Construction of Credit based Distributed Trust Management Model for P2P Network

Han Yingjun, Lian Hongjun
North China University of Science and Technology
Hebei, 063009, China
yjhanh@163.com

ABSTRACT: *With the emerging of peer-to-peer (P2P) network in recent years, unsafety problems underlying becomes more obvious, such as dishonest recommendation, collusive cheat and complex strategic attack behavior. But the current trust model is able to process the above problems in a better way. Thus this study proposes a credit-based distributed trust management model for P2P, named RA Trust and applies it to quantify and evaluate credibility of peer. In construction of trust model, we use time interval to mark time property of experience and recommendation and describe the final trust level of peer using peer credibility, short-term trust and long-term trust as well as trust measurement of peer in a more accurate way by introducing trust deviation value and trust abuse value. Results suggest that, RA Trust has better dynamic adaptive ability and can effectively process strategic behavioral changes of dynamic malicious peer and attack of dishonest feedback on system.*

Keywords: P2P, Trust Management Mode, Malicious Peer, RA Trust

Received: 18 March 2019, Revised 19 June 2019, Accepted 28 June 2019

DOI: 10.6025/jnt/2019/10/3/71-78

1. Introduction

In recent years, peer-to-peer (P2P) technology has been extensively applied in document sharing, distributed computing, electronic market and information management field. But due to open and dynamic nature, benefit and risk of P2P system coexist. It has been found that [1-3], establishing effective credit based trust model can successively avoid risk. Moreover, most credit based trust model are considered being not able to accurately reflect actual trust condition of peer, giving no measure for quantifying and updating reliability of trust information of peer and lacking of effective recognition and punishment for dynamic strategic cheating behavior of peer in the process of trust model construction [4,5].

In terms of how to accurately and reasonably describe trust of peer, many scholars put forward many different forms of trust management model aiming at different application model under P2P environment. Xiong L et al. [6] proposed to prevent peer to abuse network resource and inhibit malicious act of peer applying credit based trust system. This kind of system calculates trust level for peer according to historical trade feedback information of peer. Shi RH et al. [7] put forward a kind of group based trust

management model aiming at multiple malicious acts existing in P2P network. That model calculates overall trust degree of peer by introducing direct trust degree, intragroup credit degree and intergroup credit degree and multiple controlling factors using grouping strategy, which improves reliability of trust mechanism. Li Jialun et al. [8] put forward a fuzzy theory based P2P network trust management model which can be customized based on demand of under. Aiming at the deficiencies of traditional trust model this study proposes a method for constructing credit based trust management model, RA Trust, and fully verifies practicability and reliability of the model with simulation experiment. Eventually, we find, RA Trust can more effectively inhibit dishonest feedback, collusive cheating and complex strategic attack behavior made by malicious peer.

2. Overview of Trust Management Model RA Trust

2.1 Analysis of Characteristics of Trust Model

We propose a credit-based trust management model RA Trust and it has the following characteristics.

First, RA Trust is an anti-attack trust management model based on credit. It not only considers credibility of peer but also clearly distinguishes long-term trust and short-term trust of peer and effectively restrains complex strategic attack.

Secondly, RA Trust model can investigate accuracy of feedback information provided by recommendation peer and thus identify and inhibit dishonest feedback and collusive cheating behavior of malicious peer.

Thirdly, RA Trust model uses time interval to mark time property of experience and recommendation and meanwhile offers punishment mechanism such as trust deviation value and trust abuse value. These measures can more accurately describe various trust measurement of peer, precisely reflect actual trust level of peer, thus to effectively defense attack behaviors of malicious peer and improve dynamic adaptive ability of trust model.

2.2 Definition of Relevant Index of Trust Model

The following first gives out definition for satisfaction evaluation function, direct trust degree, indirect trust degree of peer, then definition of trust deviation value and trust abuse value and finally definition for short-term trust and long-term trust.

Definition 1: Satisfaction evaluation function. Satisfaction evaluation is submitted after peers interact. We define satisfaction of peer i to peer j as Map function $f(i, j)$:

$$f(i,j) = \begin{cases} 1, \textit{totaly satisfactory} \\ 0, \textit{totaly unsatisfactory} \\ e \in (0,1)) \quad \textit{else}. \end{cases} \tag{1}$$

We distinguish different service quality provided by peers with method of probability. I stands for full satisfaction of peer i to peer j, 0 stands for full dissatisfaction of peer i to peer j. Higher value refers to higher satisfaction degree.

