EnhanEigen: A New Comprehensive Trust Model for Peer-to-Peer Network

Xiali Li, Qiao Gao, Licheng Wu, Xun Sun and Songting Deng

1 Introduction

Different from the client/server model, peer-to-peer network has no central server and the peers are equally privileged, equipotent participants in the application. Peers share some resources such as processing power, disk storage or network bandwidth. Each peer can act as both server and client. It can request the service or respond to some requesting some resource [1–4].

Peer-to-peer networks have proven to be an effective way of sharing data and have been used in large scale file sharing system (Napster, Kazaa, Gnutella, eMule) [5], ecommerce [6, 7], instant messaging systems [8], distinct picture archiving and communication system (PACS) archives [9], cloud service selection [10, 11] and so on. Because of the open, anonymous nature of peer-to-peer network and their current level of popularity, users are increasingly concerned about defending attacks and threatens from malicious peers [12]. The notion trust is derived from psychology and sociology [13] and defined as a subjective expectation an entity has about another's future behavior [14, 15]. In trust model, peers gather information about other peers by using their network [16].

The trust model in eBay system is typically centralized structured and use central server to store and manage all user feedback scores and worthiness of the peers [17]. It is successful global reputation model. However, peers will not have any centralized authority to manage distribute reputation information. PeerTrust [18] is a coherent adaptive trust model based on a transaction-based feedback system. EigenTrust [19] proposed an algorithm which used global trust value to decrease inauthentic files downloading in peer-to-peer file sharing network. EigenTrust significantly decrease the number of unauthentic files on the network and can

X. Li · Q. Gao · L. Wu (✉) · X. Sun · S. Deng
Minzu University of China, Beijing 100081, China
e-mail: wulicheng@tsinghua.edu.cn

© Springer Nature Singapore Pte Ltd. 2018

Z. Deng (ed.), *Proceedings of 2017 Chinese Intelligent Automation Conference*,
Lecture Notes in Electrical Engineering 458,
https://doi.org/10.1007/978-981-10-6445-6_12

identify malicious peers. PowerTrust [20] used a trust overlay network to model the trust and generate the global trust value on the base of considering the power-law distribution of peer feedbacks. GossipTrust [21] is the extension of PowerTrust, proposed a gossip-based reputation system to aggregate global trust scores fast.

2 EnhanEigen Model

In the EnhanEigen trust model, each node stores the local trust values of all the other nodes of the entire network. After every transaction, the global trust value of the nodes will be updated by iterative calculation. We put forward two new parameters *MP* and *FCP* for each node to serve as the new evaluation criterion on judging the feedbacks. The comprehensive trust value is aggregated by the local trust value, global trust value, *MP* and *FCP*.

2.1 Local Trust Value

When two nodes in the network finish one transaction, we assume peer *i* downloads file *f* from peer *j*. The model asks the requiring party to evaluate the serving party's service. Each node in the network saves the local trust value for all other nodes in the entire net. The local trust value s_{ij} is calculated by the following equation

$$s_{ij} = sat(i,j) - unsat(i,j) \tag{2.1}$$

where *sat*(*i, j*) is the number of the times *i* feels satisfied with *j* in all the transactions, and *unsat*(*i, j*) is the number of the times *i* feels unsatisfied with *j* in all the transactions. If *i* offers satisfied evaluation on *j*, then add 1 to *sat*(*i, j*); otherwise add 1 to *unsat*(*i, j*).

To avoid malicious peers from giving higher value than the authenticity to the malicious peers, or giving lower value than the authenticity to the good peers, we make the local trust value normalization by the following equation

$$c_{ij} = \max((s_{ij}),0) \Big/ \sum_j \max((s_{ij}),0) \tag{2.2}$$

where c_{ij} is the normalized local trust value.

2.2 Global Trust Value

If peer i needs to know peer k's global trust value, it will firstly get peer k's credibility from all the nodes which transact with peer k directly, then combine the credibility with these nodes' own local credibility (from i's perspective) to finally work out k's global trust value t_{ik}. If we use matrix to represent it, we can get the following

$$\overrightarrow{t} = c^T \cdot \overrightarrow{c_i} \tag{2.3}$$

where c represents the matrix in which the element is $c(ij)$, c^T is the vector of the global trust value t_{ik}.

