International Journal of Smart Business and Technology
Vol.1, No.1 (2013), pp.49-58
http://dx.doi.org/10.21742/ijsbt.2013.1.1.05

Research on Trust Model of E-commerce in P2P Environment

Jianbang Du[1]

Innovative Transportation Institute, Texas Southern University, USA
dujianbang@gmail.com

Abstract

In the current e-commerce in the Peer-to-Peer (P2P) environment, security issues such as network fraud and network sway are repeatedly banned. Considering the influence of different transaction factors on the trust value of nodes, a penalty mechanism is introduced to prevent nodes from repeatedly performing malicious behaviors, and at the same time, reward factors are introduced to encourage honest transactions of nodes. The transaction limit was established and its relationship with the trust threshold was discussed. Based on the influence of multiple factors on trust value, this paper proposes a new trust evaluation model to make up for the deficiencies of some existing trust models. Experiments show that the trust model can effectively prevent malicious behaviors of nodes, has a good effect in resisting large-scale transaction attacks and swinging behaviors of oscillating nodes, and can reduce transaction risks.

Keywords: *Trust evaluation model, P2P network, Transaction restriction, Trust threshold*

1. Introduction

In e-commerce in the P2P environment, users have flexible and changeable communication and transaction modes, and each user node in the network may access each other and directly conduct transactions. However, due to its characteristics of openness, dynamics, anonymity, and non-centrality, there are a large number of fraudulent activities and low-quality services in transactions, which severely restrict the wide application and development of P2P systems. Therefore, how to implement an evaluation model that restricts malicious behaviors, encourages honest behaviors, and reduces transaction risks is of decisive significance for the application and development of P2P networks in e-commerce systems.

At present, many domestic and foreign scholars are devoted to the research of the trust model. For example, Mortera et al. 58 proposed a trust model based on a Bayesian network, which calculates the trust degree of nodes by statistically updating the probability density function and describes different aspects of trust to distinguish different preferences. However, this trust model lacks a corresponding penalty model and is not suitable for large-scale P2P environments. Hu et al, [2] proposed a trust model Peer Trust based on reputation. The model calculates the trust value of the entity by statistics and classification of the evaluation feedback received by the entity. The model believes that it is necessary to identify deceptive behaviors and punish the deceiver, but it does not propose a specific method and model. Kamvar [3] and others proposed the Eigen Trust model, which calculates the global trust value of nodes through trust query and detects malicious nodes through the calculation of recommended trust values. The trust value may even increase, which is unreasonable.

Article history:
Received (August 26, 2013), Review Result (September 30, 2013), Accepted (November 10, 2013)

Print ISSN: 2288-8969, eISSN: 2207-516X IJSBT

The existing trust model solves the security problem of e-commerce in the P2P environment to a certain extent, but some models [4][5] calculate the trust value of the node based on the number or probability of successful transactions, which is likely to cause malicious nodes to first Honesty in small transactions, and then deceive buyers in large transactions through accumulated reputation, and some models [6][7] are vulnerable to malicious attacks and collaborative cheating by nodes because they have no penalty mechanism. To solve the above problems, based on introducing transaction amount factors, reward factors, and punishment factors, and setting dynamic transaction limits based on past communication history, this paper proposes a new trust evaluation model. This article gives some related concepts as follows:

Definition 1 The empirical trust value $ET(i, j)$ refers to the degree of trust accumulated by the evaluation node i through direct transactions with the evaluated node j.

Definition 2 The recommended trust value $RT(i, j)$ refers to the degree of trust that node i obtains for the evaluated node j through feedback from the third-party node k (herein refers to the neighboring nodes that have had transactions with the evaluated node).

Definition 3 The comprehensive trust value $CT(i, j)$ is based on the empirical trust value and the recommended trust value and is comprehensively solved by a certain algorithm to express the trust value of the evaluated node.

Definition 4 Weight Generally, the importance of each factor that affects the trust value is different. To reflect the importance of each factor, each factor is assigned a corresponding weight, and each weight should meet the normalization and non-negative conditions.