Definition 2: Direct trust degree, i.e., normalized local satisfaction degree. To improve accuracy and dynamic adaptive ability of trust evaluation, a period of time is divided into several time intervals which are set as $t_1, t_2, ..., t_n$. Length of time interval can be confirmed according to detailed application scenarios. Within time interval n, we suppose peer i and peer j interact for m times, then direct trust degree $D(i, j)$ can be defined as:

$$D_n(i,j) = \begin{cases} \dfrac{\sum_{k=1}^{m} f(i,j)}{m}, m \neq 0 \\ 0, m = 0 \end{cases} \tag{2}$$

$m = 0$ means that peer i and peer j has not interacted before. We set direct trust degree of peer i to peer j as 0.

Definition: Time fading function. Function of discount rate of trade occurring in k^{th} time interval at the time of trust degree

calculation comparing with trade in the current time interval (n^{th} time interval) is defined as fading function and is expressed as:

$$g(k) = g_k = \rho_{fade}^{n-k},\ \rho_{fade} \in (0, 1) \cap k \in [1, n] \tag{3}$$

Where ρ_{fade} stands for time fading rate.

Definition 4: Indirect trust degree. Indirect trust degree is trust evaluation on object formed based on evaluation information provided by different recommendation peer and reliability of recommender and it is expressed as $R(i,j)$. Indirect trust degree of peer i to peer j in time interval n is defined as:

$$R_n(i,j) = \begin{cases} \dfrac{\sum_{m \in k} D_n(m,j)\, Cr_{im}}{\sum_{m \in k} Cr_{im}} \end{cases} \tag{4}$$

In the formula, K stands for set of recommenders.

Definition 5: Peer trust degree. Peer trust degree is composed of direct trust degree and indirect trust degree. i and j stand for evaluation subject and evaluation object respectively. $PT(i,j)$ stand for trust degree of peer i to peer j. Considering time interval n, its calculation formula is:

$$PT_n(i,j) = \alpha D_n(i,j) + (1-\alpha) + R_n(i,j),\ \alpha \in [0, 1] \tag{5}$$

Where $\alpha\ (0 < \alpha < 1)$ is trust degree regulatory factor. Its value is associated with emphasis of evaluation subject on direct trust and indirect trust. Generally, it can be confirmed according to interaction time of evaluation subject and recommendation peer with evaluation object.

Definition 6: Trust deviation value. To reflect how request deviation degree of peer i in some specific period deviates direct trust degree and indirect degree of target peer j, we introduce trust deviation value of peer P_{ij} whose calculation interval can cover the whole trade period or one time interval therein. Calculation formula for trust deviation value is as follows:

$$p_{ij} = \sqrt{\frac{\sum_{k=1}^{max\ TZ} \{g_k D_k(i,j) - R_k(i,j))^2\}}{\sum_{k=1}^{max\ TZ} g_k}} \tag{6}$$

Where *max TZ* refers to the maximum time interval length of trust deviation value and its upper limit is the whole trade period.

Definition 7: Trust abuse value. It refers to punish fluctuated peer, i.e., distribute appropriate weight to decrease trust degree of peer, thus to inhibit fluctuation. Calculation formula of trust abuse value is:

$$Q_{ij} = \frac{\sum_{k=1}^{max\ TZ} \{g_k \max(0, R_k(i.j) - P_{ij} - D_k(i,j))\}}{\sum_{k=1}^{max\ TZ} g_k} \tag{7}$$

Definition 8: Short-term trust. Short-term trust of peer *i* to peer *j* is set as $ST(i, j)$. $ST_{n+1}(i, j)$ after $(n+1)^{th}$ time interval can be updated through strengthening learning method. Update function is defined as:

$$ST_{n+1}(i,j) = \begin{cases} (1-u)\, ST_n(i,j) + uPT_{n+1}(i,j) \\ PT_{(n+1)}(i,j) - ST_n(i,j) \geq -\in \\ (1-v)\ ST_n(i,j) + vPT_{n+1}(i,j) \\ otherwise \end{cases} \quad (8)$$

Where $PT_{n+1}(i, j)$ stands for trust degree of peer *i* to peer *j* in time interval *n; u* and *v* stand for trust increasing and decreasing learning factor.