If peer i get peer k's global trust value by n times transitive inquiring its friends, we can get the global trust value by the following equation

$$\vec{t} = (c^T)^n \vec{c}_i \tag{2.4}$$

Introduce the pre-trusted peers, which never harm the network and has the preset trust value, then the global trust value is calculated by the following question

$$\vec{t}^{k+1} = a(c^T)\vec{t}^k + (1 - a)\vec{p} \tag{2.5}$$

where a is a constant that is between 0 and 1, $\vec{p}$ is the vector of pre-trusted value.

2.3 Malicious Percent (MP) and Feedback Consistency Percent (FCP)

EnhanEigen model uses the local trust value and global trust value concept of EigenTrust model. Apart from the global trust value, we introduce two parameters Malicious Percent (*MP*) and Feedback Consistency Percent (*FCP*) to help evaluate the trust value of one peer and filter the malicious and cheating peers in the network. The meaning of (*MP*) and (*FCP*) is illustrated in the following.

MP is the probability at which node i provides malicious service

$$MP_i = M_i/Tran_i \tag{2.6}$$

where M_i is the number of node i providing malicious services and $Tran_i$ is the number of node i providing all services.

FCP is defined as the following

$$FCP_i = Con_i/Recv_i \tag{2.7}$$

where $Recv_i$ is the number of i playing the roles of requiring peer.

2.4 Comprehensive Trust

Supposing node *i* finally select node *j* as its download source and successfully finishes file downloading in peer-to-peer file sharing network, now node *i* should offer its assessment to node *j*. The comprehensive trust value F_i are calculated by the following

$$F_i = \alpha t_i + \beta FCP_i - \gamma MP_i \tag{2.8}$$

where t_i is the global trust value of node *i*, FCP_i is feedback consistency rate of node *i*, MP_i is the probability at which node *i* provides malicious service. α, β, γ satisfies that α plus β plus γ equals 1.

Analyze the comprehensive trust value of good nodes, feedback cheating nodes and malicious slandering nodes respectively. Results are showed in the Table 1.

2.5 Resistance on the Malicious and Feedback Cheating Peers

In the peer-to-peer file sharing network, the following cooperative cheating behaviors may exist. Feedback cheating nodes (or malicious nodes) slander good nodes, feedback cheating nodes raise malicious nodes (or vice versa), feedback cheating nodes raise themselves, malicious nodes raise themselves. The model proposed in this paper make strict judgment both on the raising behavior from cooperative cheating nodes and slandering behavior on good nodes, which can dramatically reduce the possibility to succeed in feedback-cheating.

2.6 Enhanced Probabilistic Peer Selection Algorithm

Malicious nodes offers malicious service, such as uploading untrue files. Supposing node *i* requires to download file *f*, it finally receives a responding node set *S*. Accordingly, let *G* be the set of the global trust value of these *n* nodes, g_i is the global trust value of node *i*. Then we divide set *G* into two subset *A* and *B*.

The Enhanced Probabilistic Peer Selection Algorithm is described in the following.

Table 1 Comprehensive trust values of three kinds of nodes

	FCP	MP	F
G peers	High	Low	High
FC peers	Low	Low	Relatively high
MM peers	Low	Low	Relatively high

if $t_i = 0$, then we get the following set T

$$T = \{t_i \,|t_i \subseteq B \cap MP_i \leq \varnothing \cap \varnothing \, is \; a \text{ constant}\} \tag{2.9}$$

We choose t_i as the download source at the probability of 10%.

If $t_i \neq 0$, then we choose the node i from set A as the download source at the probability p

$$p = g_i \Bigg/ \sum_{j=1}^{A} g_i \tag{2.10}$$

This model adds MP to help assess the peer trust. There are two kinds of peers whose global trust value can be 0. One is that who offer malicious service and the other is the new adding peers in the net. EigenTrust choosing 10% of these nodes is to help new nodes establish their global trust value. At the same time 10% of these peers can maintain the balance between malicious peers and new entry peers. This can prevent malicious peers from getting big chance to upload false files.

3 Experiment and Analysis

We use java programming language to implement a peer-to-peer file sharing system in which EigenTrust model and EnhanEigen model are both used. To validate the performance of resisting cooperative-cheating, we divide experiment into two parts, one part is for MM peers and the other part is for FC peers. The parameters of the trust model are set as Table 2. To prevent the possible impacts on the simulation results for unreasonable files allocation, each file at least is owned by one good peer and each node has the same probability of requiring download files.

