Trust Evaluation Model for P2P Networks based on Time and Interaction

KE Xuemeng[1], *ZHOU* Guofu[1, 2], *DU* Zhoumin[2]

[1]State Key Laboratory of Software Engineering, Wuhan University, China
[2]Computer School, Wuhan University, China

Abstract. The traditional centralized trusting mechanism does not meet the requirements of the modern P2P network, so it is necessary to establish a distributed trusting mechanism to strengthen the system's reliability. Factors including time attenuation factor, interactive frequency factor, interactive size factor and average online time factor markedly influence the trust of the nodes in a P2P network. This paper defines the precise effects of these factors on trust and proposes a comprehensive trust model and global trust model based on direct trust and indirect trust.

1 Background

P2P networks have become the focus of the Internet due to their application in file distribution, streaming media transmission, distributed computing, and more [1]. The sharp increase in the number of P2P network users and the openness of P2P networks themselves has created an increasing complexity of trust between network nodes. In 1994, Marsh first extended the "trust relationship" concept from the social network to the computer network and research on trust management in computer networks began in earnest [2]. The traditional centralized trusting mechanism does not meet P2P network requirements, so it is necessary to establish a new distributed trusting mechanism to build trust relationships between nodes, as the basis of the interaction among them.

The interactive success rate of nodes that select interactive objects with higher trust is higher. The block chain[3][4], a relatively new P2P network application, is a mode of distributed data storage [5], a point-to-point transmission consensus mechanism, and an encryption algorithm [6], The consensus mechanism is a method of building trust between nodes and accessing rights in a block chain system [7].

2 Related Work

Many P2P-based trust models have been proposed in recent years. EigenTrust [8][9], for example, is one of the first models of dynamic computing the global trust value of nodes. In EigenTrust, the local trust value of a node is calculated after its interactions; the results are fed back to calculate the global trust value of the node. When applied to a large-scale network, EigenTrust suffers poor scalability, inappropriate convergence, and high computational complexity. FCTrust [10] also uses the feedback concept, under which the trust of nodes is determined by interaction frequency. However, it equally assigns weight to all the transactions instead of giving more importance to recent ones in calculating local trust, resulting in an inaccurate evaluation of the target node.

Based on the above literature review, we examined the factors which significantly influence the trust among nodes including time attenuation [11], interactive frequency, interactive size and average online time. We established a novel model of trust evaluation based on time and interaction accordingly, discussed in detail below.

3 The Trust Factor

3.1 Time Attenuation Factor

Definition 1 (Time Attenuation Factor): The attenuation of the influence of nodes' interaction history on its trust over time is represented by h and calculated as follows:

$$\rho^{h} = \min\left(\rho_{e}^{\lfloor t_h - t_n \rfloor}, 1\right). \quad (1)$$

where tn is for the current moment; th is for the historical moment of interaction. The closer to the current moment the moment of historical interaction this, more influence the interaction has on the trust evaluation values. Conversely, there is less impact to the trust evaluation farther from the current moment[12][13]. The EigenTrust 89 model ignores the impact of time attenuation on trust calculation and thus is not sufficiently objective. In our model, the time attenuation factor is introduced into the calculation of each trust factor.

ρ_e is the base of the exponential attenuation function. ρ_e takes the value e, i.e., ρ_e=e. The time attenuation is always less than or equal to 1. The time attenuation

factor is greater, approaching to 1 when the moment of historical interaction is closer to the current time. When the moment of historical interaction occurred a long time ago, the time attenuation factor value approaches infinitesimal. Time attenuation factor h is represented by ρ^h_{sat} and ρ^h_{unsat} according to a successful or failing result, respectively.

ρ^h_{sat}: The time attenuation factor in the case of a successful interaction. In this case, t_h represents the historical moment of a successful interaction.

ρ^h_{unsat}: The time attenuation factor in the case of a failing interaction. In this case, th represents the historical moment of a failing interaction.

The moment of historical interaction has a great influence on trust value. The effect of historical interaction between nodes on the trust evaluation values attenuates gradually as time goes by, and this attenuation is not linear. When the historical interaction occurred a long time ago, the influence on trust shrinks towards zero[14]. The difference between the moments of historical interaction and the current moment is rounded down unlike the calculation method of time attenuation factor in previous studies[14]. Each time attenuation factor is matched with a corresponding time period. The time attenuation factor is h when the interaction occurs within the period from $\lfloor t_h - t_n \rfloor$ to $(\lfloor t_h - t_n \rfloor + 1)$.

