



GSBDTRUST: GROUP STRUCTURE-BASED DYNAMIC TRUST MODEL FOR PEER-TO-PEER NETWORKS

Jie Chen

School of Computer Science and Software Engineering, Tianjin Polytechnic University, Tianjin 300387, China.

ABSTRACT

The trust model is one of the most important technologies of Peer-to-Peer (P2P) security. The popular EigenTrust reputation system can well resist the attack of malicious peers, which aggregates the extensive view of all other peers in the system to compute the global trust values for the peers, and relies on a set of pre-trusted peers heavily to ensure that the malicious peers do not subvert the system. Nevertheless, the EigenTrust model, which designates early participants or creators of a P2P network as pre-trusted peers statically, poses a high security risk, especially for the targeted attacks. To solve this problem, it is an inevitable trend to select pre-trusted peers dynamically according to the interaction between peers. And thus, this paper selects pre-trusted peers dynamically based on the time-interactivity of peers in the network, which can avoid a series of problems caused by statically specified pre-trusted peers. Meanwhile, the peers can not be effectively organized together for network models with community structure, which increases the unnecessary interaction between peers greatly, and aggravates the load rate of the system heavily. In order to better organize peers together in the distributed network, this paper proposes a P2P network trust model based on group structure based on the interaction characteristics of peers. To ensure the high credibility of P2P network, we choose the peers with high global trust values as pre-trusted peers in each group. The final simulation experiments show that the GSBDTrust model not only has strong robustness against malicious peer attacks with different thread models, but also has low query overhead and failure rate in resource search.

KEY WORDS: P2P network security; trust model; group structure; EigenTrust.

1. INTRODUCTION:

In recent years, Peer-to-Peer (P2P) network has been fully researched and widely applied in the field of resource sharing, instant messaging, collaborative computing and so on, such as Napster[1], Gnutella[2], SETI@home[3] and JXTA[4], due to the characteristics of openness, scalability, robustness, and decentralization, etc. However, the development of the network is like a double-edged sword, which brings us some benefits while causing new problems. Compared with the traditional C/S architecture, today's central servers are static, easy to control, and once switched to P2P network, these uncontrollable factors are all highlighted. It is precisely the features of open, autonomous and anonymous of these networks [5][6][7][8] that lead to a complete lack of accountability for the content a peer puts on the network, opening the door to abuses of these networks by malicious peers [9], such as Trojan virus, the theft of sensitive files and the malicious transmission of junk files, etc. At the same time, the peers are completely unfamiliar with each other in the P2P network environment due to lack of further information. The distrust between the peers makes the peers unwilling to share the resources they own actively, even though other peers actively provide the resources they own, in order to prevent attacks by malicious peers or receive Trojan viruses, peers do not dare to interact on account of the imperfect constraint mechanism between peers. Therefore, there is an urgent need for a mechanism to restrict the behavior of peers in the network, and the reputation system has emerged. The establishment of trust relationship between peers is both important and difficult, since Marsh[10] first introduced trust relationship in social network into computer network in 1994 and put forward the concept of trust management, the research on reputation system has not been interrupted, such as EigenTrust[9], PDTrust[11], PeerTrust[12] and PowerTrust[13]. In most trust models, the EigenTrust system proposed by Kamvar S.D. et al. is the most classic [14]. The algorithm calculates the global trust values of the peers in the network according to the historical upload behavior of the peers, which effectively reduces the download amount of the unauthentic file. However, the introduction of static pre-trusted peers in a dynamic P2P environment is vulnerable to attacks by malicious peers. At the same time, the limitations of EigenTrust are highlighted in a network environment based on group structure. In a group with pre-trusted peers, the global trust value ranking of most peers is significantly higher than that of groups without pre-trusted peers. This is mainly because the former are better connected to the pre-trusted peers than the latter [15].

