Risk Evaluation of Information Exchange among Nodes under P2P Net work Environment

Han Yingjun*, Wang Xiaoyang
North China University of Science and Technology
Hebei, 063009
China
yjhanh@163.com

JDIM
Journal of Digital Information Management

ABSTRACT*: In recent years, because of anonymity and dynamics, P2P network have suffered from more and more security problems, which means that traditional trust management cannot be well adapted to P2P network environment, making dynamic trust a new research focus. Based on trust mechanism in P2P environment, this paper analyzes the trust of consumption node to service node, coming upon an advanced trust evaluation model pointing at information exchange among nodes to evaluate credit changes when service provider exchanging information. With risk mechanism, this paper also analyzes risks of information exchange among nodes in P2P network. It is proved that the model mentioned can effectively resist credit speculation and periodic deception.*

Subject Categories and Descriptors
I.6.4 [Model Validation and Analysis]: Credit Evaluation Model; **G.4. [Mathematical Software]**

General Terms : P2P, Credit Evaluation Model

Keywords: P2P, Information exchange among nodes, Trust mechanism, Credit risk

Received: 12 January 2016, Revised 19 February 2016, Accepted 24 February 2016

1. Introduction

P2P network, a newly blooming technology, develops in a high speed, which attracts the public's attention on its security and reliability when it offers services [1]. All bodies in P2P network are equal and independent. While with distributivity, anonymity and dynamics, P2P system faces hidden safety hazards [2]. Nodes differ from each other with unknown qualities; and to be specific, some nodes provide right services honestly, but some offer malicious service, such as spread of virus and Trojan, and false document download [3]. Network-related dishonest is unavoidable, and P2P network is a proper example. Since P2P network cannot promise reliable service, information sharing is accompanied with huge safety problems. For another thing, the lack of central node as the manager makes distributed P2P network cannot stop and "punish" malicious nodes [4]. Besides, traditional safety technologies, like access authorization of service nodes and service authentication consumption nodes, in some sense can prevent information exchange with malicious nodes, but cannot prevent malicious nodes offering unreliable services [5, 6].

Trust management is a effective way to deal with P2P network safety, which faces imperfection of safety information of the system, and admits that decision of system safety needs to depend on attached and reliable safety information provided by a third party [7]. Trust management predicts future actions of users and resources through evaluating users and resources in the system. However, to some extent, immature trust management and access control for current P2P network environment prevent P2P application promotion [8]. According to above statement, based on analysis of trust mechanism in P2P environment, this paper analyzes trust of consumption node to service node, coming upon an advanced trust evaluation model pointing at information exchanges among nodes to evaluate credit changes when service provider exchanging information.

2. P2P Network Trust System Status

2.1 P2P network trust system type

To date, trust system of P2P network is based on information feedback, which can be classified into two types, global trust and local trust. In details, trust degree

of global trust refers to trust degree of all consumption nodes in network to service ability of trust degree owner, and different nodes show different trust degrees to a same node. As for local trust, trust degree means trust degree of some consumption node in network to service ability of trust degree owner, and different nodes may show different trust degree to a same node. At present, most trust models of P2P network are local trust models based on shared information; this model has two ways to obtain shared information: one way is through request to other node information, which has poor extendibility and another way is through P2P storage system of DHT mechanism, such as Chord and P-Grid, which is inapplicable for frequently added nodes and node departure from P2P system.

2.2 P2P trust mechanism type and existing problems

Under P2P environment, four representative trust mechanisms [9] include EigenTrust using trust transfer line and matrix iteration, Credence (planed and applied) based on document voting, LIP accounting trust values by mean retention time of applied documents in P2P document sharing system, and TrusTGuard, a safe trust mechanism frame.

However, though four trust mechanisms mentioned above are able to evaluate and measure safety information under P2P network environment, shortcomings also cannot be ignored. First, trust expression and measurement rationality needs more explanation, since present models, based on certain probability presumption, tend to express and measure trust relations through event probability; second, current models usually combines trust from various approaches by working out simple arithmetic means, which cannot soundly deal with influence on trust evaluation by malicious recommends. Third, trust evaluation lacks flexible mechanism, such as parameter setting, to reflect natures and features of different bodies when processing trust evaluation. Finally, even with derivation and comprehensive formula for trust, how to gain the initial trust value remains unknown.

3. Model Description

Trust, a subject inter-action among bodies, judges by self-knowledge and experience [10]. The greatest challenge for trust evaluation and reliability prediction is trust dynamics whose characteristics decide that trust evolves with time changes and context changes. In this paper, body trust refers to comprehensive evaluation on trust from objects receiving and consuming services.

