An Improved Trust Mechanism Based on the Similarity

Daoquan Li[1, a], Ruimin Guo[2, b]

[1]College of Computer Engineering, Qingdao Technological University, Qingdao, 266033, China

[2]College of Computer Engineering, Qingdao Technological University, Qingdao, 266033, China

[a]email: lidaoquan@sina.com, [b]email: 2439875915@qq.com

Keywords: Trust; Similarity; Direct trust; indirect trust; Comprehensive trust

Abstract. Aiming to the trust of C2Cnetwork, indirect trust is introduced when direct trust value is lower. On this basis, the comprehensive trust value is calculated which is used to select trading node. The satisfaction factor, transaction size, transaction time, transaction frequency and other factors are taken into account to calculate the direct trust; the user similarity based on multi-evaluation is introduced to calculate the indirect trust, at last the calculation method of comprehensive trust based on user similarity is given. Simulation results show that, the model give in this paper can effectively control the malicious node recommendation, prevent fraud reputation in a certain extent, and effectively reduce the calculation error of the trust value.

1. Introduction

In recent years, the electronic commerce has also received more and more attention with network development; it's convenient and fast characteristics make more and more people to participate in it. However, as a new business model, because of the characteristics of network openness, dynamic, anonymity and geographic location, it is difficult to obtain the trust value of the two parties, so the quality and information description of goods may not match their actual things, after-sale service is not good, and there are identity fraud, conspiracy fraud, false information and so on. The existence of a large number of unknown entities in the network also increased the difficulty of solving the problem. Therefore, the research on the relationship between the buyer and the seller has become a hot issue in the field of electronic commerce.

In order to choose a reliable transaction object, the buyer can establish a perfect relationship under ideal situation, but it is difficult to achieve the ideal situation in the actual network. In order to ensure the security of the transaction, choosing a relatively high credibility entity to carry out the transaction is our current problem to be solved.

The concept of trust management is proposed by M.Blaze et al. In 1996, the scholars at home and abroad have studied the trust value under different scenarios. A multi-dimension trust management mechanism is proposed in the literature References [1], and the evaluation method of direct and indirect trust is used to measure the credibility of the user in the system. But this model consider only the impact of time on the direct trust, the transaction amount, transaction frequency and other factors are not considered, so the buyer may likely use small transactions to generate a larger trust value, then the buyer implement fraud transactions in large amount. A similarity based trust recommendation model is proposed in this paper [2], which considers that the two users have a high similarity in behavior, then the two sides can get a greater trust value, but ignoring the user's evaluation of the differences in the various dimensions will result in inconsistent with the actual situation, this will also cause indirect trust value is wrong. The paper [3] proposed a model which introduces the penalty of the malicious behavior of the malicious nodes, while the penalty is not considered in the model EigenTrust. The influence factors are also introduced in the model, so that the comprehensive trust value is more objective. Paper [4] gives a kind of model which can get rid of the collusion attack by setting trusted nodes. But due to the choice of trusted nodes is subjective, it cannot guarantee the node is a trusted node forever, once the trusted nodes change to be malicious node, this will produce significant security vulnerabilities. The paper [5] proposed a trust model based on similarity weighted recommendation, and modified the comprehensive trust value using

cosine similarity with each dimension, but using the traditional cosine similarity function to calculate the similarity of each node is not reasonable.

From the above, we can see that there are many problems in the practical application of the trust mechanism:

(1) Trust value directly affects the seller's trust. In the actual situation, the trust value can change with many factors, such as trading time, transaction amount, the number of transactions, which leads to the calculation of the trust value is relatively complex, and there is no one mechanism to accurately calculate.
(2) Trust mechanism is used in a specific application scenario, and the calculated comprehensive trust value is not sure to represent the real business of trust value.
(3) Some malicious transaction nodes can be suspected by using some schemes of trust mechanism, but it cannot guarantee its accuracy. As a result, the trust value may be wrong.

Based on the traditional multi-dimension trust management mechanism, this paper proposes a new method to calculate user similarity, and considers many factors, and discusses the direct trust, indirect trust and comprehensive trust. The model can effectively control the malicious node recommendation, prevent fraud reputation in a certain extent, and effectively reduce the calculation error of the trust value.