To this end, this paper proposes a dynamic P2P network trust model based on group structure, which is an improvement of the EigenTrust algorithm. In this model, peers with community structure are grouped, and the interaction between peers in the same group is significantly higher than the interaction between peers in the different group. Meanwhile, in order to guarantee the high credibility of the system, peers with higher global trust values are selected as pre-trusted peers dynamically. Simulation experiments show that the GSBDTrust model can not only reduce the unauthentic download of good peers in the network, but also effectively reduce the unnecessary interaction between peers, and successfully improve the number of queries.

The organization structure of this paper is as follows. In the section 2, related work is introduced briefly, the EigenTrust model and its major problems are ana-

lyzed mainly. Section 3 describes the GSBDTrust reputation model in detail. In section 4, the parameters and results of the simulation experiment are given, and analyze the results. This study is rounded off with the conclusion in the last section.

2. CURRENT SITUATION AND EXISTING PROBLEMS:

The establishment of a reputation system in the P2P network is mainly to guarantee a benign interaction between peers. At present, there are many researches on the reputation system, such as PDTrust [11], PeerTrust [12], PowerTrust [13], EigenTrust [9]. Among them, PDTrust is a partial distributed P2P network model proposed by Mekouar et al., which directly uses the feedback information of peers and is vulnerable to joint attacks by malicious collectives. PeerTrust is a local trust model proposed by Xiong et al. This model introduces 3 basic trust parameters and 2 adaptive factors in computing trustworthiness of peers, namely, the five important parameters of feedback a peer receives from other peers, the total number of transactions a peer performs, the credibility of the feedback sources, transaction context factor, and the community context factor. Dynamic feedback based on the nearest time window is proposed to solve the dynamic rocking behavior of the peers. Nevertheless, this approach is the heavy overhead associated with retrieving weighting factors [16]. PowerTrust model, proposed by Zhou & Kai, is an improvement on EigenTrust, using a look-ahead random walk strategy, which improves the accuracy of global reputation values and the convergence speed of iterations. However, it takes time until power peers are selected and identified [17]. The EigenTrust algorithm assigns a unique global trust value for each peer based on the historical upload behavior of the peer. The requesting peer selects the download source according to the global trust value of the responding peer, which can reduce the download amount of the unauthentic file. In the section 2.1, there is a brief description of the EigenTrust algorithm.

2.1 Distributed strategy of EigenTrust algorithm:

EigenTrust [9] is one of the most well-known and successful reputation systems [18]. The popular algorithm has been widely studied since it was proposed by Kamvar et al. The reputation model calculates the direct trust value between two peers according to the direct interaction behavior between peers, that is, the local trust value. In order to avoid arbitrarily high local evaluation between malicious peers or groups or any low inauthentic evaluation on other good peers, serializing the local trust value between peers, and finally gather the evaluation between other peers according to the serialized local trust value, and the global trust values of peers are finally obtained.

1) Local trust value:

In the EigenTrust reputation system, the local trust value of peer i to peer j is as shown in formula (1).

$$s_{ij} = \sum t_{ij} \cdots \cdots (1)$$

Where s_{ij} represents the local trust value of peer i to peer j . t_{ij} indicates that peer i obtains a file from peer j for download, and gives peer j a feedback evaluation according to whether the file satisfies its own requirements or

not. When peer i does not satisfy the file provided by peer j , peer i gives peer j a bad evaluation, namely, $tr_{ij} = -1$, conversely, peer i gives peer j a good evaluation, namely: $tr_{ij} = 1$. Simply, it can also be written as: $s_{ij} = \text{sat}(i,j) - \text{unsat}(i,j)$. Where $\text{sat}(i,j)$ represents the number of good evaluations of peer i for peer j , and $\text{unsat}(i,j)$ represents the number of bad evaluations.