Definition 9: Long-term trust. Long-term trust of peer *i* to peer *j* is set as $LT(i, j)$. Calculation formula of long-term trust of peer *i* to peer *j* after $(n+1)^{th}$ time interval is as follows:

$$LT_{n+1}(i,j) = \frac{LT_n(i,j)\, n + PT_{n+1}(i,j)}{n+1} \quad (9)$$

We apply method based on self-adaptive time window of Peer Trust. The minimum value among short-term trust and long-term trust is taken as the final trust evaluation result $T_n(i, j)$.

$$T_n(i,j) = min\,(ST_n(i,j), LT_n(i,j)) \quad (10)$$

3. Distributed Storage of Credit Information

Based on Terrace topology studied previously [9, 10], we design a RA Trust oriented credit information distributed storage mechanism. Terrace topology is a structured topology based on Distributed Hash Table (DHT) technology. On this account, we regard it as the bottom support for upper-layer P2P application network, i.e., trust management infrastructure taking Terrace as bottom layer provides necessary trust security for upper-layer structured or non-structured P2P application system. As Terrace applies single-track Hash method, i.e., peer acquires logic address randomly while entering into topology, logic address of peer can not be determined in advance according to some characteristic of peer (e.g., IP address), which brings certain advantage for safety of anonymous displacement of trust degree.

For *RA* Trust, information relating to credit calculation of peer is stored in corresponding logic peer. We map sign of peer *i* ID_i on logic address of some peer d in Terrace through an even Hash function *HDT*, i.e., $d = HTD\,(ID_i)$. Terrace peer corresponding to d is called as documentary point of peer *i*. Every documentary point d should contain at least one data structure as shown in figure 1.

As shown in figure 1, ID_i is sign of peer *i*; ID_{j1}, ..., ID_{jm} are peer sign which once receive direct service from peer *i*; $SVal_{j1}$,..., $SVal_{jm}$ are satisfaction evaluation of peers to service provider; Cr_{k1}, ..., Cr_{km} are credibility corresponding to recommendation provided by peer with sign ID_{j1}, ..., ID_{jm}; t_{j1}, ..., t_{jm} are time interval corresponding to service delivered (recommended) by peer with sign ID_{j1}, ..., ID_{jm} to peer *i*; k_1, ..., k_m are times of recommendation made by peer with sign ID_{j1}, ..., ID_{jm} to peer *i*.

4. Analysis of System Performance

The simulation experiment is based on document sharing application under P2P network environment. Simulation software is realized based on Java. Experimental assessment standard is successful transaction rate (STR) and unsuccessful transaction rate (UTR). Network environment parameter for simulation is shown in table 1. Suppose all documents in system can be

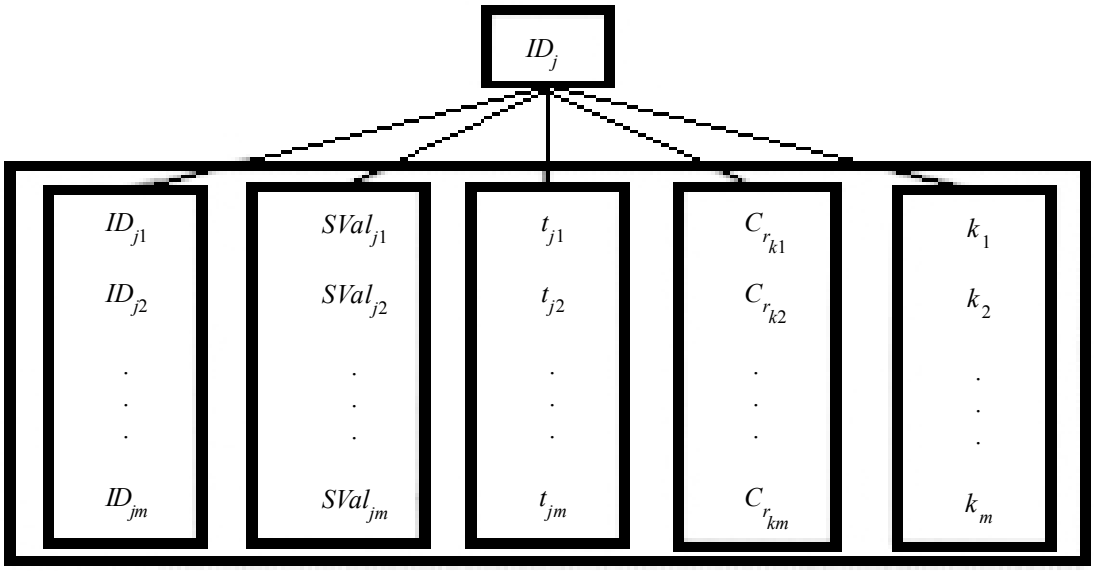

Figure 1. Structure of documentary point of peer *i*

successfully positioned, every document in system is possessed by at least one normal peer and new peer has 10% probability to be selected. This study simulates 100 query cycles and every peer can complete 100 times of transaction in the whole simulation process.