Each experiment is performed in the condition of 10 different distribution of files. In each distributing environment the model will loop 10 times. Thus each experiments finish 100 times files sharing. The reason that MP takes $\phi = 0.1$ as its threshold value is that type G nodes also have the probability (<10%) of offering malicious files, $\phi = 0.1$ is proper.

Table 2 Value of different parameters

	Total nodes	Total files	Total transactions	Preset trust nodes	MP thresh	α	β	γ
Value	50	300	10,000	5	0.1	0.2	0.5	0.3

3.1 MM Peers Experiments

In this experiment, we compared the performance of EnhanEigen and EigenTrust model from successful transactions ratio, algorithm execution time and false feedbacks adopted by the network at different malicious and slandering nodes percentage of the total nodes.

Figure 1 shows that EnhanEigen model performs better in defense against attacks from type MM than EigenTrust model. For EigenTrust model, at each percentage of MM nodes interval [0.1, 0.3], [0.3, 0.5], [0.5, 0.7], [0.7, 0.9], the success ratio curve has a slope approximately. But for EnhanEigen, the curve has only a little change. Even when MM nodes account for 90% of all the nodes in the net, the successful ratio is still near 90%. Figure 2 shows that the algorithm execution time at different malicious and slandering nodes ratio of the two models. For the two models, there are a inflection point (about at 50%) of the percentage of malicious and slandering peers. Figure 3 show false feedback adopted by network at different proportion of MM nodes. When MM nodes accounts for less than 50%, the EnhanEigen model can't influence the net hardly.

3.2 FC Peers Experiments

For cooperative cheating experiment, each time MP nodes and FC nodes account for half of all malicious nodes. Namely, each time we will let equivalent FC nodes raise MP nodes and slander other G nodes.