2. Trust management based on similarity

2.1 Trust management

The trust relationship of nodes in P2P network can be divided into two categories: direct trust and indirect trust. Direct trust means that there is a direct transaction between two nodes, when transaction is completed again, you can directly obtain the trust value of each other by the previous transaction. It can be represented as DT. Indirect trust, also known as the recommendation trust, it is built between two nodes which have no direct transaction. The trust value among them is the result of the evaluation of their common neighbor users. It can be represented as RT [6].

The basic idea of the trust mechanism of e-commerce based on the similarity is as follow:

The trust threshold is set for each node at the beginning, which is the minimum of the transaction. First, when node a wants to makes a transaction with b, trust mechanism will get the history of direct transaction between a and b, then calculate the direct trust value DT. If DT is bigger than trust threshold, then the comprehensive trust value is equal to the DT. If DT is less than the trust threshold, the trust mechanism can obtain the transaction information of the node b, and then calculate the indirect trust value through the other nodes which have transaction with node b, and finally calculate the comprehensive trust value using direct trust value and indirect trust value.

In the process of calculating the indirect trust, the trust degree of the trading nodes is calculated according to the different dimensions of the trading nodes. In addition, the transaction amount, transaction time, transaction frequency, penalty factor and other factors are also considered, so the trust mechanism has a stronger transaction security [7].

In this paper, the trust management mechanism based on the similarity is as follows:

$$T_{\mathrm{ab}} = \begin{cases} DT_{ab} & DT_{ab} > T_{th} \\ \alpha DT_{ab} + (1-\alpha) RT_{ab} & DT_{ab} \le T_{th} \end{cases} \tag{1}$$

Here, T_{ab} is the final trust evaluation of the node b to node a, DT_{ab} is the direct trust evaluation value of node a to node b, RT_{ab} is the indirect trust evaluation value of node a to node b, α is the weight factor, the greater of α, the larger of direct trust value is, the proportion of indirect trust is smaller, and vice versa. T_{th} is the threshold of transaction. Relative to the indirect trust, buyers will be more inclined to trust evaluation based on the direct experience of buyers, therefore, when DT_{ab} is greater than T_{th}, then buyers can make a trade with seller.

2.2 Direct trust

In the trust network， node a can evaluate node b by making transaction with b, thus the direct trust value of b to a is calculated. Direct trust value is a kind of assessment of the future

behavior of the two parties, the transaction size, transaction frequency and the risk of the transaction, with the increasing in the size of the transaction, the trust relationship between the two parties will be more clear.

(1) Satisfaction degree

Node a and node b make their $k-th$ direct transaction, a will give the evaluation of b, when transaction is satisfied, then evaluation is equal to 1, otherwise, evaluation is equal to 0. So the satisfaction degree $ST^{(k)}$ after $k-th$ direct transaction is as follows:

$$ST^{(k)} = \begin{cases} 1 & satisfaction \\ 0 & unsatisfaction \end{cases} \tag{2}$$

Obviously, satisfaction is as an important factor to calculate the direct trust, the unsatisfied transaction is not included in the calculation of direct trust, reducing the calculation of the value of the trust.

(2) Time factor

With the change of time, the degree of trust between buyers and sellers will change the closer the current time of the transaction, the more able to reflect the recent behavior, the more valuable, in contrast, the transaction of the most distant from the current time should be ignored. Therefore, the trust value changes with the decay of time. The following principle in the calculation of trust value should be used; the closer the time is far from current time, the bigger the weight in the trust value, and vice versa [7]. In this paper, the experimental model of time factor is as follows:

$$T^{(k)} = \begin{cases} 1 & NT\text{-}Time \le TM \\ e^{-(\frac{NT\text{-}Time}{t})} & NT-Time > TM \end{cases} \tag{3}$$

Here, NT represents the current time, $Time$ represents the $k-th$ trading time, TM is a threshold, within the threshold time, trust value of buyers to sellers does not change; if $NT-Time>TM$,trust value will attenuate according to the attenuation function .

(3) Transaction amount factor

The size of the transaction amount in the trust also plays an important role; it can reflect the importance of this transaction. The greater the amount of the transaction, the more credible the credibility, in contrast, the smaller the amount, the credibility will be smaller in the overall trust. The introduction of transaction amount factor is aim to prevent the user to obtain higher credit value in large transactions for fraud by using small transactions. Therefore, the evaluation of large transactions can reflect the entity's transaction behavior. When considering the amount factor, the effect of the small trade on the comprehensive trust value must be decreased, and the function of the large trade should be improved. In summary, the formula to calculate the transaction amount factors are as follows:

$$M^{(k)} = \begin{cases} 1 & p \ge p_0 \\ -\log\frac{p}{p_0} & p < p_0 \end{cases} \tag{4}$$

Here, p represents the price of the current transaction, and p_0 represents the largest trading amount in historical transactions.