3.2 Interactive Frequency Factor

Definition 2 (Interactive Frequency Factor): The interactive evaluation factor C_{ij} measures the effect of successful interaction frequency and failing interaction frequency on trust degree. It is calculated as follows:

$$s_{ij} = sat(i,j) - unsat(i,j), \tag{2}$$

$$C_{ij} = \frac{\max(s_{ij}, 0)}{\sum_j \max(s_{ij}, 0)}. \tag{3}$$

Based on the time attenuation factor, the definition of $sat(i,j)$ and $unsat(i,j)$ is :

$$sat(i,j) = \sum_{k=1}^{n} vs_{ij}^k \cdot \rho^h_{sat}, \tag{4}$$

$$unsat(i,j) = \sum_{k=1}^{n} vf_{ij}^k \cdot \rho^h_{unsat}. \tag{5}$$

sat(i,j) represents the number of successful interactions between node i and node j having taken time attenuation factor into consideration. Node i is a requesting node and node j is a requested node. In sat(j,i), node j is a requesting node and node i is a requested node. Therefore, sat(i,j) is different from sat(j,i), and their values may differ.

unsat(I,j) represents the number of failing interactions between node i and node j with time attenuation factor taken into consideration. Node i is a requesting node and node j is a requested node. In the same way, unsat(i,j) is different from unsat(j,i).

k represents a period from $\lfloor t_h - t_n \rfloor$ to $(\lfloor t_h - t_n \rfloor + 1)$ approaching the current moment; k has the same meaning in the post.

vs_{ij}^k represents the number of successful interactions between node i and node j within the period k. vf_{ij}^k represents the number of failing interactions between node i and node j within the period of k.

In order to avoid unfairness to new nodes and to distinguish new nodes from bad nodes, node i is considered to be a new node if:

$$\sum_j (sat(i,j) + unsat(i,j)) = 0. \tag{6}$$

Because the new nodes have no interaction with any other node, the trust evaluation of new nodes to other nodes can only be evaluated by the indirect trust degree and the attributes of the nodes. No node has interacted with a new node in the network, so each new node is given an initial global trust $GTrust_{new}$ which is equal to the global trust value of its invitation node, that is to say, the higher the global trust of its invitation node, the higher the initial global trust that the new node is given. If

$$\sum_j (sat(i,j) + unsat(i,j)) \neq 0, \tag{7}$$

Node i is not a new node. The interactive evaluation factor for node i and node j is calculated according to (2) and (3).

3.3 Interactive Size Factor

Definition 3 (Interactive Size Factor): The interactive size factor measures the impact of interactive data volume on trust degree between node. It is denoted as D_{ij} and calculated as follows:

$$data_{ij} = data_{sat}(i,j) - data_{unsat}(i,j), \tag{8}$$

$$D_{ij} = \frac{\max(data(i,j),0)}{\sum_j \max(data(i,j),0)}. \tag{9}$$

where data(i,j) represents the interactive data volume between node i and node j. $data_{sat}(i,j)$ represents the data volume of successful interaction between node i and node j. $data_{unsat}(i,j)$ represents the data volume of failing interaction between node i and node j.

The time attenuation factor is also calculated during calculation of the interactive data volume. The definitions of $data_{sat}(i,j)$ and $data_{unsat}(i,j)$ are:

$$data_{sat}(i,j) = \sum_{k=1}^{n} satdata_{ij}^{k} \cdot \rho_{sat}^{h}, \quad (10)$$

$$data_{unsat}(i,j) = \sum_{k=1}^{n} unsatdata_{ij}^{k} \cdot \rho_{unsat}^{h}. \quad (11)$$

$satdata_{ij}^{k}$ represents the data volume of successful interaction between node i and node j within period k. $unsatdata_{ij}^{k}$ represents the data volume of failing interaction between node i and node j within period k.

The interactive size factor can prevent malicious nodes from performing well in smaller-sized interactions, but cheating in larger interactions while the trust is still good. The EigenTrust89 model ignores the impact of interactive size on trust calculation.

3.4 Average Online Time Factor

The node is more likely to be online in the future, and considered to be generally more reliable, when it has a longer average online time. The average online time factor reflects the influence of average online time on trust. Again, the EigenTrust89 model ignores the impact of time factor on trust calculation.

Definition 4 (Average Online Time Factor): Average online time factor measures the impact of the node's average online time on its trust degree. It is represented by Tj and calculated as follows:

$$T_j = \frac{t_j}{N_j}. \quad (12)$$

t_j represents the total online time of node j. Nj represents the number of times that node j has gone online.