2. Trust evaluation model

The basic idea of the model proposed in this article is that when a node receives a service provided by a node elsewhere, it will give a certain evaluation based on the transaction scale and service quality and establish a local trust evaluation table for the nodes that have a transaction history based on the transaction records. When one of the parties has malicious behavior, the other party will have corresponding losses. Therefore, before a node conducts a transaction with a node, it needs to first examine its trust level and determine the relationship between the trust level obtained and the transaction limit. Determine whether to trade with it. The trust evaluation model designed in this paper is shown in [Figure 1].

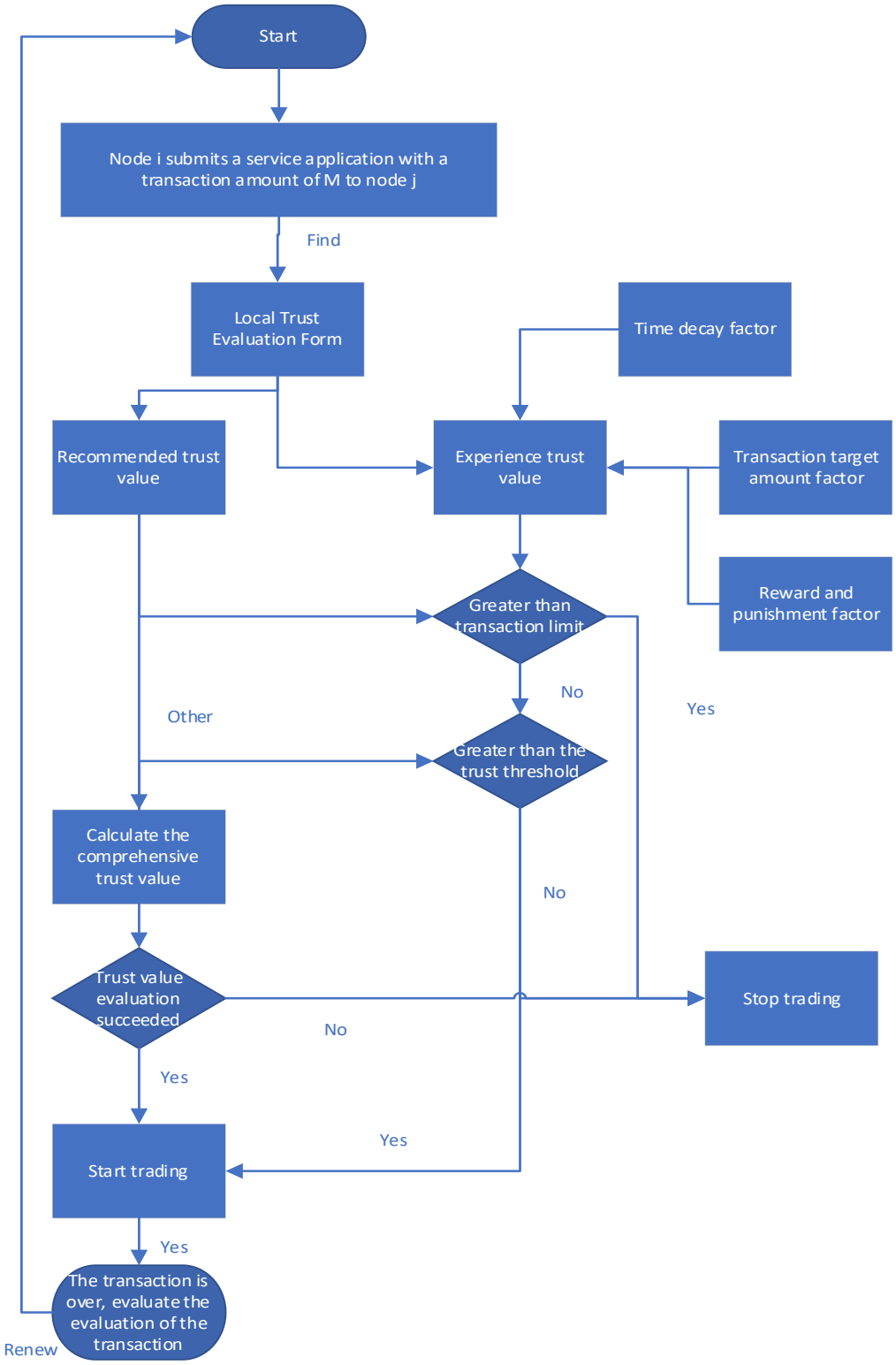

Figure 1 Trust evaluation model

It can be seen from [Figure 1] that the trust value of a node is composed of two parts: the empirical trust value and the recommended trust value. Among them, the empirical trust value must consider three influencing factors: one is the time attenuation factor. If there is no transaction with other nodes for a long time, the trust value will decrease. The second is the transaction amount factor. This article believes that the larger the transaction amount, the greater the impact on the trust value of the node. The third factor is rewards and punishments. This article believes that the more successful node transactions, the higher the trust value. Through the integration of these two trust values, the comprehensive trust value can be calculated.

Evaluate based on its comprehensive trust value. If the evaluation fails (that is, the obtained trust value is low), it shows that it is not suitable for trading. If the evaluation is successful (that is, the obtained comprehensive trust value meets the transaction standard), it means that the node can be traded. After the transaction is completed, the evaluation is performed and the local trust evaluation table is updated. The specific execution process is as follows:

(1) According to its own needs, node i submits to node j a service application with a transaction subject of M.

(2) Look up the empirical trust value with the node through the local trust evaluation table and get the most suitable transaction amount based on its historical transaction situation. If the transaction amount does not exceed its limit and the empirical trust value is greater than its trust threshold, choose direct transaction; If the limit is exceeded and the trust threshold is lower, the transaction is stopped; if the transaction amount does not exceed the limit and the empirical trust is lower than the trust threshold, or the limit is exceeded but the empirical trust is greater than the trust threshold, the neighbor needs to be inspected The recommended trust value of the node.