(4) Transaction frequency factor

It is generally considered that the two nodes make many transactions in a period of time, the credibility of the two nodes is higher, but this may cause that reputation can be improved rapidly by using many times transactions during a short period of time , resulting in trading risk. In order to effectively reduce the cumulative effect of several transactions over a period of time, so the transaction frequency factor is introduced. The formula for calculating trading frequency factor is as follows:

$$C^{(k)} = \frac{n}{N} e^{-\left(n+\frac{1}{2}\right)} \tag{5}$$

here, n represents the total number of transactions between the two nodes, N represents the

number of nodes of all transactions, $e^{-\left(n+\frac{1}{2}\right)}$ represents the adjustment factor.

(5) Adjustment factor

γ is the adjustment factor, it means the credibility of the evaluation of this transaction, which can effectively avoid the malicious node's recommendation. The calculation formula of the adjustment factor is as follows:

$$\gamma = \frac{n_s}{N_a} \tag{6}$$

Here， n_s represents the number of successful transactions, N_a represents the total number of transactions.

(6) Penalty factor

The penalty factor is mainly used to encourage honest users, to punish some dishonest users, to achieve the establishment of a standardized, secure electronic commerce transaction environment, reduce the failure rate of transactions. The calculation formula of the penalty factor is as follows:

$$F = f(n) \times e^{\frac{Q}{3}-0.9} \tag{7}$$

$$f(n) = \begin{cases} -1 & n-th\ transaction\ is\ fraudulent \\ 0 & n-th\ transaction\ is\ honest \end{cases} \tag{8}$$

And here, $e^{\frac{Q}{3}-0.9}$ is the acceleration factor, Q is the number of fraudulent transactions of user to carry out, with the increasing in the number of fraudulent transactions, the acceleration factor will make the trust value reduce rapidly, to achieve the purpose of rapid drop.

Based on the above considerations, the calculation method of the direct trust value is defined as:

$$DT_{ab} = \sum_{k=1}^{N} ST^{(k)} \times T^{(k)} \times M^{(k)} \times C^{(k)} \times \gamma + F \tag{9}$$

2.3 indirect trusts

Indirect trust is the most important content in the trust evaluation mechanism, because there are a certain unpredictable characteristics of indirect trust, So it needs to be considered from multiple angles to minimize the probability of the user being cheated.

The indirect trust of a node is related to the following factors: the number of nodes which has trade with him, the evaluation given by other nodes, the similarity between the buyer nodes and the seller nodes, the transaction amount, transaction time, and the transaction frequency.

The similarity of user evaluation reflects the trust degree of the evaluation given by nodes. If there is no direct transaction between the two sides, the trust value can only rely on the evaluation of other nodes, which are used to calculate the indirect trust. If a node makes a malicious evaluation, it has a great impact on the comprehensive trust value, which is not conducive to the success of the transaction. So, the similarity is very important in calculating the comprehensive trust value. It is generally considered that the two users have a high similarity in behavior, they are more likely to trust each other, and the model of the user similarity given in this paper is an important factor in the indirect trust, making the indirect trust has a very strong reliability [8].

Cosine similarity is often used to judge the similarity of the user, as shown in Figure 1. Because user's data are difficult to collect, in this paper, we calculate user similarity using user ratings for the following five dimensions: the quality of the products (o_1), the price of the products (o_2), picking speed (o_3), service attitude (o_4), information of goods (o_5) ([9]).

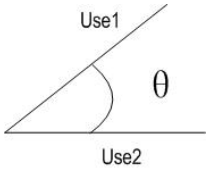

Figure 1 Vector angle

Similarity calculation formula between user a and b is as follows:

$$sim\_\cos(a,b)=\frac{\sum_{m\in D'}\left(f\left(o_{i(am)}\right)-E\right)\times\left(f\left(o_{i(bm)}\right)-E\right)}{\left(\sum_{m\in D'}\left(f\left(o_{i(am)}\right)-E\right)^2\times\sum_{m\in D'}\left(f\left(o_{i(bm)}\right)-E\right)^2\right)^{\frac{1}{2}}} \tag{10}$$

$$E=\frac{\sum_{i=1}^{n}f(o_i)}{n} \tag{11}$$

a and b represent user a and b, E represents average user ratings, $f(o_i)$ represents the user's rating on O_i, N represents the dimension of evaluation, $sim\_\cos(a,b)$ represents the similarity of user a and b, $m\in D'$ represents user set in which has common transaction with user a and b.