2) Normalizing Local Trust Values:

In order to prevent arbitrary evaluation between malicious peers, the EigenTrust model serializes the local trust value of the peer interaction. The serialization process is as shown in formula (2).

$$s_{ij} = \frac{\max(r_{ij}, 0)}{\sum_j \max(r_{ij}, 0)} \dots \dots (2)$$

3) Aggregating Local Trust Values:

In order to obtain a wider view, peer i can get the reputation values of other peers in the system through its own neighbor peers:

$$t_{ik} = \sum_j c_{ij} c_{jk} \dots \dots (3)$$

Where t_{ik} denotes that peer i obtains its reputation value for peer k by asking its neighbor peer. However, the reputation value obtained in this way has certain limitations (peer i only obtains the reputation value for k by itself or its own neighbor peers). In order to make t_{ik} more comprehensive, peer i can obtain more peers' evaluation of k peers through neighbors of its own neighbors, and so on, as the number of iterations increases, the credibility of t_{ik} also increases.

One problem to consider is that if peer i is the new peer that first enters the system and it does not have any trusted peer, then peer i will choose to trust the pre-trusted peers in the system (the EigenTrust algorithm assumes that the creator of the system will not destroy the system all the time). The method for calculating the global reputation value is shown in formula (4).

$$\vec{t}^{(k+1)} = (1-a)C^T \vec{t}^{(k)} + a\vec{p} \dots \dots (4)$$

Where a is a constant and $0 < a < 1$. In this way, the peers entering the system for the first time can trust the pre-trusted peers, so that the system can interact safely and stably.

2.2 The main problem of the EigenTrust algorithm:

The EigenTrust model can guarantee the transmission rate of authentic files in the distributed network. It has been proved by many experiments that it has good robustness under various threat models. However, the EigenTrust model is still not robust enough in pre-trusted peers static designation and peers query efficiency. The following summarizes the major problems in the EigenTrust model.

The EigenTrust algorithm relies heavily on statically specified pre-trusted peers. As the interaction of peers, the behavior of the peers also changes dynamically in the system. If the behavior of the pre-trusted peers becomes bad, other peers will be provided with unauthentic files, but they still choose to trust the pre-trusted peers, which would be a serious disaster for the system.

For network models with community structure, peers can not be effectively organized together, which greatly increases the unnecessary search interaction between peers and aggravates the load rate of the system.

3. GSBDBTRUST REPUTATION MODEL:

The GSBDBTrust model improves the static designation of pre-trusted peers and the peer query structure in the network. First, the GSBDBTrust model organizes the relationship between peers with a network model based on group structure. There is a pre-trusted peer and multiple common peers in each group. The peer roles in the group are not fixed. As the peers interaction, the normal peer may become a pre-trusted peer, and vice versa, the pre-trusted peer may become a normal peer. The interaction relationship between peers is divided into intra-group interaction and inter-group interaction. The probability of interaction between peers in the group is much greater than the interaction between groups.

3.1 The dynamics of pre-trusted peer:

In the GSBDBTrust reputation model, each group is provided with a pre-trusted peer in order to ensure that the good peers get better service quality in the group. The reputation value of the peer is also changed from time to time due to the constant interaction between peers in the network. We select the peer with the highest global trust value in each group as the pre-trusted peer to ensure the high credibility of the pre-trusted peers, as in the formula (5):

$$p_{g_{max}} = \max \text{GlobeTrust} \{p_{g_1}, p_{g_2}, \dots, p_{g_k}, \dots\} \dots \dots (5)$$

Where $p_{g_{max}}$ is the peer with the highest global trust value in the g -th group, that is, which is the pre-trusted peer of the g -th group, and p_{g_k} is the k -th peer in the g -th group.

3.2 Network model based on group structure:

The GSBDBTrust reputation model is based on a network with a community structure, and is grouped according to the characteristics of the peers. Therefore, the interaction probability of peers within groups is higher than that of peers between groups. At the same time, in order to maintain connectivity and interaction between peers of the groups, peers of different groups use the probability p to perform inter-group searching. Due to the clustering of peer interaction features, the probability of peer interaction within the group is higher than that between the groups, so the probability p is small relatively. The query efficiency of the peer is further improved, and the query cost and failure rate are lower in resource search.