(3) According to the empirical trust value of the local node and the recommended trust value of other nodes, the comprehensive trust value of the transaction node is calculated.

(4) Perform trust evaluation based on the obtained comprehensive trust value to see if it is suitable for the transaction. If the transaction is completed, evaluate the transaction and update its local trust evaluation table.

3. Quantification of trust value

3.1. Experience trust value

Empirical trust is the subjective evaluation of the transaction behavior of target node j by node i based on the transaction records between itself and node j. This article chooses to use the continuous value [0,1] to represent the level of trust, where 0 represents complete distrust, 1 represents complete trust, mainly from the perspective of the number of transactions, transaction satisfaction, transaction scale, time decay, punishment, and rewards [8][9], to discuss the calculation method of empirical trust. At the current time t_n, the specific calculation formula of the empirical trust value of node j relative to node i is as follows:

$$ET(i,j) = \begin{cases} \dfrac{\sum_{s=1}^{n} ST_s(i,j) \times \tau_s \times \gamma_s}{n} \times (1-\lambda) \times (1+\theta) \\ 1 \end{cases} \quad (1)$$

Where $ST(i,j)$ is transaction satisfaction (also known as single transaction trust value): this is a subjective parameter, which means that after a transaction between node i and node j ends,

node i will give node j based on the transaction experience. The evaluation reflects the degree of satisfaction of the evaluation node to the evaluated node.

τ_s is the time attenuation factor:

$$\tau_s = \frac{1}{(t_n - t_s + 1)} \quad \tau_s \in (0,1) \tag{2}$$

Where t_n is the current transaction time, t_s is the s-th transaction time between node i and node j. In the actual transaction process, as time goes by, the trust between nodes is constantly changing. If the transaction time The closer it is to the current time, that is $(t_n - t_s) \to 0$, $\tau_s \to 1$, it means that the transaction records between nodes are fully remembered, which will have a greater impact on the trust value; on the contrary, if the transaction time is farther away from the current time, That is, when $(t_n - t_s) \to \infty$, $\tau_s \to 0$, the transaction history can be ignored, and the impact on the trust value is smaller.