Notations	Parameter Descriptions	Initial Values
N	Total number of peers	1000
ρ_{fade}	Time fading rate	0.8
α	Trust regulatory factor	0.5
σ	Credibility regulatory factor	0.4
γ	Credibility regulatory factor	0.8
μ	Trust deviation value weight	0.5
T	Trust abuse value weight	0.5
β	Punishing density coefficient	0.8
u	Trust increasing factor	0.1
v	Trust decreasing factor	0.2

Table 1. Setting of simulation parameter

4.1 Classification of behaviors of peer

To evaluate effectiveness of RA Trust in inhibiting attack from malicious peer, we construct the following kinds of malicious peer [11, 12]:

1) Simple malicious (SM) peer: It is the most basic malicious peer which provides malicious peer only.

2) Dishonest recommendation (DR) peer: It provides dishonest recommendation only. This kind of peer does not show up group cheating and the malicious behavior is the individual performance of each peer.

3) Collusive Malicious (CM) peer: This kind of malicious peer has group cheating behavior. It provides real service for members and exaggerates trust evaluation of companion in group, but provides false service for peers outside group and defames their trust evaluation.

4.2 SM Simulation and Discussion

SM type simulation refers to all malicious peers in network are SM peers. This experiment aims to test influence of different-scale SM peers on RA Trust. To convenient comparison, we simulate Peer Trust under the same condition. It can be seen from figure 2 that, curves of two kinds of models tend to decline with the increase of SM peers, but the decreasing amplitude of RA Trust is smaller than Peer Trust. When SM peers accounts for 50%, the corresponding STR of the former is 90.5% and the latter is only 87%. The above conclusion proves the effectiveness of RA Trust in inhibiting malicious behavior of SM peer.

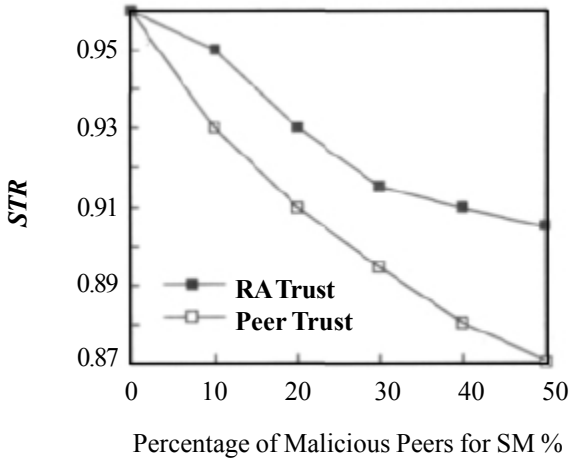

Figure 2. The varying tendency of STR with the percentage of malicious peers for SM

4.3 DR Simulation and Discussion

Malicious behavior of DR peers is confuses. As service provider, it provides real service to make trust illusion. But once it becomes recommender, it provides dishonest recommendation for other peers. Experimental results of different-scale DR peer are shown in figure 3. As peer Trust measures recommendation quality of peer with feed similarity, it can effectively inhibit malicious behavior of DR peer to certain extent. For RA Trust, punishment mechanism such as trust deviation value and trust abuse value can also be used, besides credibility mechanism of peer. These measures can more accurately describe trust measurement of peers and effectively normalize recommendation behavior of peer, thus to inhibit bad influence of dishonest recommendation peer. Moreover, its performance is better than Peer Trust mode. Simulation conclusion of figure 2 powerfully proves this point.

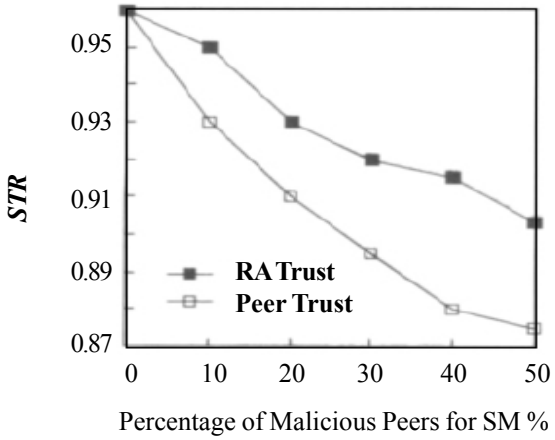

Figure 3. The varying tendency of STR with the percentage of malicious peers for DR

4.4 CM Simulation and Discussion

CM peers know each other. They have stronger collusive cheating ability. It can be seen from figure 4 that trust degree becomes higher with the increase of CM peers. Though Peer Trust integrates feedback quality identification mechanism based on feedback similarity, punishment mechanism is not sufficient, leading to obvious decrease of effective transaction (load). In contrast, RA Trust introduces peer credibility and corresponding punishment mechanism which can exaggerate trust degree of collusive cheating peers, and effectively identify malicious behavior which defame trust degree of peers outside group and exert punishment, thus to ensure inhibition of exaggeration and slander behavior of malicious peer in collusive cheating and maintain STR at a relatively high level.