Critical idea of the GSBDBTrust model can be implemented by algorithm 1.

Algorithm 1: GSBDBTrust Algorithm

A_d : the set of peers which downloaded files from its daughter peer d .

B_d : the set of peers which peer d downloaded files from.

foreach group G_i do

foreach peer j do where $peer\ j \in G_i$

Query all peers $j \in A_d$ for $c_{jd} p_j$

Repeat

Find $l \in A_d$ where $t_l^{(k)} = \max\{t_1^{(k)}, \dots, t_r^{(k)}, \dots, t_n^{(k)}\}$ and peer $r \in G_i$

Compute $t_d^{(k+1)} = (1-a)(c_{1d}t_1^{(k)} + c_{2d}t_2^{(k)} + \dots + c_{nd}t_n^{(k)}) + ap_d$

Send $c_{dj}t_d^{(k+1)}$ to all peers $j \in B_d$

Wait for all peers $j \in A_d$ to return $c_{jd}t_j^{(k+1)}$

until $|t_d^{(k+1)} - t_d^{(k)}| < \delta$

end

end

end

4. SIMULATIONS AND RESULTS:

4.1 Simulation parameters:

The simulation experiment is based on the QueryCycleSimulator developed by Stanford University to improve the EigenTrust algorithm. Each thread model was tested for 5 times with a simulation cycle of 600, and the final results were analyzed by the average of 5 times. In the simulation model, there are 105 peers in total, with the number of good peers being 48, the number of pre-trusted peers being 15, and the number of malicious peers being 42. The number of neighbor peers is 5, the probability of interaction between groups is $p=0.05$, and the probability of interaction between peers in the group is $1-p$. Where, the number of Time to Live (TTL) is 5. The detailed parameters of the simulation experiment are shown in Table 1.

Table 1: Configuration of the simulation parameters

Parameter	Value	Parameter	Value
Times of experiment	5	No. of cycles of querying	600
No. of good peers	48	No. of malicious peers	42
No. of pre-trusted peers	15	No. of neighbor peers	5
p	0.05	Time to live(TTL)	5

4.2 Simulation results and analysis:

In the experiment, the abscissa is the number of query cycles, and the ordinate is the total number of inauthentic files acquired by each good peer. The squares represent the number of inauthentic files received by good peers in the EigenTrust model, and the circles represent the number of inauthentic files received by good peers in the GSBDBTrust model.

According to the behavioral characteristics of malicious peers, they are mainly divided into single peer malicious attacks and malicious group attacks. In order to verify that the GSBDBTrust model can reduce the number of inauthentic file downloads and reduce the unnecessary query interaction rate of peers, the simulation experiment demonstrates the following 4 threat models.

Threat Mode 1 Individual Malicious Peers. This threat model is one of the simplest attack models. When a malicious peer is selected as the download source, they always provide inauthentic files and malicious peers value inauthentic file downloads instead of authentic file downloads, namely, $s_{ij} = \text{unsat}(i,j) - \text{sat}(i,j)$. The simulation results are shown in Figure 1.

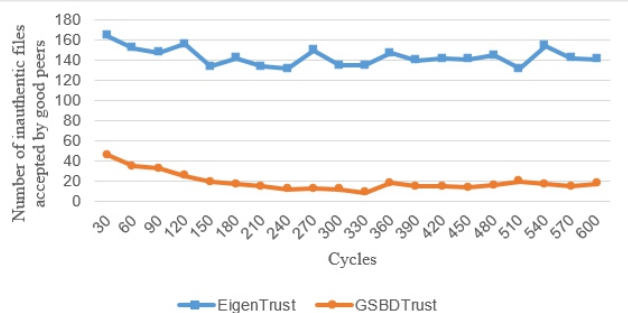


Figure 1: Individual Malicious Peers

From Figure 1, we can see that in the EigenTrust model, the good peers receive more unauthentic files than the GSBTrust model. Because in the group-based network model, the global trust value of ordinary peers is not high in the group without pre-trusted peers, the probability of the malicious peer being selected increases. Therefore, the authentic files received by the good peers in the network are higher than the EigenTrust model.

