Correlation Trust Authentication Model for Peer-to-Peer Networks

Wei Cheng
Information Security Institute
Software College of Northeastern University
Shenyang, China

chengw@mail.neu.edu.cn

Zhenhua Tan
Information Security Institute
Software College of Northeastern University
Shenyang, China
(Corresponding author)
tanzhenhua192@126.com

***Abstract*—A requester node requesting a service in a peer to peer network transmits a request to a service provider node. The request may include a communication history of the requester node identifying other nodes with which the requester node has previously communicated. The service provider node authenticates the requester node based on the communication history. The service provider node may ask other nodes with which the requester node has communicated for evaluation of the requester node. The other nodes may calculate a trust metric of the requester node and provide this metric to the service provider node. The service provider node may use this trust metric in combination with a similarity calculation of the requester node and the service provider node to make a determination whether the requester node is to be authenticated. The service provider node may evaluate the requester node and store the evaluation in its communication history.**

Keywords-p2p, network security, trust model

I. Introduction

Communication nodes are often interconnected through networks. Peer-to-peer networks include communication nodes communicating with other communication nodes. The nodes may communicate with each other, share information, provide services, and perform other network interactions. Peer-to-peer networks may be decentralized, without a central network authority. Thus, communication nodes in a peer-to-peer network may be thought of as peers or equals. Authentication in a peer-to-peer network helps ensure that content communication between nodes in the network is safer.

In a peer-to-peer network one node can share information with another node. For example, node A as a service provider can share locally stored information or data such as video, audio, and the like, with node B. Node B can then download/transfer the information/data from node A. In a situation where no authentication mechanism is provided, many undesirable situations may arise. For example, some nodes may only obtain services and provide no services themselves, some nodes may provide malicious services, some nodes may undermine resources on other nodes, and some malicious nodes may act as a group to cheat other nodes.

Many researchers dedicated themselves to the P2P trust model. But what is trust? In social networks, trust has several connotations, the typical definition of trust follows the general intuition about trust and contains such elements as: (1) the willingness of one party (trustor) to be vulnerable to the actions of another party (trustee); (2) reasonable expectation (confidence) of the trustor that the trustee will behave in a way beneficial to the trustor; (3) risk of harm to the trustor if the trustee will not behave accordingly; (4) and the absence of trustor's enforcement or control over actions performed by the trustee. In 1990s, Marsh [8] uses the definition by Gambetta [1], which is commonly accepted in the literature: "…trust, (or symmetrically, distrust) is a particular level of the subjective probability with which an agent will perform a particular action, both before he can monitor such action (or independently of his capacity to monitor it) and in a context in which it affects his own action." Almost all of the related works on trust is based on the above definitions.

Trust is very important to a distributed P2P system. Many researchers do contributions to the P2P trustworthy issues [2-9] in recent ten years.

Aberer and Despotovic [2] propose a complaint-only trust management method for a distributed P2P system, due to the lack of incentives for submitting feedbacks. The complaint-only trust metric works in very limited cases and is over-sensitive to the skewed distribution of the community and to several misbehaviors of the system. Although this mechanism has some limitations, it is the very early trust model for P2P E-commerce.

Kamvar et al. present the EigenTrust reputation system [3] to compute a unique global trust in very distributed way. Such a global model does not need an administration center, but it is difficult to guarantee a fast and secure convergence when computing the global trust. And it inspires our works.

Dou and Wang et al. [4] improve the EigenTrust in computing convergence and model security. However, there remain efficiency problems and its security mechanism is only from punishment and certification.

Xiong and Liu [5] propose a PeerTrust model with three basic trust parameters and two adaptive factors in computing trust of peers, and then define a general trust metric to combine them.

Published by Atlantis Press, Paris, France.
© the authors

Jøsang et al. [6] propose a method for simplifying a complex network so that it can be expressed in a series parallel network and then be computationally analyzed. This solution may lead to loss of trust information. An edge splitting method is proposed in their further works [7] to address this problem. But this method is valid only on a simple trust network. It may not be valid on a complex trust network.

Wang and Wu [8] propose a multi-dimensional evidence-based trust management system with multi-trusted paths (MeTrust for short) to conduct trust computation on any arbitrarily complex trusted graph. The trust computation in MeTrust is conducted at three tiers, namely, the node tier, the path tier, and the graph tier. It is an excellent trust model. But it doesn't provide distributed storage structure for P2P system.