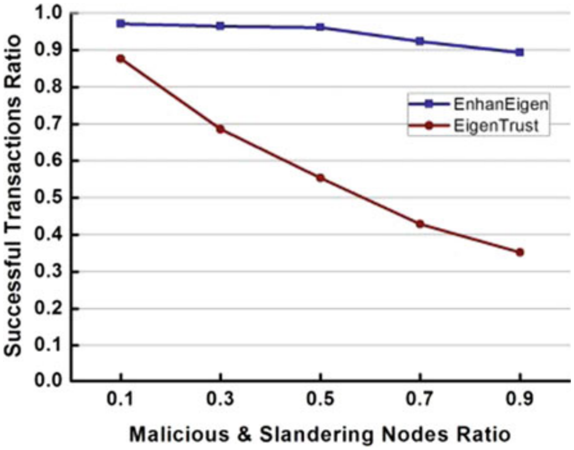


Fig. 1 Successful transactions ratio in different MM ratio

Fig. 2 Algorithm execution time at different MM peers

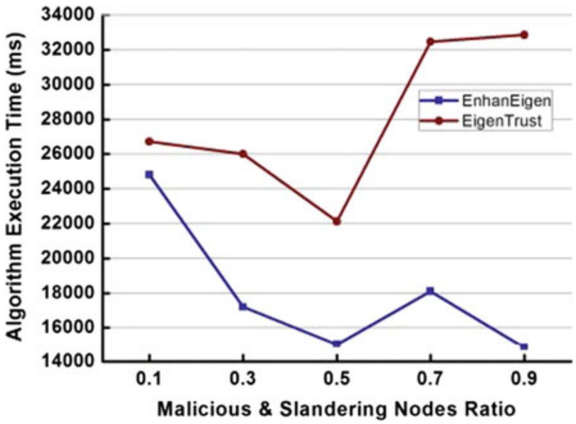


Fig. 3 False feedbacks adopted at different MM peers ratio

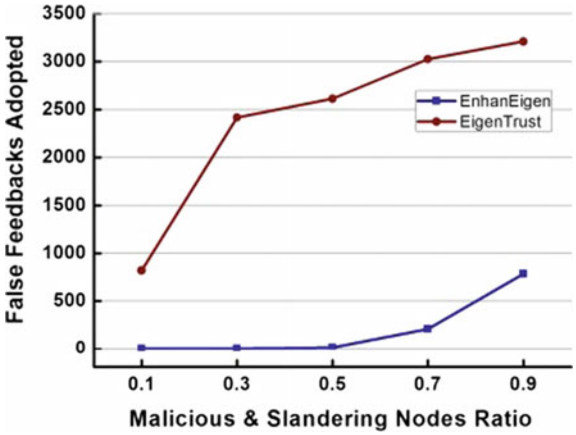


Figure 4 show that the two models have the inflection point at about 70 proportion of the cooperative cheating nodes. Before this point, the two curves are slopping and the EnhanEigen model slopes gently. After the point, the two curves all rise. It is obviously that EnhanEigen model plays better than Eigen Trust in defense against cooperative cheating. Figure 5 shows the algorithm execution time contrast between the two models. EnhanEigen model does not have obvious advantages on the algorithm execution time at different cooperative cheating peers. Figure 6 show false feedback adopted by network at different proportion of cooperative cheating nodes. EnhanEigen model adopted much fewer false feedbacks than EigenTrust.

Fig. 4 Successful transactions ratio at different FC peers ratio

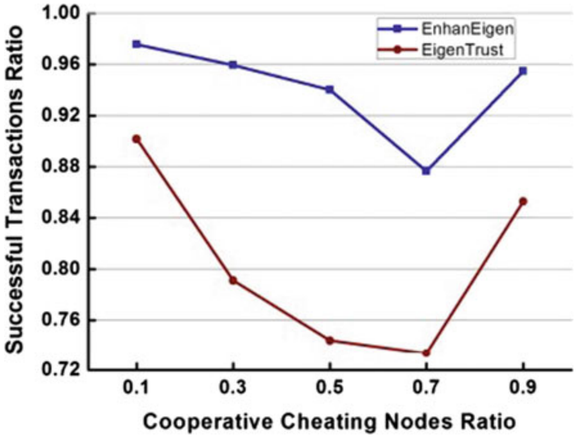


Fig. 5 Algorithm execution time at different FC peers ratio

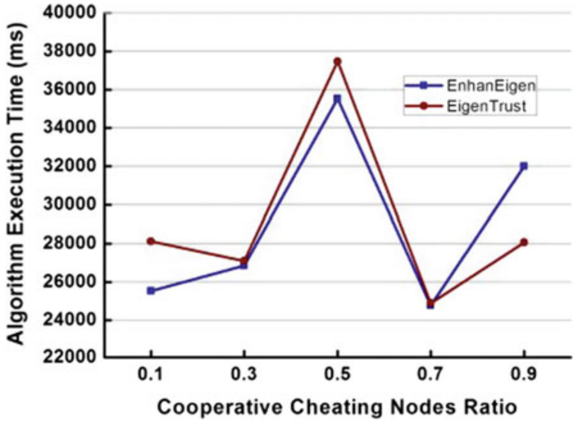
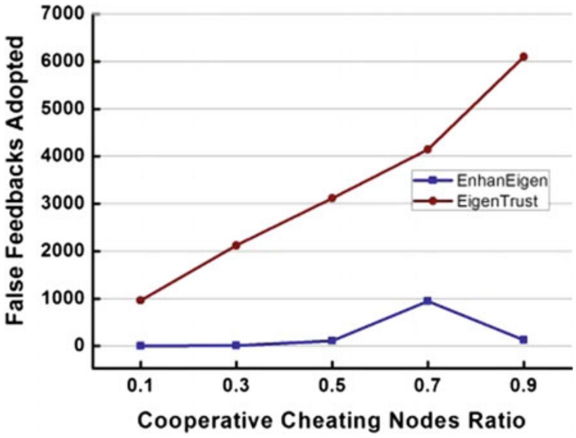


Fig. 6 False feedbacks adopted at different FC peers ratio



4 Conclusion

EnhanEigen trust model propose comprehensive trust value and enhanced probabilistic peer selection algorithm to overcome the shortages that previous trust models can't effectively judge the feedback authenticity and resist cooperative feedback cheating peers. This comprehensive trust is aggregated by local trust value, global trust value, Malicious Percent (MP) and Feedback Consistency Percent (FCP). *MP* and *FCP* are used to filter the malicious peers when selecting peers providing service. Experiments validate that new trust model can distinguish and judge the authenticity of feedbacks, resist the cooperative attacks from malicious peers and feedback cheating peers effectively.