Introducing the time factor, transaction size factor, transaction frequency factor, we can give the following formula for the calculation of indirect trade.

$$RT_{ab}=T_m\times C_m\times M_m\times sim\_\cos(a,b)\times DT_{mb} \tag{12}$$

Here, The scope of action of T_m、T_m、M_m are only in $m\in D'$.

2.4 comprehensive trusts

Comprehensive trust can be calculated using the direct trust and indirect trust, which is used to determine make transaction or not. Computational methods are as follows (This model is named as comprehensive trust based on similarity, CTBS):

$$T=\alpha DT+(1-\alpha)RT \tag{13}$$

Here, α is confidence factor, $0\le\alpha\le1$, α express confidence level in their own judgment, the formula does not only consider their own experience, but also consider the recommendation of other nodes within the network, which is in line with the actual situation. Confidence factor is determined by its own trading experience, the formula is as follows:

$$\alpha=\begin{cases}0 & n=0\\ \frac{n}{N} & n>0\end{cases} \tag{14}$$

Among them, n represents the number of successful transactions; N represents the total number of transactions.

3. Experimental results and analysis

In this paper, the proposed trust model (named as CTBS) is simulated. In order to verify the accuracy of the model, the PeerTrust and EigenTrust models are added to the simulation experiments. The experimental results of the three models are compared in the same scene.

Figure 2 shows the impact of the transaction frequency on the merchant's comprehensive trust value. In EigenTrust model, the proportion of direct trust is just simply growing with increasing of the transactions times, and the accuracy of the recommendation node is not considered. In the PeerTrust model , the trust value is completely dependent on the indirect trust , the direct transaction experience of the two sides is not be considered, , which is the main effect of the trust; Later comprehensive trust value growth is not big, this is due to direct trust plays a major role, the proportion of indirect trust reduces. CTBS model not only considers the direct trust and indirect trust, but also considers the transaction time, transaction size, penalty factor, and the adjustment factor, which makes the node's trust value more close to the true value of trust.

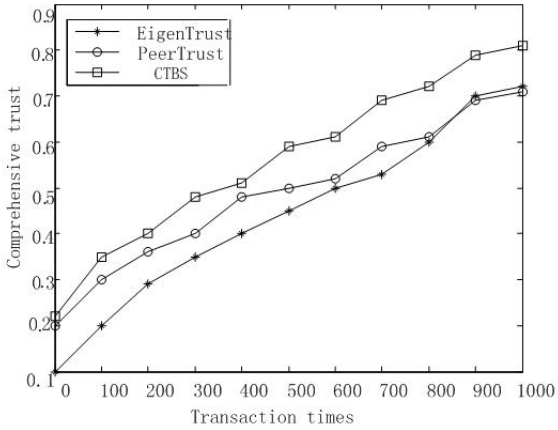

Figure 2 the influence of the number of transactions on the comprehensive trust value

Figure 3 shows the impact of the ratio of different malicious nodes on the success of the transaction. it shows that, with the increase of the proportion of malicious nodes, the success rate of the various models has declined, but because EigenTrust model does not make a certain punishment to malicious nodes to make some correction, when the proportion of malicious nodes increases to a certain proportion, the error rate is increased, resulting in a rapid decline in transaction success. EigenTrust is clearly not applicable when there are plenty of malicious nodes in the networks. In PeerTrust model, with the increase of the proportion of malicious nodes, the success rate of the transaction has not declined rapidly. Figure 3 shows that the model given in this paper has a higher success rate of the transaction, which proves that CTBS model can guarantee the security of the transaction in practical application, and it can protect interests of buyers in a large extent.