Threat Mode 2 Malicious Collectives. In threat mode 1, since malicious peers always provide unauthentic files, the global trust value will be very low, and the probability of being selected as a service peer will be reduced accordingly. In order to increase the probability of being selected, individual malicious peers will form a malicious group. In the malicious group, malicious peers form a malicious chain. When malicious peers in a group are selected as service peers, they always provide unauthentic files, but always give good feedback and evaluation to the neighbor peers in the group chain, that is, $tr_{ij}=1$. The simulation experiment results are shown in Figure 2.

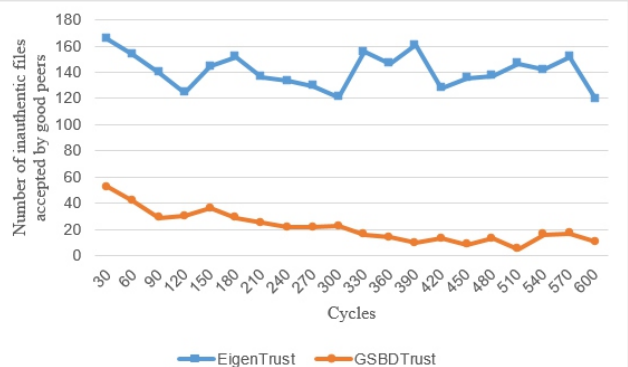


Figure 2: Malicious Collectives

It can be seen from Fig. 2 that the formation of a malicious chain between malicious peers does not improve the global trust value of the malicious peer, and the probability that the malicious peer is selected as the service peer is still very low. The system easily breaks up malicious groups through highly trusted pre-trusted peers. If pre-trusted peers are not present in the group, forming a malicious collective in fact heavily boosts the trust values of malicious peers [9]. In the GSBTrust model, there are pre-trusted peers in each group, which is easy to break up the malicious group. And thus more resistant than the EigenTrust model.

Threat Mode 3 Malicious Collectives with Camouflage. In threat mode 2, the malicious collective does not significantly improve the global trust value of the malicious peer. The probability of being selected as the service peer is still very low. In order to improve the global trust value in the network, they form malicious collectives with camouflage. In this threat model, a malicious peer can disguise its own behavior to destroy the system. When they are selected as service peers, they provide authentic files at $f\%$. The simulation experiment results are shown in Figure 3.

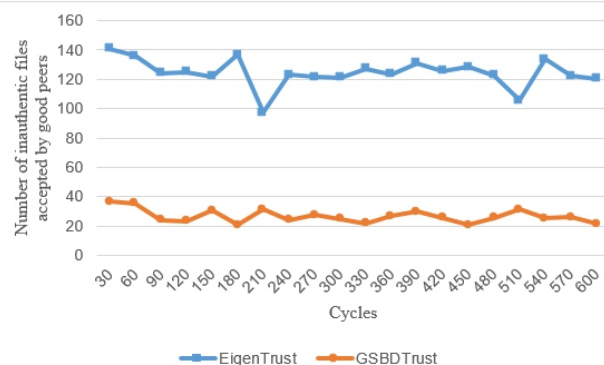


Figure 3: Malicious Collectives with Camouflage

In threat model 3, a malicious peer attempts to obtain a good evaluation from other peers by masquerading its own behavior. In this experiment, we set $f\%=20\%$. As can be seen from the figure 3, in the GSBTrust model, a small amount of real feedback evaluation still can not provide the global trust value of the malicious peers. In the GSBTrust model, each group of pre-trusted peers still breaks up the malicious camouflage group well, and the model still performs better than the EigenTrust model.