4 Trust Model

A P2P network can be modeled as a directed graph G={V,E}. The vertex set is represented by V={P1,P2,⋯,Pn} where n represents the number of nodes in the network. The edge set is represented by E={(Pi,Pj)|i,j=1,2⋯,n}, where $E \subseteq V \times V$. e_{ij} is the weight of edge (Pi,Pj) calculated by the number of interactions between Pi and Pj having taken the time attenuation into consideration. Pi is a requesting node and Pj is a requested node. It is defined as follows:

$$e_{ij} = sat(i,j) + unsat(i,j). \quad (13)$$

We also introduced the concept of a set Qj into the trust model, where Qj represents a collection of nodes that have interactions with P_j.The definition of set Qj is:

$$Q_j = \{P_k \in V | e_{ij} > 0\} \quad (14)$$

4.1 Direcct Trust

Definition 5 (Direct Trust): Direct trust[15], also referred to as local trust, is represented by DTrust(i,j). It is the trust degree that P_i has established over the history of direct interaction with P_j.

The following penalty function is introduced into the direct trust model:

$$pen(i,j) = -\frac{\sum_i DTrust(i,j)}{|Q_j|} \times \frac{unsat(i,j)}{sat(i,j)}. \quad (15)$$

Pen(i,j) is the penalty function of node i to node j. unsat(i,j) is the number of failing interactions between node i and node j, and sat(i,j) is the number of successful interactions between node i and node j. The more the node fails to interact and the less it succeeds, the greater the punishment.

When calculating direct trust, EigenTrust89 adopts an iterative approach, which requires excess computation resources. FCTrust10 equally assigns weight to all the factors, which obscures the importance of each factor.

The greater the interactive frequency factor, the greater the interactive size factor, the greater the average online time factor, and the greater the direct trust value of this node, here, we built a direct trust model by multiplying these factors. The mathematical definition of direct trust of Pi to Pj is :

$$DTrust(i,j) = C_{ij} \times D_{ij} \times T_j + pen(i,j)\frac{1}{1+\rho_e^{-n}} \quad (16)$$

$\frac{1}{1+\rho_e^{-n}}$ represents the accelerating factor and $\rho_e = e$. When the node's behavior becomes malicious, the acceleration factor reduces the trust value rapidly. When the node's behavior becomes normal, the trust value slowly increases.

4.2 Indirect Trust

Definition 6 (Indirect Trust): Indirect trust[16], also referred to as recommendation trust, is represented by ITrust(i,j); it is the trust degree that nodes build through indirect interactive history.

When Pi has no direct interaction or very few direct interactions with P_j, the trust degree of Pi to P_j .depends on the recommendations from other nodes that have direct interaction with P_j.

For any $P_k \in Q_j$, the direct trust degree of P_k to P_j can be calculated according to (16). The definition of indirect trust ITrust(i,j) of Pi to Pj:

$$ITrust(i,j) = \frac{\sum_{P_k \in Q_j} DTrust(k,j)}{|Q_j|} \quad (17)$$

4.3 Comprehensive Trust

Definition 7 (Comprehensive Trust): Comprehensive trust is the trust established by direct trust and indirect trust. The comprehensive trust of P_i to P_j is represented by STrust(i,j) and calculated as follows:

$$q_1 = \frac{e_{ij}}{\sum_i e_{ij}}, \quad (18)$$

$$q_2 = 1 - \frac{e_{ij}}{\sum_i e_{ij}}, \quad (19)$$

$$STrust(i,j) = q_1 \cdot DTrust(i,j) + q_2 \cdot ITrust(i,j) \quad (20)$$

q_i, the weight of STrust(i,j) is a dynamic value. q_i is related to the frequency of interaction between Pi and Pj.

The more frequently Pi interacts with Pj, the greater q_1 is, the smaller q_2 is and the more important the direct trust is. The less frequently Pi interacts with Pj, the greater q_2 is, the smaller q_1 is and the more important the indirect trust is.

$e_{ii} = 0$ indicates that Pi does not interact with P_j. Therefore $q_1 = 0$ and $q_2 = 1$. The trust value to P_j is measured by the indirect trust.

When Pi only interacts with Pj and has no interaction with other nodes, then $q_1 = 1$ and $q_2 = 0$. The trust value is measured by the direct trust.

4.4 Global Trust

Definition 8 (Global Trust): To measure the trust of each node based on the entire network, the global trust of Pi is calculated according to the comprehensive trust of other nodes in the network to P_i. The global trust degree of P_i is represented by GTrust(i).