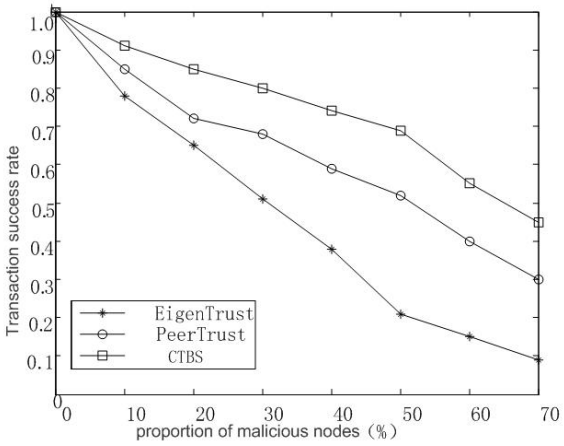

Figure 3 Transaction success rate under different proportion of malicious nodes

In Figure 4, the initial trust value is set to 0.5, with the increase in the number of nodes, the degree of trust will be gradually accumulated, when a malicious recommendation appears, , the node's trust follow the principle of "fast down" with introducing of the penalty factor , and then trust value will be cumulative through later multiple transactions. "Fast down" principle makes the cost of malicious recommendation greatly increase; the accumulated trust value will be wasted in vain, reducing the possibility of collusion.

4. Conclusions

This paper analyzes the existing trust mechanism, and describes a comprehensive trust model based on similarity. Taking into account various factors affecting trust value , and introducing the similarity algorithm, the model makes it more sensitive to calculate the similarity of user evaluation. When calculating the comprehensive trust value, the weight factor is introduced to

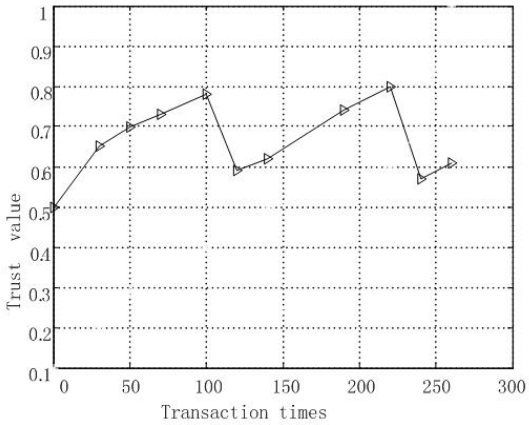

Figure 4 Changing curve of node trust value

measure direct trust value and indirect trust value, which makes the trust worthy of higher accuracy, the transaction success rate is significantly improved, the model can effectively prevents collusion attacks, malicious nodes recommended. When calculating the similarity of user's evaluation, the dimension of rating is more comprehensive, and it is also in accord with the actual situation. Compared with the original model, the model can improve the success rate of the transaction.

Acknowledgments

This research was financially supported by The Natural Science Foundation of Shandong Province, China. (Project No. ZR2011FL002).

Reference:

[1] ZHAO Yuan, LU Tianbo. Multi-dimensional trust management mechanism for peer-to-peer network [J]. Journal of Computer applications, 2014,34(11)：3157-3169

[2] DONG Xiao hua , ZHOU Yan hui, Similarity-based Trust Recommmended Model [J]. Computer Scince, 2013，40(10)：132-158

[3] LI Jun, XUEWei, GAN Xu yang. Improved Trust Mechanism Based on EigenRep Trust Model. [J]. Computer Scince, 2013，40(7):113-115

[4] Orsenigo C，Vercellis C．Kernel ridge regression for out-ofsample mapping in supervised manifold learning[J].Expert Systems with Applications， 2012，39(9) : 7757-7762．

[5] LI Jing-Tao, JING Yi-Nan, XIAO Xiao-Chun, WANG Xue-Ping, ZHANG Gen-Du. A Trust Model Based on Similarity-Weighted Recommendation for P2P Environments [J]. Journal of Software, 2007, 18(1):157−167

[6] Liu Qingyu, Ye Zhen,Zheng Liliang. Study on an Improved Trust Model [J]. Computer Application and Software, 2011，28 (3) ： 293-295

[7] ChANG Jun-sheng, WANG Huai-min,YIN GNAG. DyTrust: A Time-Frame Baed Dynamic Trust Model for P2P System[J]. Chinese Journal of Computer, 2006，29(8)：1301-1307

[8] Xu Feng-ling, Meng Xiang-wu, Wang Li-cai. A collaborative Filtering Recommendation Algorithm Based on Context Similarity for Mobile Users [J]. Journal of electronics and information Technology, 2011，33(11)：2785-2789

[9] GAN Cao-bin, DING Qian, LI Kai, XIAO Guo-qiang. Reputation –Based Multi-Dimensional Trust Algorithm[J]. Journal of Software, 2011，22(10)：2401-2411