Threat Mode 4 Malicious Spies. In threat model 3, malicious collectives with camouflage provide 20% of authentic files that they are not willing to do. At the same time, saving authentic files also requires a certain amount of overhead. Therefore, under the condition of threat model 2, malicious peers are more willing to choose the most popular queries in the response network to form malicious spies. In this model, malicious peers answer 0.05% of the most popular queries and provide a authentic file when selected as service peer. The simulation experiment results are shown in Figure 4.

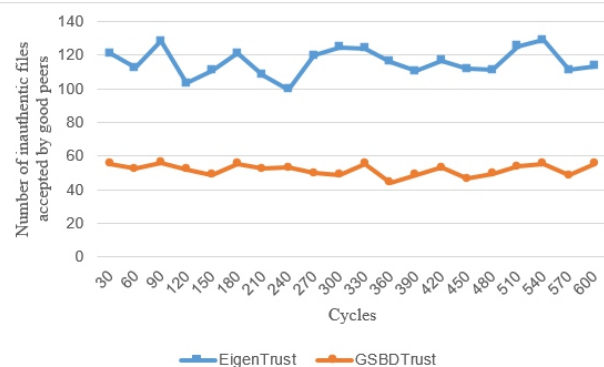


Figure 4: Malicious Spies

As can be seen from Figure 4, as in the previous models, the GSBTrust model dynamically selects peers with high global trust values as pre-trusted peers in the group-based structure to ensure stability within each group, and thus has more stability than the performance of EigenTrust model.

As we can see from the above 4 figures, GSBTrust model under various malicious models, the number of unauthentic files downloaded by good peers in the system is significantly smaller than that of the EigenTrust model. This is mainly due to the fact that the GSBTrust model can break up the malicious collectives well in the group-based structure, thus improving the response service of the good peers in the system.

For the network model with a community structure, peers cannot be effectively organized together, which greatly increases the unnecessary interaction between peers and increases the load on the system. In the P2P network model based on group structure, the peers can be well organized, and the number of interactions of peers in the group is significantly higher than that between the groups. In the process of query response, the resources to be requested can be found more quickly. And the query efficiency of P2P system is more efficient. Figure 5 shows the number of requested resources successfully queried by peers in the system under the GSBTrust model and the EigenTrust model.

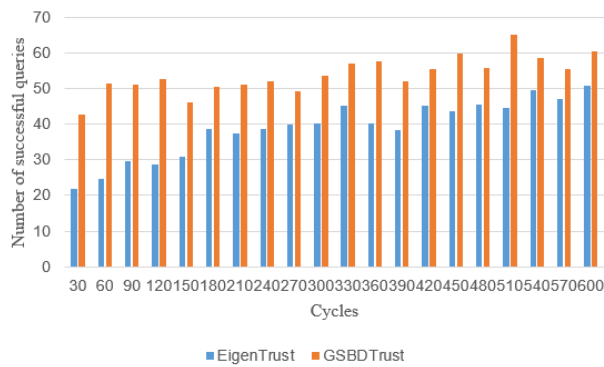


Figure 5: Number of successful queries

As can be seen from Figure 5, the number of peers requesting resources in the GSBDTrust model is higher than the EigenTrust model in the group-based network. This is because the GSBDTrust model is better able to adapt to P2P networks based on group structure, and the peers are organized together more efficiently, thus improving the number of successful queries.