γ_s is the transaction amount factor:

$$\gamma_s = \frac{M_s}{\frac{1}{n}\sum_{s=1}^{n} M_s} \tag{3}$$

Where n is the total number of transactions; M_s is the amount of the s transaction. It means that the importance of the transaction scale should be treated differently. The larger the transaction scale, the greater the impact on the trust value of the node. This can prevent some malicious nodes from increasing their trust value through small-scale successful transactions, and then cheating during large-scale transactions.

λ is the penalty factor:

$$\lambda = \begin{cases} 0 & p = 0 \\ \dfrac{1}{1 + e^{1-p}} & p \geqslant 1 \end{cases} \tag{4}$$

Where p is the number of transaction failures (fraud). In the transaction process, to punish malicious nodes, a penalty factor λ is introduced in the calculation of the trust value. It can be seen from the formula that when there is a dishonest transaction, the value range of λ is: $\lambda \in (0.5,1)$, and the penalty factor will make the node's empirical trust value drop rapidly, which makes the node not easy to fail. Honest transactions, and make malicious nodes pay a greater price for accumulating trust value.

θ is the reward factor:

$$\theta = \begin{cases} 0 & q \leqslant c \\ \dfrac{1}{2} e^{-\frac{1}{q-c}} & q > c \end{cases} \tag{5}$$

The reward factor is introduced to stimulate the enthusiasm of the node for successful transactions [10], where q is the number of successful transactions, $\theta \in (0, 0.5)$, where c is a constant, which is used as the pair transaction set by the user. The initial value of the number of honest transactions rewarded by the node, that is, the reward value will be calculated when the number of successful transactions reaches a certain level, which can encourage the node to increase the number of honest transactions for obtaining greater experience trust.

To prevent malicious nodes from increasing their trust value through oscillating transactions, the punishment should be greater than the reward. According to the formula, it is not difficult

to conclude that $\lambda > \theta$, that is, once a node has fraudulent behavior, its trust will decline rapidly. The state of slowly rising.

3.2. Recommended trust value

This article discusses how to determine the trust value between nodes when there are direct transactions between nodes. However, in P2P networks, there is often no transaction behavior between nodes, or there is little transaction experience, and it is impossible to determine the trust value between nodes by the empirical trust. This requires the recommendation of its neighbor nodes to judge its trust. Value, which is the recommended trust value.

The recommended trust value is related to the following factors:

(1) The number of recommended nodes for node j. The more recommended nodes, the more accurately the recommended trust value can be obtained. In this article, it is assumed that the recommended node selected by i is a node that has direct transaction history with j, and the set of nodes is $A(i,o)$;

(2) Node i's evaluation of recommended node k; represents the credibility of node i's recommendation to node k. If the evaluation of the recommended node is higher, its evaluation is more credible

(3) Recommend the evaluation of node k to node j; if the evaluation of the recommended node is higher, the greater the influence on the recommendation trust value of node j.

This paper divides the neighbor nodes into neighbor nodes with transaction history with node i and neighbor nodes with no transaction history with node i. Combining these two types of nodes, the recommended trust value of node j is obtained as follows:

$$RT(i,j) = \alpha \times \frac{\sum_{i=1}^{u} \left(E(i,k)E(k,j)\right)}{\sum_{k=1}^{u} E(i,k)} + \beta \times \frac{\sum_{i=1}^{v} \Phi_l E(l,j)}{\sum_{l=1}^{v} \overleftarrow{\omega}_l} \quad (6)$$

Where $E(i,k)$represents the trust value of node i to recommended node k, that is, the trustworthiness of neighbor node k relative to node i. $E(i,k)$ represents the trust value of recommended node k to node j, that is, the trustworthiness of neighbor node j relative to node k. α and β are two weighting factors and satisfies $\alpha + \beta = 1$, α indicates that node i assigns the weight of recommendation trust to all neighbor nodes that have transaction history with itself, and β indicates that node i assigns to all nodes that have no transaction history with itself. The recommended trust weight of neighbor nodes can be determined according to the trust strategy required by the user. u and v respectively represent the number of two types of neighbor nodes, and $u + v = |A(i,o)|$.

