An Effective Trust Evaluation Scheme against the Malicious Nodes in P2P Network

Do-sik An[1], Byong-lae Ha[2], Gi-hwan Cho[1,*]

[1] Div. of Computer Science and Engineering(Cloud Open R&D Center), Chonbuk National University, Jeonju, South Korea
[2] Div. of IT Center, NongHyup, Seoul, South Korea
[1]{rokmcads, ghcho}@jbnu.ac.kr
[2]honest521@nonghyup.com

Abstract. By adapting the trust concept prevailing in human life to computer network, a trust evaluation scheme has been widely investigated to prevent malicious threats. However, there will be security threats in the scheme itself. That is, a malicious peer can affect other peers in bad by providing them a dishonest opinion. This paper aims to propose an effective trust evaluation scheme to improve reliability and effectiveness of P2P network by identifying these malicious threats and then limiting the attacker's participation. The proposed scheme is expected to effectively protect attacks from malicious peers with improving credibility as well as exactness.

Keywords: P2P network, Trust Evaluation, Direct Trust, Indirect Trust

1 Introduction

It is very important to retain a trust among the constituted nodes in P2P network due to the lack of central server. In addition, P2P network has advantage of overcoming a single node failure and shows great flexibility compared with the conventional client-server model. If all nodes normally participate to a network, the network status will be very safe. However, when the resources are falsified by any peer with malicious purpose, the mutual trust between users is reduced resulting in degrade of service quality[1].

To prevent these malicious threats, a trust evaluation scheme has been widely investigated by adapting the trust concept prevailing in human life in to computer network[2-6]. Most existing researches just tried to distinguish the untrustworthy users who are sharing the same resource, but they did not consider the user who gives a trust evaluation the threat and honesty of trust value itself. Their works also were quite unclear to distinguish the malicious users.

In this paper, we deal with an effective trust evaluation scheme against the malicious nodes' attacks. The proposed scheme utilizes a time decay function to

[*] Corresponding author.

reflect much the recent trust than that of the past. It also utilized credibility as well as similarity among the users to efficiently reflect the trust value offered by adjacent nodes.

2 Proposed Scheme

2.1 Overview

Trust on the proposed scheme is consisted of two values; direct trust and indirect trust. As shown in Fig. 1. below, direct trust value is calculated by evaluating the neighbor node(C, D) based on its own experience. In case of indirect trust value, neighboring node D evaluates node E using formulaic method, and informs the value to node A; that is a recommended trust value. By using these trust values(direct and indirect), resources could be safely provided from which shows the most highest trust value. Thereafter, trust value for each node is renewed by re-evaluating the direct and indirect trust values.

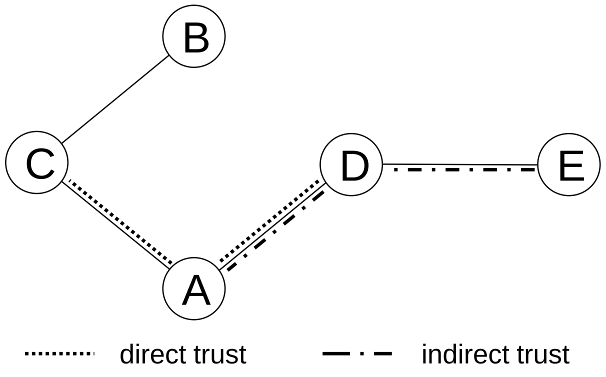

Fig. 1. Direct trust vs. indirect trust

The whole trust evaluation is as equation (1). T_{ij} means node *i* evaluates trust for node *j*.

$$T_{ij} = \alpha \times DT_{ij} + (1-\alpha) \times IdT_{ij} \qquad (1)$$

DT_{ij} is a direct trust value which node *i* evaluates node *j* based on node *i* experiences. Idt_{ij} is an indirect trust value by adjacent nodes. α is a confidence factor which means how the node *i* is able to be convinced for the direct trust value by itself. If the node *i* communicates with node *j* k^{th} times, the confidence factor can be calculated like equation (2) and here, the threshold stands for the number of communication.

