshold is not reached, the node s sends the consultation to nodes in the group and K groups which are connected with the group.

$$TrustData_d = \left(\begin{array}{l} \alpha \times value \times T_i + \dfrac{\beta \times \sum_{i=1}^{n} \left(LtrustData_i \times W_i \right) \times T_j}{n} \\ + \dfrac{\delta \times \sum_{i=1}^{m} \left(GtrustData_j \times W_j \right) \times T_k}{m} \end{array} \right) \times T_{count} + F \quad (1)$$

α, β, δ refer to weight value. $TrustData_i$ is the trust value of node d; *value* is the direct trust value of node; $LtrustData_i$ is the feedback of trust value in groups; *Gtrustvalue* is the feedback of trust value in other groups; T is the transaction time index; T_{count} is the transaction number index and F is the penalty.

4. Simulation and Analysis

The simulation is used to verify the validity and accuracy of improved trust model. In order to compare the performance of this model, this paper also verified the traditional trust model. The number of nodes in the simulation was 1000, 2000, 3000 and 5000. trust group was divided into 10 groups, and α, β and δ were respectively 0.5, 0.3 and 0.2. Among them, the proportion of malicious nodes was 10%~30%, K was 5. At last, the performance of the improved TGTM is verified and compared with the traditional trust model.

4.1 Network Performance

The impact on network performance mainly from the data request and response. In the improved trust model, the increase of node number has little influence on network performance, as well as the alternation of node number, which indicates the system has a good scalability. At the same time, the alternation of node number has a great impact on network performance in traditional trust model, as shown in Figure 4.

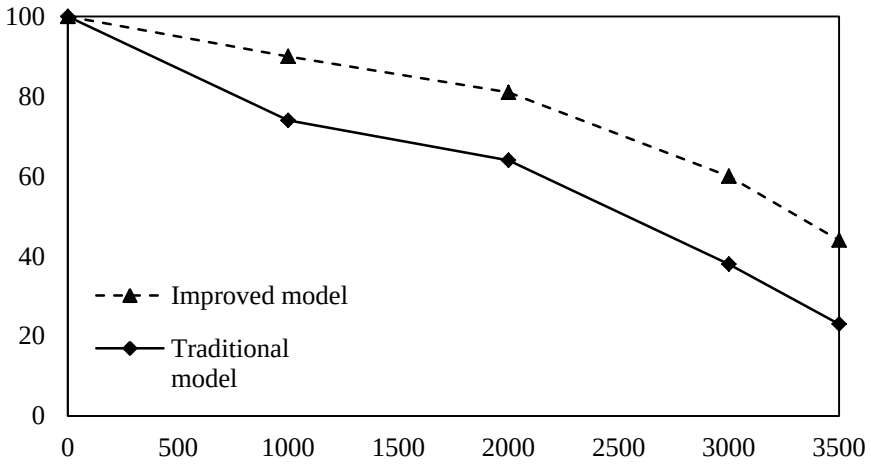

Figure 4: The network performance of improved model and traditional model

4.2 Transaction Success Rate

The traditional trust model collects the trust value of all nodes to calculate the trust value of the node, so that the amount of information is large, and the trust value is relatively accurate. Since the improved model is based on the group, the information it collects is not from all nodes, but related to the node when transaction is started. Therefore, the amount of information obtained by improved model is far less than the traditional trust model, and the success rate of transaction is relatively low. However, the improved model will be in a relatively stable state during transaction, as shown in Figure 5.