$\overleftarrow{\omega}_l$ is the trust evaluation weight of neighbor node l that has no transaction history with node i. It can effectively prevent joint deception between nodes and malicious nodes to increase mutual trust value through collusion. The main factors affecting Φ_l are as follows. For the transaction scale and transaction time of node j, if the transaction scale is large and the transaction time is relatively close, then the weight is relatively large; conversely, if the transaction scale is small and the transaction time is relatively long, the weight is relatively small.

3.3. Comprehensive trust value

In P2P e-commerce, many nodes are not a single behavior. Its trust value often includes the node's empirical trust value and recommended trust value. Therefore, it is not possible to use

only one situation to obtain the trust value of the node, and the trust value is obtained in this way. It is not complete and reliable, so the empirical trust of the node and the recommendation trust obtained from neighboring nodes must be considered comprehensively. The comprehensive trust value is obtained by calculating the weighted average of the two. Calculated as follows:

$$CT(i,j) = \varepsilon \times ET(i,j) + \eta \times RT(i,j) \tag{7}$$

Where $\varepsilon + \eta = 1$, which are the weights of empirical trust and recommendation trust, respectively, indicate the proportion of the two in the calculation. If there are fewer transaction history records between node i and node j, the corresponding ε should be a smaller value. On the contrary, if there are more transaction history records between node i and node j, the corresponding ε should be a larger value.

3.4. Transaction limit and trust threshold

In the transaction behavior of the node, the two parties of the transaction pay different attention to different transaction scales. The traditional trust model considers the transaction scale to be smaller than the total transaction scale in history, or to set a transaction scale authority based on the difference in trust value, but both of these situations have obvious drawbacks. The first type, although the size of each transaction is small, it is an additive process. As the number of transactions increases, its transaction size may be a very large value. In the second case, although the transaction scale is restricted, the specific calculation method of the authority is not given. There is a large subjectivity and arbitrariness, and it is often affected by the subjective emotions of each person in the transaction process.

Considering the above situation, this article sets the n-th transaction limit $M_{\max}^{(n)}$ based on the historical transaction records of node i and node j, which is calculated based on the previous maximum transaction amount, and it is a calculation method of the slow increase process is:

$$M_{max}^{(n)} = \left(1 + \frac{M_{n-1}}{\sum_{g=1}^{n-1} M_g}\right) \times M_{max}^{(n-1)} \tag{8}$$

Where M_g is the g-th transaction amount between node i and node j.

In addition, when a node conducts a transaction, it often sets a psychological bottom line for the trust value of the selected transaction object according to personal habits. This article calls it the trust threshold, which is represented by ω, which is the lowest trust value set to ensure the normal progress of the transaction. Is set by the node according to its own needs. For example, $\omega = 0.8$ means that node i only considers transactions with nodes whose trust value is greater than 0.8, which can guarantee the success of the transaction to a certain extent. In the actual transaction process, the node must comprehensively consider the transaction limit and trust threshold. This article defines their relationship as follows:

(1) If $M \leqslant M_{\max}^{(n)}$, and $ET(i,j) \geqslant \omega$, i directly trust j and directly trade with it

(2) If $M \leqslant M_{\max}^{(n)}$, but $ET(i,j) < \omega$, if i and j are more familiar, that is, there are more transactions, then i will directly reject j's transaction. If the number of transactions between i and j is small, it is not possible to accurately judge its trust value by its own experience. At this time, i will send a recommendation request message to the neighbor node, requesting an evaluation of the trust situation of j within the authority of M. And calculate the recommended trust value $RT(i\ ,\ j)$ according to the recommendation situation, if $RT(i,j) \geqslant \omega$, i chooses to

trade with j; (for a newly entered entity, the trust value is 0 and the authority is the lowest Entity, directly allow its transactions within the scope of authority);

(3) If $M > M_{\max}^{(n)}$ and $ET(i,j) < \omega$, i will directly refuse the transaction with j;

(4) If $M > M_{\max}^{(n)}$, but $ET(i,j) \geqslant \omega$, i will send a recommendation request message to neighbor nodes, requesting to evaluate the trust situation of j within the authority of M. And calculate its comprehensive trust value $CT(i,j)$ according to the recommended trust value, if $CT(i\ ,\ j) \geqslant \omega$, i choose to trade with j.