Jiang at el. [9] present a novel reputation-based trust mechanism for P2P e-commerce systems. In this mechanism, a peer has two kinds of reputations, namely local reputations and global reputations. To compute the local and global reputations precisely and to obtain stronger resistibility to attacks as well, many comprehensive factors in computing trust value are introduced in the mechanism. Anyway, this model is a comprehensive mechanism. However, its time factor is only linear to express the time's importance and there is no clear method to resist team malicious behaviors.

Generally speaking, trust models above can be classified into two modes, one is local information based and one is global trust information based. The local trust of a peer relative to another peer is calculated in terms of the reference peer's rating of the transaction between the two peers, whereas the global trust is computed based on all peers' rating of the transaction between them.

II. DETAILED DESCRIPTION

In an embodiment, an authentication method may include receiving at a service provider node a request for a service from a requester node. Further, the authentication method may include authenticating the requester node based on a communication history of the requester node included in the request for the service. Further, the method may include determining whether to provide the service to the requester node based on a result of the authenticating, and providing the service when it is determined that a service should be provided.

An authentication method may also include receiving from the requester node at the service provider node a communication history of the requester node, the communication history including identification of nodes with which the requester node has previously communicated. These other nodes may be peer nodes in a peer to peer network.

An authentication method may also include determining one or more other nodes belonging to the communication history of the requester node, transmitting to those other nodes a request for evaluation of the requester node, receiving from those other nodes an evaluation of the requester node based on the request for evaluation, and determining whether to authenticate the requester node based on the evaluation received from the other nodes.

An authentication method may also include calculating a global trust degree of the requester node as a weighted average of the evaluations given to the requester node by the other communication nodes. In addition, the authentication method may include calculating a relative trust degree based on the global trust degree and a similarity calculation of the service provider node and the requester node. The relative trust degree may be compared to a predetermined threshold to determine whether the requester node is to be authenticated.

The correlation of appraisals by two different nodes is used to describe the associated extent of the specified two nodes via computing the history among these two nodes and their common third-party nodes. This situation is similar to social networks in judging a strange person. For example, A didn't know B, but both share common friends {C, D}, then A can judge the correlation with B via his friends {C, D}. If the communicated history between A-{C, D} is similar to the history between B-{C, D}, then we call A and B have very similar correlation.

The local trust degree is the trust expectation of one node to another node according to the transaction history data between the two nodes. From the perspective of social networks, higher transaction frequency, more transaction amount and better appraisals will help the trust value between nodes. Meantime, elder transaction history should give lighter impact on the trust computing. Therefore, we discuss three factors for local trust firstly, including time factor, transaction amount factor and frequency factor.

Using TL_{ij} to express the local trust degree of node j which is computed by node i. In other words, from the perspective of node I, the TL_{ij} is the trust expectation of node j. It is composed of appraisals, time stamp, amount and frequency, ranged between [-1, 1]. Assumed the TL_{ij}=0 at the initialized time and max=s_{ij}+f_{ij}. And:

$$TL_{ij}=\begin{cases}0, & time=t_0^i\\ \sqrt[5]{\sum_{m\in[1,\max]}\left(tf_m^{ij}\bullet\omega f_m^{ij}\bullet\varphi f_m^{ij}\bullet\phi_m^{ij}\right)\Big/\max}, & time=others\end{cases}$$

Local trust has some limitations on evaluating nodes' trust because of the computed history only comes from the related two nodes (nodes i and j) and couldn't avoid single malicious node's cheating or data attacking. For example, node may revise its history data or give false appraisal to a transaction.

Via average value method, the global trust degree is multiplied by three decimal fractions who are global success rate factor λ_i^{now}, global frequency factor φ_{now}^i and global time factor gf_j^i. Thus, to facilitate the computing and analysis, we amplify the result by extract the result three times. Formula for global trust degree (ranged between [-1,1]) is:

$$TG_i = \sqrt[3]{\left(\sum_{c\in I_i} \left(gf_c^i \bullet TL_{ci} \right) \Big/ Count(I_i) \right) \bullet \lambda_i^{now} \bullet \varphi_{now}^i}$$

Unlike the local trust degree, the global trust degree can avoid malicious behaviors from single node. However, it can't defend attacks from team malicious nodes that are cooperated with each other as a team. For example, the global trust degree couldn't recognize malicious team nodes' high appraisals to each other. Thus, a correlation trust degree is created.