Definition 9 (Approve): When the comprehensive trust degree of Pi to Pj exceeds a certain value, Pj is approved by Pi and denoted by R(i,j)=true. Otherwise, Pj is not approved by Pi and denoted by R(i,j)=false.

When STrust(i,j)> λ , P_j is approved by Pi and denoted by R(i,j)=true. When STrust(i,j)< λ ,P_j is not approved by Pi and denoted by R(i,j)=false.

The λ variable mentioned above is an approbation threshold which distinguishes good nodes from bad nodes. If the threshold is too high, the global trust of nodes in the network is generally low. Conversely, if the threshold is too low, the global trust is generally high and good nodes may not be sufficiently distinguishable from bad nodes. We set λ =0.2 in our experiment.

The greater the proportion of nodes that recognize this node in the network, the higher the global trust degree the node has; therefore the global trust degree of P_i can be calculated by the percentage of the nodes approve P_i in the entire network. The global trust degree has global uniqueness.

A node set W_i is defined to represent the set of nodes that approve P_i in the network. Definition of W_i is shown in

$$W_i = \{P_k \in V | R(k,i) = \text{true}\} . \quad (21)$$

The global trust of P_i is calculated by the percentage of the approve nodes with all nodes in the network. The global trust degree is defined as follows:

$$\text{GTrust}(i) = \frac{|W_i|}{|V|} . \quad (22)$$

5 Experiment And Analysis

We designed several nodes to simulate the application scenarios of a P2P network in order to verify the proposed trust evaluation model. The historical interaction records of nodes served as inputs to calculate the trust degree.

In the number of initial nodes is too large, the calculation is may be overly complex and the result may not be conducive to observation and comparison. If the number of nodes is too small, the advantages of the model are not effectively reflected. We set the number of nodes to 10 in our experiment. Node 5 and node 10 are bad nodes which provide one bad service for every two good services. Other nodes are normal nodes which consistently provide good service. In the P2P network, all shared files are randomly distributed evenly. The nodes in the network randomly download or upload files from other nodes. During the experiment, online status of nodes, number of interactions, requesting node, requested node, volume of interactive data and results of interaction were recorded. These records were then used as input data to calculate the direct trust, indirect trust, comprehensive trust and global trust of each node in the network. For the sake of comparison, we choose a normal node and a bad node for separate recordings of changes in global trust over defined time period. We also selected a node to record the attenuation of the node global trust degree as time progressed.

Figure 1 shows the global trust between nodes after a period of interaction as-calculated using the proposed model and EigenTrust, respectively. Node 5 and node 10 showed the lowest global trust degree, as each provided bad service once time. We found it much easier to distinguish the good nodes from the bad nodes using the proposed model compared to EigenTrust.

Figure 2 shows the changes in global trust degree of nodes 3 and 5. One period is defined as the end of the previous service to the completion of the present service. Node 3 is a normal node and always provides good service; node 5 provides two good services followed by a bad one. Node 3's global trust degree continually increased over the observation period, while the global trust of node 5 fluctuated. When providing a good service, node 5's global trust rebounded to some extent before decreasing when it subsequently provided bad service. The amplitude of its decline was always greater than the amplitude of increase due to the penalty function. When the node is behaving badly, the node is punished and the trust degree quickly drops. When node's behavior gets better, its trust degree increases, but slowly.

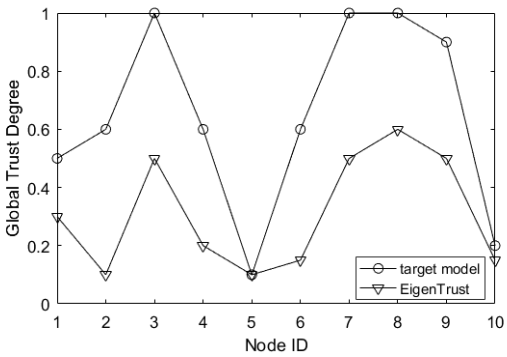

Fig 1. Global trust degree.

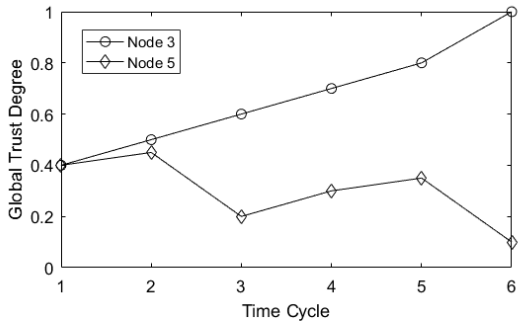

Fig 2. Changes in global trust after interaction.