4. Experimental simulations

In this section, the model is simulated experimentally to verify the effectiveness of the model. To compare the transaction effects of various nodes, this article mainly chooses to compare the effects of preventing large transactions from deceiving nodes and oscillating node attacks.

(1) Prevent malicious nodes from using the small-scale accumulation of trust value to carry out large-scale fraud attacks

Assume that two nodes have a certain amount of direct transaction experience, and assume that before malicious nodes conduct fraudulent transactions, the two models have the same transaction history. The honest node i and the malicious node j conduct transactions. In the beginning, each transaction is a small-scale transaction, and it accumulates to a certain extent. Node j cheats in transactions with a large transaction amount. The experimental results of this model and the Peer Trust model are compared as shown in [Figure 2] shown.

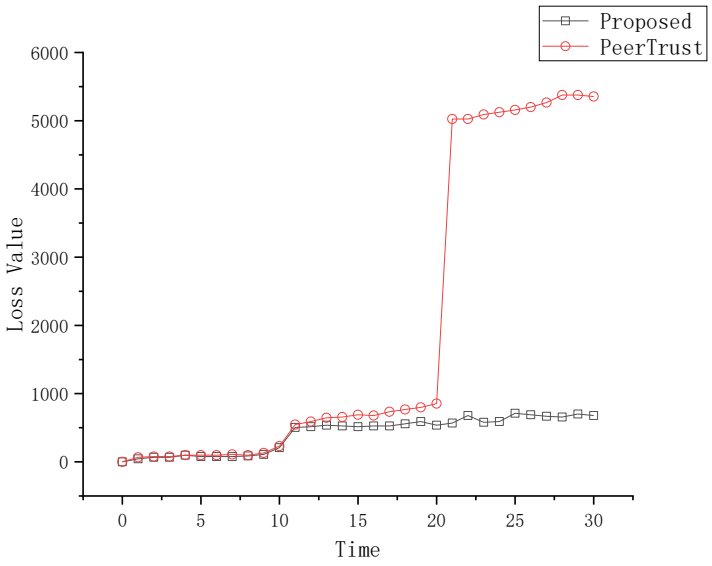

Figure 2. Comparison of node maximum loss changes during large-scale transaction attacks

It can be seen from [Figure 2] that when malicious nodes use small-scale transactions to accumulate high trust values and choose to commit fraud in large-scale transactions, the loss of integrity nodes in the Peer Trust model is greater because the model has a greater impact on

transactions. There are no restrictions on permissions and no control over such attacks. In this model, due to the establishment of the transaction limit $M_{\max}^{(n)}$, in the transaction, if the i-node is not willing to take risks, when there is an abnormal large-scale transaction application, it can choose to stop the transaction, and then the overall transaction with j Basically, the loss will not exceed the maximum value of the previous transaction. It can be seen that this model has made great improvements in preventing large-scale fraud attacks after accumulating trust values on a small scale.

(2) Prevent attacks from oscillating nodes

Suppose that the oscillating node periodically selects a certain number of honest transactions and malicious fraudulent transactions and assigns an initial trust value $ET_0(i,j) = 0.5$ to the node that conducts the transaction for the first time. In this model and the Eigen Trust model, the trend of trust value changes when the node oscillates trading is shown in [Figure 3].