As shown in figure 4, when CM malicious peer accounts for 50%, STR of RA Trust still can be 89% and STR of Peer Trust is 82%. The above simulation result proves the robustness and effectiveness of RA Trust in coping with attack from malicious peer in collusive cheating.

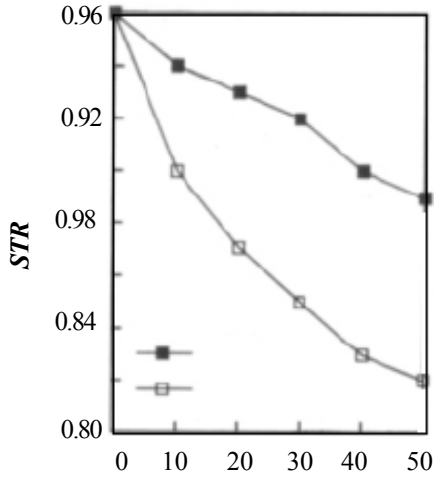

Figure. 4 The varying tendency of STR with the percentage of malicious peers of CM

5. Conclusion

This study put forward a credit based trust management model for P2P network and carries out experiments to simulate actual effect of mode. Analysis and simulation suggest that, the model overcomes partial limitation, is able to effectively cope with attack on system from malicious peer. Therefore, the model can be extensively used in multiple application scenarios and higher engineering feasibility.

However, we have not discussed over distributed storage mechanism and trust solution algorithm of P2P credit information and given no definite solution for how to motivate peer to provide real service and feedback. These are all the focus in future research.

References

[1] Li, J.T., Jing, Y.A., Xiao, Xi.C., WangC X.P., Zhang, G.D. (2007). A trust model based on similarity-weighted recommendation for P2P environments. *Journal of Software*, 18 (l) 158-166.

[2] Tian, C.Q., Zou, S.H., Wang, W.D., et al (2007). Building an attack resistant trust management model for distributed P2P systems. *Journal of Beijing University of Posts and Telecommunications*, 30 (3) 62-65.

[3] Tang, W., Chen, Z. (2003). Research of subjective trust management model based on the fuzzy set theory. *Journal of Software*, 14 (9) 1401-1408.

[4] Xie, Y.Y., Hu, X.G., Liu, J., *et al.* (209). Research overview of trust model in P2P network. *Information Security and Communications Privacy*, 30 (2) 38-42.

[5] Chang, J.S., Wang, H. M., Yin, G. (2006). DyTrust: A time-frame based dynamic trust model for P2P systems. *Chinese Journal of Computers*, 29 (8) 1301-1307.

[6] Xiong, L., Liu, L. (2004). Peer Trust: Supporting reputation-based trust in peer-to-peer communities. *IEEE Trans on Data and Knowledge Engineering: Special Issue on Peer-to-Peer Based Data Management*, 16 (7) 843-857.

[7] Shi, R.H., Xin, J. J. (2010). New P2P trust model based on group. *Application Research of Computers*, 27 (7) 2638-2640.

[8] Li, J.L., Gu, L.Z., Yang, Y.X. (2009). A new trust management model for P2P networks. *Journal of Beijing University of Posts and Telecommunications*, 4, 32 (2) 71-74.

[9] Kaelbling, L.P., Littman, M.L., Moore, A.W. (1996). Reinforcement learning: A survey. *Journal of Artificial Intelligence Research*, 4. 237-285.

[10] Dou, W., Wang, H.M., Jia, Y., *et al.* (2004). A recommendation-based peer-to-peer trust model. *Journal of Software*, 15 (4) 571-583.

[11] Hu, J. L., Wu, Q.Y., Zhou, B., *et al.* (2009). Robust feedback credibility-based distributed P2P trust model. *Journal of Software*, 20 (10) 2886-2887.

[12] Tian, C.Q., Zou, S.H., Tian, H.R., *et al.* (2007). A new trust model based on reputation and risk evaluation for P2P networks. *Journal of Electronics & Information Technology*, 29 (7) 1628-1629.