Acknowledgements This paper is supported by the National Science Foundation (Granted number is 61602539 and 51375504).

References

1. Yang M, Yang Y (2014) Applying network coding to peer-to-peer file sharing. IEEE Trans Comput 63(8):1938–1950
2. Dharanipragada J, Chennai J, Haridas H (2012) Stabilizing peer-to-peer systems using public cloud: a case study of peer-to-peer search. In: Proceedings of 11th international symposium on parallel and distributed computing (ISPDC), IEEE, Munich, Germany, pp 135–142
3. Haase P, Siebes R, van Harmelen F (2008) Expertise based peer selection in peer-to-peer networks. Knowl Inf Syst 15(1):75–107 (Periodical style)
4. Schollmeier PR (2001) A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: Proceedings of the first international conference on peer-to-peer computing, IEEE, Linkoping, Sweden, pp 101–102
5. Yu J, Li M (2008) CBT: a proximity-aware peer clustering system in large-scale BitTorrent-like peer-to-peer networks. Comput Commun 31(3):591–602 (Periodical style)
6. Feigenbaum J, Parkes DC, David M (2009) Computational challenges in e-commerce. Commun ACM 52(1):70–74 (Periodical style)
7. Beatty P, Reay I, Dick S, Miller J (2011) Consumer trust in e-commerce web sites: a meta-study. ACM Comput Surv 43(14):1–46 (Periodical style)
8. Hoffman K, Zage D, Nita-Rotaru C (2009) Expertise-based peer selection in peer-to-peer networks. A survey of attack and defense techniques for reputation systems. ACM Comput Surv 42(1):1–31 (Periodical style)
9. Oliveira L (2012) Clustering of distinct PACS archives using a cooperative peer-to-peer network. Comput Methods Programs Biomed 108(3):1002–1011 (Periodical style)
10. Fan W-J, Yang S-L, Perros H, Pei J (2015) A multi-dimensional trust-aware cloud service selection mechanism based on evidential reasoning approach. Int J Autom Comput 12 (2):208–219
11. Noor TH, Sheng QZ, Zeadally S, Yu J (2013) Trust management of services in cloud environments: obstacles and solutions. ACM Comput Surv 46(1):12
12. Hughes D, Coulson G, Walkerdine J (2005) Free riding on Gnutella revisited: the bell tolls. IEEE Distrib Syst Online 6(6):1–18
13. Marsh SP (1994) Formalising trust as a computational concept. Ph.D. dissertation, University of Stirling, UK

14. Mui L (2003) Computational models of trust and reputation: agents, evolutionary games, and social networks. Ph.D. dissertation, Massachusetts Institute of Technology, USA
15. Mui L, Mohtashemi M, Andhalberstadt A (2002) A computational model of trust and reputation. In: Proceedings of the 35th Hawaii international conference on system sciences (HICSS02), IEEE, Los Alamitos, Canada, pp 188–196
16. Sherchan W, Nepal S, Paris C (2013) A survey of trust in social networks. ACM Comput Surv 45(4):1–33
17. Stoica I, Morris R, karger D, Kaashoek F, Balakrishnan H (2001) Chord: a scalable peer-to-peer lookup service for internet applications. In: Proceedings of special interest group on data communication, ACM, California, USA. Availabe: http://www.cse.iitb.ac.in/dbms/Data/Courses/CS632/2010/Papers/chord.pdf
18. Xiong L, Liu L (2004) PeerTrust: supporting reputation based trust for peer-to-peer electronic communities. IEEE Trans Knowl Data Eng 16(7):843–857
19. Kamvar SD, Schlosser MT, Garcia-Molina H (2003) The EigenTrust algorithm for reputation management in P2P networks. In: Proceedings of the 12th international conference on world wide web, New York, USA, pp 640–651
20. Zhou R, Hwang K (2007) PowerTrust: a robust and scalable reputation system for trusted peer-to-peer computing. IEEE Trans Parallel Distrib Syst 18(5):1–14
21. Zhou R, Hwang K, Cai M (2008) GossipTrust for fast reputation aggregation in peer-to-peer networks. IEEE Trans Knowl Data Eng 20(9):1282–1295