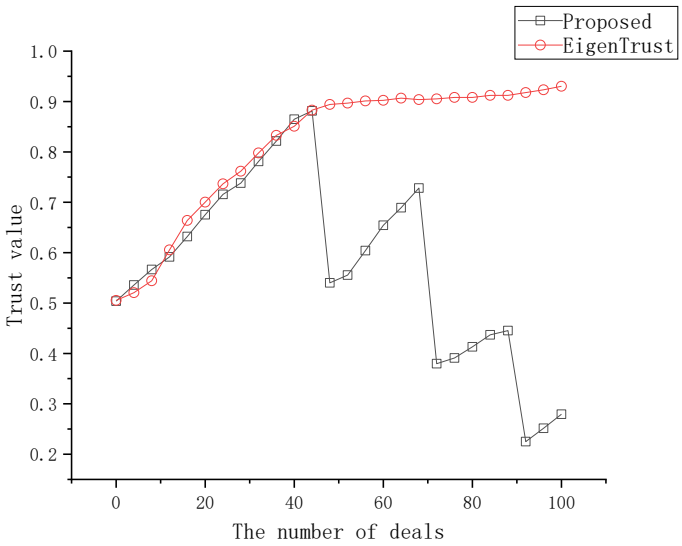

Figure 3. Comparison of changes in trust value of oscillating nodes when they maliciously deceive

It can be seen from [Figure 3] that for this model and the Eigen Trust model, when the node chooses an honest transaction, the trust value of both parties increases, and when the trust value reaches a certain level when the oscillating node j starts to choose a malicious transaction, the Eigen Trust The trust value of the node in the model is still rising. This is because there is no penalty mechanism in the model. After a malicious transaction occurs, the trust value of the node still rises slowly. However, in this model, the trust value of a node drops rapidly after malicious transactions, and the more malicious transactions, the faster the trust value drops. This is because the penalty factor is introduced in the model. When there is a trustworthy transaction afterward, because of the existence of the reward factor, its trust value begins to increase again. When the node slowly accumulates a high trust value, it starts to cheat again, and then the punishment factor will make the trust The value drops again, and the punishment is increasing, so that its trust degree presents a slow rise and rapid decline trend. If it conducts periodic malicious transactions for a long time, its trust value will quickly drop to trust. Below the threshold, no one will eventually trade with it.

5 Conclusion

Based on the influence of multiple factors on the trust value, this paper proposes a new trust evaluation model. The calculation of recommended trust value is classified and considered, and the dynamic transaction limit is set at the same time to make up for the deficiencies of some existing trust models. Simulation experiments show that this model has a good effect in resisting large-scale transaction attacks and the swinging behavior of oscillating nodes.

References

[1] J. Mortera, P. Vicard, and C. Vergari, "Object-oriented Bayesian networks for a decision support system," Departmental Working Papers of Economics - University 'Roma Tre', vol.7, no.2, pp.714-738, **(2012)**

[2] J. Hu, Q. Wu, and B. Zhou, "FCTrust: A robust and efficient feedback credibility-based distributed P2P trust model," // International Conference for Young Computer Scientists, IEEE, **(2008)**

[3] D. Kovac and D. Trcek, "Qualitative trust modeling in SOA," Journal of Systems Architecture, vol.55, no.4, pp.255-263, **(2009)**

[4] A. Tajeddine, A. Kayssi, and A. Chehab, "Fuzzy reputation-based trust model," Applied Soft Computing Journal, vol.11, no.1, pp.345-355, **(2011)**

[5] E Fragnière, J. Gondzio, and Y. Xi, "Operations risk management by optimally planning the qualified workforce capacity," European Journal of Operational Research, vol.202, no.2, pp.518-527, **(2010)**

[6] A. Zeng, "Enhancing network robustness against malicious attacks," Physical Review, Statistical physics, plasmas, fluids, and related interdisciplinary topics, vol.85, no.6, pp.066130, **(2012)**

[7] P. Inacio, M. M. Freire, and M. Pereira, "Analysis of the impact of intensive attacks on the self-similarity degree of the network traffic," // International Conference on Emerging Security Information, IEEE, **(2008)**

[8] P. Dwivedi and Bharadwaj, "Effective resource recommendations for e-learning: A collaborative filtering framework based on experience and trust," Communications in Computer and Information Science, vol.1, no.250, **(2011)**

[9] N. Griffiths, "Task delegation using an experience-based multi-dimensional trust," // International Joint Conference on Autonomous Agents and Multiagent Systems, ACM, **(2005)**

[10] J. Haowei and T. Yubo, "P2P trust model in the trust value," IEEE, **(2010)**