The calculation of the correlation trust degree may be based on the formula

$$CorTG_{ij} = \begin{cases} \min(0, TG_j) & (sim(i,j) = 0) \\ sim(i,j) \bullet TG_j & (sim(i,j) > 0) \end{cases},$$

wherein sim (i,j) is the similarity of the service provider node and the requester node.

The similarity of the service provider node and the requester node may be calculated according to the formula

$$sim(i,j) = \left| \frac{\sum_{c\in I_{ij}} (TL_{ic} - \overline{R_i})(TL_{jc} - \overline{R_j})}{\sqrt{\sum_{c\in I_{ij}} (TL_{ic} - \overline{R_i})^2} \sqrt{\sum_{c\in I_{ij}} (TL_{jc} - \overline{R_j})^2}} \right|$$

wherein Iij is a set of common nodes that are present both in a communication history of the service provide node and the communication of requester node, Tic is a trust evaluation of node c by the service provider node, Tjc is a trust evaluation of node c by the requester node, $\overline{R_i}$ is normalized average evaluation given by the service provider node to nodes in the communication history of the service provider node, and $\overline{R_j}$ is a normalized average trust evaluation given by the requester node to nodes in the communication history of the requester node.

The sim(i, j) ranged between [0, 1], and the similarity increases when the value sim(i,j) increased. Nevertheless, it would be error when the denominator in formula above is zero. We couldn't get the similarity at that time. Moreover, it would be trouble when nodes in I_{ij} (which are the common third-party nodes) are so very rare that can't calculate the similarity. To solve these problems, we adjust the similarity formula and assume that sim(i, j) equals to zero when $Count(I_{ij}) < \tau$ (τ is a settable threshold value by user). The adjusted formula is:

$$sim(i,j) = \begin{cases} 0, when \sqrt{\sum_{c\in I_{ij}} (TL_{ic} - \overline{R_i})^2} \sqrt{\sum_{c\in I_{ij}} (TL_{jc} - \overline{R_j})^2} = 0, or Count(I_{ij}) < \tau; \\ \left| \frac{\sum_{c\in I_{ij}} (TL_{ic} - \overline{R_i})(TL_{jc} - \overline{R_j})}{\sqrt{\sum_{c\in I_{ij}} (TL_{ic} - \overline{R_i})^2} \sqrt{\sum_{c\in I_{ij}} (TL_{jc} - \overline{R_j})^2}} \right|, else \end{cases}$$

In an authentication method where a calculated relative trust degree is compared to a predetermined threshold, the threshold may be set individually for each node participating in a peer-to-peer network, or the threshold may also be set uniformly across all nodes in the network.

An authentication method may also include requesting a service from a service provider node and including as authentication credentials a communication history in the request for service. The authentication method may also include receiving the requested service from the service provider node based on the authentication credentials. The communication history may span a predetermined time period.

An authentication method may also include generating a request for the service in a service module of the requester node, providing the request for the service from the service module to an authentication module of the requester node, and adding to the request for the service the communication history of the requester node.

An authentication method may also include evaluating the service provider node based on the received service, and updating the communication history of the requester node based on the evaluating.

An authentication method may include receiving from a service provider node a request for a communication history between a peer node and a service requester node. The method may also include generating a trust metric of the requester node at the peer node, and transmitting the communication history and the trust metric of the service requester node to the service provider node.

The trust metric of the service requester node may be calculated based on the equation $T_{ij} = TS_{ij} + TF_{ij}$, where $TS_{ij} = S_{ij} / (S_{ij} + F_{ij})$, $TF_{ij} = (-1) \times F_{ij} / (S_{ij} + F_{ij})$, Sij is a count of successful communications between the peer node and the requester node, and Fij is a count of failed communications between the peer node and the requester node.

In an alternative embodiment, an apparatus may include an authentication module configured to receive a request for a service, and a service module configured to provide the requested service to a requester apparatus, based on authentication performed by the authentication module.

The communication history of the requester apparatus may include identification of one or more other communication apparatuses with which the requester apparatus has communicated.

Further, the authentication module may include a first determining unit configured to determine one or more other communication apparatuses belonging to the communication history of the requester apparatus, a transmitter configured to transmit to the one or more communication apparatuses a request for evaluation of the requester apparatus, a receiver configured to receive from the one or more other communication apparatuses an evaluation of the requester apparatus in response to the request for evaluation, and a second determining unit configured to determine whether to authenticate the requester apparatus based on the evaluation received from the one or more other communication apparatuses.