$$a = \begin{cases} k^{th} / Threshold, & k^{th} < Threshold \\ 1 & , \ else \end{cases} \tag{2}$$

2.2 Direct Trust

When node *i* communicates with another node directly, node *i* is able to evaluate it based on his experiences. This direct trust is presented as DT_{ij}. If node *i* communicates with node *j* k^{th} times, we are able to calculate the satisfaction value, that is, ex_{ij}^{k}, which is expressed as equation (3) bellow. Using this satisfaction value, we can calculate the direct trust value for node *j*, that is, DT_{ij}, which follows as equation (4). The number of communication k has the value of k=1, 2, ..., n.

$$ex_{ij}^{k} = \begin{cases} 1, \ satisfactory \\ 0, \ unsatisfactory \end{cases} \tag{3}$$

$$DT_{ij} = \frac{\sum_{k=1}^{n} f(x) \times ex_{ij}^{k}}{\sum_{k=1}^{n} f(x)} \tag{4}$$

The satisfaction value of each communication is obtained by mapping the time decay function *f*(*x*) as *f*(*x*) = λ^{n-k}. Thus, *n* means the number of communications, which has a range of $0.5 \le \lambda \le 1$, $1 \le k$.

2.3 Indirect Trust

Indirect trust can be calculated based on similarity of two nodes and the trust value of node offering confidential value. Its value is able to be evaluated using the equation (5) below.

$$IdT_{ij} = \frac{\sum_{k=1}^{n} CR_{im} \times DT_{mj}^{New}}{\sum_{k=1}^{n} CR_{im}} \tag{5}$$

DT_{mj}^{New} reflects the number of communication with the direct trust value of node *m*, which is calculated as equation (6). Thus, *n* indicates the communication times between the node *m* and the node *j*. β is a scaling factor to keep the direct trust, and it has the range as $0.5 < \beta \le 1$.

$$DT_{mj}^{New} = DT_{mj} \times \beta^{\frac{1}{n}} \tag{6}$$

Credibility presented as CR_{im} is an inter-peer evaluated value for node *m* in the point of view of node *i*. When the node *m* offers the indirect trust value of the node *i*, node *i* evaluates the indirect trust value by its own regulation in order to be applied as an trust value of node *m*.

3 Conclusion

In this paper, we proposed a trust evaluation scheme to treat attack against malicious nodes based on user's trust value in P2P network environment. Especially, our scheme focused on false rating and on-off attack. We utilized the user credibility as well as the similarity among the users to efficiently reflect the trust value offered by adjacent nodes. For the future work, we are going to simulate the proposed scheme with variable attack scenarios(that is, bad mouthing, on-off and etc.) along with further refinement.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(KRF) funded by the Ministry of Education, Science and Technology (2012R1A1A2042035)

References

1. Liu, Y. H.: A Two-hop Solution to Solving Topology Mismatch. In: IEEE Transactions on Parallel and Distributed Systems, 19 (11), pp. 1591--1600. (2008)
2. Kamvar, S., Schlosser, M.: The Eigentrust Algorithm for Reputation Management in P2P Networks. In: 12th International Conference on World Wide Web, pp. 640—651. (2003)
3. Zhou, R. F., Hwang, K.: PowerTrust: a Robust and Scalable Reputation System for Trusted Peer-to-peer Computing. In: IEEE Transactions on Parallel and Distributed Systems, 18 (4), pp. 460-473. (2007)
4. Abrams, Z., McGrew, R., Plotkin, S.: A Non-manipulable Trust System based on EigenTrust. In: ACM SIGecom Exchanges, 5(4), pp. 21--30. (2005)
5. Rao, S., Wang, Y., Tao, X.: The Comprehensive Trust Model in P2P Based on Improved EigenTrust Algorithm. In: International Conference on Measuring Technology and Mechatronics Automation, pp.822--825. (2010)
6. Zhang, Y. C., Chen, S. S., Yang, G.: SFTrust: a Double Trust Metric based Trust Model in Unstructured P2P System. In: 23rd IEEE International Parallel & Distributed Processing Symposium, pp. 1--7. (2009)