5. CONCLUSION:

The trust model of P2P network is a current research hotspot. Based on EigenTrust algorithm, this paper proposes a GSBDTrust model based on group structure. The model is grouped according to the similarity of peers according to the community structure characteristics of peers in P2P networks. To ensure the robustness of the system, peers with higher global trust values are selected as pre-trusted peers in each group. At the same time, for the statically specified problem of the pre-trusted peer in the EigenTrust algorithm, this paper selects the peer with the highest global trust value as the pre-trusted peer dynamically based on the group structure to guarantee the high credibility of the pre-trusted peer. The simulation results show that the GSBDTrust model goes with good robustness under various threat models. At the same time, the success rate of the search is improved, the unnecessary interaction is reduced, as is the system load in the progress of request response search.

REFERENCES:

1. N.Inc. (2000): The napster homepage, available at <https://us.napster.com/music>, accessed 16 October 2018.
2. Ripeanu, M. (2001). Peer-to-Peer Architecture Case Study: Gnutella Network. Proceedings of the First International Conference on Peer-to-Peer Computing, Sweden: IEEE Computer Press.
3. Anderson, D. P. (2002). Seti@home: an experiment in public-resource computing. Communications of the ACM, New York: ACM New York, NY, USA, 56-61.
4. L. Gong. (2001). Project JXTA: A Technology Overview, Internet Computing, 5(3):88-95.
5. Tian, C., Jiang, J., Hu, Z., & Li, F. (2010). A novel super-peer based trust model for peer-to-peer networks. Chinese Journal of Computers, 33(2), 345-355.
6. Tian, C., Yang, B., Zhong, J., & Liu, X. (2014). Trust-based incentive mechanism to motivate cooperation in hybrid p2p networks. Computer Networks the International Journal of Computer & Telecommunications Networking, 73(C), 244-255.
7. Meng, X. (2018a). Speedtrust: a super peer-guaranteed trust model in hybrid p2p networks. Journal of Supercomputing, 74(9), 1-28.
8. Meng, X. (2018b). Suretrust: a super peer-aware trust model for 2-level p2p networks. Peer-to-Peer Networking and Applications, 11(3), 619-631.
9. Kamvar, Sepandar, D., Schlosser, Mario, T., GarciaMolina, & Hector. (2003). The eigentrust algorithm for reputation management in p2p networks. Proc. WWW2003.
10. Marsh, S. P. (1994). Formalising trust as computational concept. Thesis University of Stirling.
11. Mekouar, L., Iraqi, Y., & Boutaba, R. (2004). A reputation management and selection advisor schemes for peer-to-peer systems. Proceedings of the 15th IFIP/ IEEE International Workshop on Distributed Systems: Operations & Management. CA, USA, 3278, 208-219.
12. Xiong, L., & Liu, L. (2004). Peertrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge & Data Engineering, 16(7), 843-857.
13. Zhou, R., & Kai, H. (2007). Powertrust: a robust and scalable reputation system for trusted peer-to-peer computing. IEEE Transactions on Parallel & Distributed Systems, 18(4), 460-473.
14. Kenli Li, Yan He, Xiaoling Liu, et al. (2005). Security-driven scheduling algorithms based on eigentrust in grid[C]. Proceedings of the Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies, 1068-1072.
15. Chiluka, N., Andrade, N., Gkorou, D., & Pouwelse, J. (2012). Personalizing EigenTrust in the Face of Communities and Centrality Attack. IEEE, International Conference on Advanced Information NETWORKING and Applications (pp.503-510). IEEE Computer Society.
16. Hwang, K., Dongarra, J., & Fox, G. C. (2011). Distributed and cloud computing: from

parallel processing to the internet of things.

17. Kurdi, H. A. (2015). Honestpeer: an enhanced eigentrust algorithm for reputation management in p2p systems. Journal of King Saud University - Computer and Information Sciences, 27(3), 315-322.
18. Kurdi H.A. (2015). HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems[J]. Journal of King Saud University - Computer and Information Sciences, 27(3):315-322.
19. Tan Z, Wang X, Wang X. (2016). A Novel Iterative and Dynamic Trust Computing Model for Large Scaled P2P Networks[J]. Mobile Information Systems, 2016(4):1-12.