The authentication module may also include a calculator configured to calculate a global trust degree of the requester apparatus as a weighted average of evaluations given to the requester apparatus by the one or more other communication apparatuses. Further, the authentication module may include a second calculator configured to calculate a relative trust degree based on the global trust degree and a similarity of the apparatus and the requester apparatus. Further, the authentication module may also include a comparator configured to compare the relative trust degree to a predetermined threshold value.

The threshold may be set individually at each apparatus, or set globally to be equal across all apparatuses in a network.

The apparatus may also include a memory storing the communication history of the apparatus. The communication history stored in the memory may be updated after the apparatus provides a service to a requesting apparatus. Further, the memory may also be updated to indicate that the service was successfully provided to the requesting apparatus or that the service was not successfully provided. The requesting apparatus may also have a memory storing communication history indicating whether the service provided by the service provider apparatus was a success or a failure.

III. Simulations and Conclusions

In order to verify the rightness of the proposed trust model, we design a simulation platform by C# programming language, and simulate the P2P environment with multi processes and threads. Three kinds of nodes are designed.

(1) Class A. It describes the normal and 'good' nodes that provide correct appraisals and good service in P2P E-commerce system.

(2) Class B. It describes single malicious node in P2P E-commerce system, providing false service and making false appraisals. But this kind of node doesn't work coordination with other malicious nodes.

(3) Class C. It describes team malicious nodes in P2P E-commerce system, providing dishonest service and giving incorrect appraisals to A nodes or B nodes. At the same time, these C nodes overstate appraisals to each other.

Assumed TotalCount is the total transaction times and BC_Count is the total transaction times with B-nodes or C-nodes which are malicious nodes. Then, the download-resisting performance from malicious nodes could be described as

$$dr = \frac{BC\_Count}{TotalCount}$$

. For example, a node from A-nodes has 100 transactions, and 20 transactions with B-nodes or C-nodes, then the download-resisting performance is dr=20%. We do statistics of the download-resisting performance for these trust models. Figure 1 shows the results.

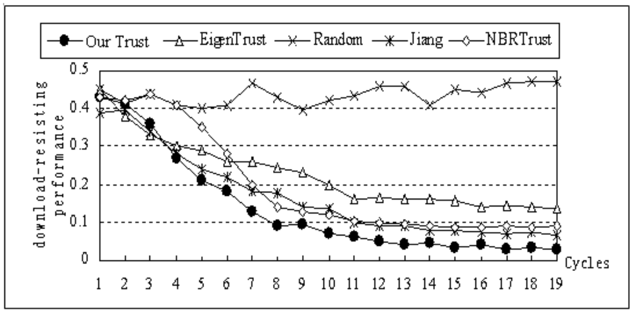

Figure 1. Download-resisting performance for these trust models

As we can see, the random model had the worst performance while the proposed trust model had the best convergence. EigenTrust and Jiang had also good convergences but they couldn't resist team malicious nodes. This result proved rightness and is effective of the proposed trust model.

References

[1] Gambetta, D.: 'Can we trust Trust?' in Gambetta, Diego (ed.) Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, Basil Blackwell. (2000)

[2] Aberer K., Despotovic Z.: Managing trust in a peer-to-peer information system. In proceedings of the 10th International Conference on Information and Knowledge Management, ACM Press, Atlanta, GA, United states, 1-7. (2001)

[3] Kamvar S.D., Schlosser M.T., GarciaMolina H.: The EigenTrust algorithm for reputation management in P2P networks. In proceedings of ACM WWW 2003, 640-651. (2003)

[4] Dou W., Wang H. M., Jia Y.: A recommendation-based peer-2-peer trust model. Journal of Software, Vol.15, no.4, 571−583. (2004)

[5] Xiong L., Liu L.: PeerTrust: supporting reputation-based trust for Peer-to-Peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, Vol.16, no.7, 843-857. (2004)

[6] Jøsang A., Hayward R., Pope S.: Trust network analysis with subjective logic. In proceedings of ACSC 2006, 85-94. (2006)

[7] Jøsang A., Bhuiyan T.: Optimal trust network analysis with subjective logic. In proceedings of SECURWARE 2008, 179-184. (2008)

[8] Wang G., Wu J.: Multi-dimensional evidence-based trust management with multi-trusted paths. Future Generation Computer Systems, doi:10.1016/j.future.2010.04.015, in press. (2010)

[9] Jiang S. X., Li J. Z.: A Reputation-Based Trust Mechanism for P2P E-Commerce Systems. Journal of Software, Vol.18, no.10, 2551-2563. (2007)