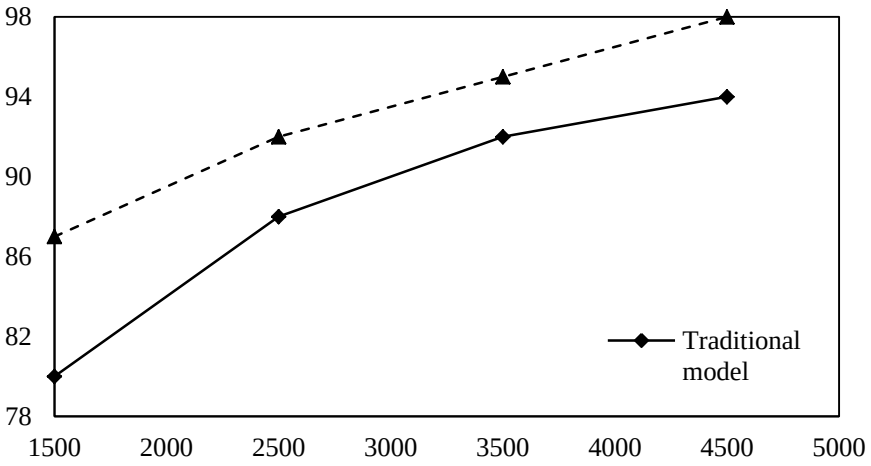

Figure 5 The transaction success rate of improved model and traditional model

4.3 Collusion Resistance

In the process of e-commence transaction, there are often some nodes collude with each other, give other nodes a higher trust value and exist dynamic swing. In the improved model, the nodes join groups to be determined by hash function, and the nodes cannot determine the group they want to join, which has a great randomness. Therefore, this model prevent the collusion of nodes to a great extent, as shown in Figure 6.

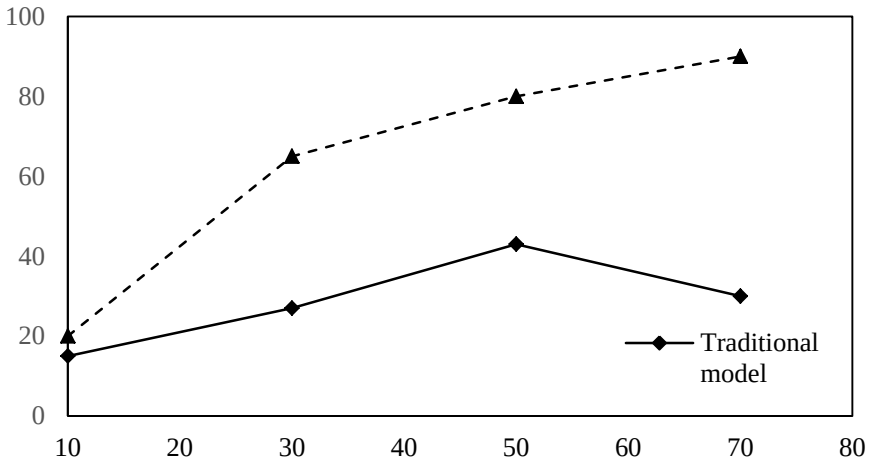

Figure 6 The collusion resistance of improved model and traditional model

5. Conclusion

E-commerce is a revolution in the field of circulation, and e-commerce in P2P environment is the future of e-commerce. The trust model promotes the development of e-commerce. On the basis of analyzing the traditional trust model, the TGTM is improved, and the Hash function is used to determine the nodes to join, and the fault of nodes is taken into account as well. compared with the traditional trust model, the improved trust model is in a relatively stable state, the transaction success rate of is not too large, and the network performance and collusion resistance appear a further improvement. The future research is to further improve the credibility of trust value, improve the success rate of transactions, reduce the risk of user transactions.

References

[1] Abhilash, G., Jong P., 2004. Model in group trust for peer-to-peer access control, *Proc of 15th International Workshop on Database and Expert System Applications*,.

[2] Baoyu, Wang, Chengshi, Gao, Qing, Dai, 2013. Research on Trust Evaluation Model in P2P E-commerce, Computer Application and Software. (12), pp.3067-3069.

[3] Can, Chen, Fengsong, Hu, Huijuan, Wang, 2010. Improved reputation-based trust model in P2P environments, Computer Engineering and Design. 31(5), pp.999-1001.

[4] Guha, R., Kumar, R., Raghavan P., 2004. Propagation of trust and distrust, WWW2004.

[5] Mujtaba, K., Partha D., Kyung D., 2004. A role-based trust model for peer-to-peer communities and dynamic coalitions, Proceedings of Second IEEE International Conference on Information Assurance Workshop.

[6] Qiaozhi Xu, Dongsheng, Liu, 2006. A Trust Model Used in P2P Electronic Commerce, Computer Engineering and Application. 42(21), pp.134-138.

[7] Qian, Wang, Jinjun Du, 2006. A Security -Trust Model for P2P E-Commerce, Computer Science. 33(9), pp.54-57.

[8] Yao, W., Julita, V., 2003. Bayesian network-based trust model, Proceedings of the IEEE/WIC International Conference on Web Intelligence.