Figure 3 shows the change curve of the global trust degree of node 3. The closer to the current moment, the greater impact the interaction of nodes on trust degree. The farther from the current moment, the smaller the impact the interaction has on the trust degree. Node 3 appears to provide good service in the previous interaction and has a high level of trust. Once node 3 has not provided any service for a long time, its trust degree drops off.

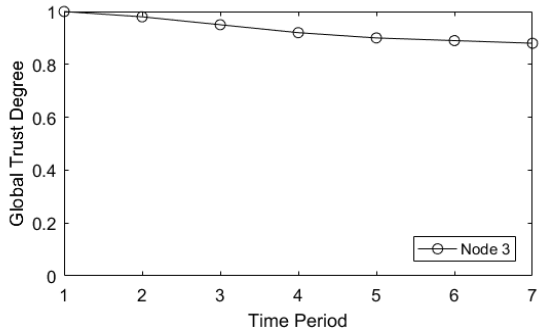

Fig 3. Changes in global trust over time.

6 Conclusion

There is no third-party authentication in the P2P network, so it is necessary to judge and select appropriates node with which to interact to ensure system reliability. This paper proposed a trust evaluation model based on time and interaction which resolves trust problems in P2P networks. Multiple factors including the time attenuation factor, interactive frequency factor, interactive size factor and average online time factor were introduced to calculate the direct trust degree and indirect trust degree respectively. The comprehensive trust degree and global trust degree can be obtained according to the direct trust degree and indirect trust degree.

In the future, we plan to apply the trust evaluation model in actual P2P networks, including the block chain. We will choose appropriate trust nodes for effective and safe interactions to download and upload files, and thus realize distributed storage and access for files in the P2P network.

References

1. HuiGuo Dong. The application and implementation of search technique based on p2p networks. Computer Knowledge and Technology, 2010.
2. Stephen Paul Marsh.Formalising trust as a computational concept. University of Stirling, 1994.
3. Aaron Wright and Primavera De Filippi. Decentralized blockchain technology and the rise of lex cryptographia. Social Science Electronic Publishing, 2015.
4. Xianmin Yang, L. I. Xin, W. U. Huanqing, and Keyun Zhao. The application model and challenges of blockchain technology in education. Modern Distance Education Research, 2017.
5. Hoang Giang Do and Wee Keong Ng. Blockchain-based system for secure data storage with private keyword search. In IEEE World Congress on Services, pages 90–93, 2017.
6. Yuqin Xu, Qingzhong Li, Xingpin Min, Lizhen Cui, Zongshui Xiao, and Lanju Kong. E-commerce blockchain consensus mechanism for supporting high-throughput and real-time transaction. 2016.
7. Yong Yuan and Feiyue Wang. The development status and prospect of blockchain technology. Automated journal, 42(4):481–494, 2016.
8. Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The eigentrust algorithm for reputation management in p2p networks. In International Conference on World Wide Web, pages 640–651, 2003.
9. Kenli Li, Yan He, Xiaoling Liu, and Ying Wang. Security-driven scheduling algorithms based on eigentrust in grid. In International Conference on Parallel and Distributed Computing, Applications and Technologies, pages 1068–1072, 2005.
10. Jianli Hu, Quanyuan Wu, and Bin Zhou. Fctrust: A robust and efficient feedback credibility-based distributed p2p trust model. pages 1963–1968, 2008.
11. Blackburn and Joseph. The time factor. National Productivity Review, 9(4):395–408, 1991.
12. Limin Tao. Research on Subjective Trust Management Based on Uncertainty Theory in Open Network Environment. PhD thesis, Zhejiang University of Technology, 2013.
13. Yu Bao, Guosun Zeng, Liansun Zeng, Bo Chen, and Wei Wang. A measure of trust in p2p networks to prevent deception. Journal of communication, 29(10):215–222, 2008.
14. Yanxia Cui. Study and Improvement of EigenTrust Trust Model Based on P2P Network. PhD thesis, Tianjin university of technology, 2016.
15. Kiefhaber R, Jahr R, Msadek N, et al. Ranking of Direct Trust, Confidence, and Reputation in an Abstract System with Unreliable Components[C]// Ubiquitous Intelligence and Computing, 2013 IEEE, International Conference on and, International

Conference on Autonomic and Trusted Computing. IEEE, 2014:388-395.

16. Barsoum A, Hasan A. Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems[J]. IEEE Transactions on Parallel & Distributed Systems, 2013,24(12):2375-2385.