3.1 Trust evaluation approach

Trust, node measurement, calculates according to exchanging histories which record node information exchanges once a time and contain evaluation values of nodes about service quality of information exchanges and time for information exchanges. When an exchange finishes, consumption nodes fairly evaluate quality of service offered by service nodes based on the service quality. For example, it is assumed that evaluation information is objective comments given by consumption nodes during exchange.

A simple expression as 0 for unsatisfied service or 1 for satisfied service cannot precisely evaluate service quality, thus this paper concludes three kinds of service on the basis of service quality provided by service nodes, which is shown in table 1. Service quality formalization is defined as a assemble, SQ={G,L,W} where each element value can be specifically set according to demands of different resource sharing systems.

Exchange evaluation is presented as “Good”, “Low Grade” and “Worst Behavior”, and values of exchanged information are shown as $\bullet 1, \bullet 2, \bullet 3 \ldots$, such as [0, 50], (50, 150], and (150, 300]. Rule for grading is as follows.

(1) Extra credit rule for “Good”: add 1 for the first “Good”, and add Li for the following “Good”. To be explained, Li means the information occupation in i value segment during history exchanges, and $\mu_i = N(\bullet i)/N(\Sigma \bullet)$

(2) Deduction rule for “Worst Behavior”: service nodes in i credit level will be deducted ki once they receive “Worst Behavior”. In details, ki refers to deduction coefficient; if i<j, ki<kj. Therefore deception cost for service nodes increases to prevent periodic deception.

(3) Taking unavailability of repeated trust between same consumption node and service node into consideration, this model only accounts once the evaluation on various information by same consumption node in time t. within evaluation section T, even the same information between same service nodes is exchanged for several times, only once evaluation is accounted.

Service	Service Comments
Good	With high-qualified service provided by service nodes, exchanges go on smoothly.
Low Grade	Though with right service offered by service nodes, services are delayed and lowered in some extent
Worst Behavior	Service nodes provide wrong information and Behavior even malicious document download

Table 1. Three different services

3.2 Anti- periodic deception analysis

Periodic deception refers to once or more failed exchange when service nodes have successful exchanges for a certain times. This paper selects a set of data with above features to compare and analyze the count method in this paper and traditional count based on credit value accumulation

through simulation experiment. Please refer to figure 1.

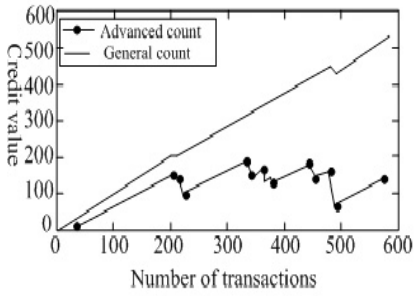

Figure 1. Trust evaluation under periodic deception

4. The PN - SM Service Modeling Experiment

In figure 1, simple credit value accumulation cannot effectively control periodic deception, while advanced count describes periodic deception in details and controls credit value increase, which is benefit for consumption node risk judgment and pushes forward service nodes. Besides, threshold of exchange failure rate decides degrading of credit value.

4.1 Anti- credit speculation analysis

Credit speculation turns into two consequences.

(1) Service nodes in the first place give up a great amount of low-valued information to fast gain higher credit level, and then sell higher-valued information without deception.

(2) Service nodes in the first place give up a great amount of low-valued information to fast gain higher credit level, and then sell higher-valued information to obtain extravagant profits through deception.

Two sets of data matching above two situations are selected to carry on analysis, whose simulation experiment results are respectively shown in figure 2 and figure 3.

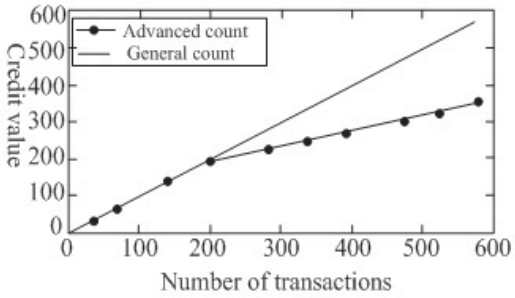

Figure 2. Analysis on credit speculation without deception

From figure 2 pointing at situation (1), service nodes after credit speculation face great potential deception risks even without deception on the condition of traditional and simple credit value accumulation, so those nodes are easy to be confused by credit values. But advanced method lowers credit increase rate during high-valued information exchange,whichis an advantage for risk judgment.Coincide of two curves means that advanced method shows fairness to service nodes exchanging low-valued information.

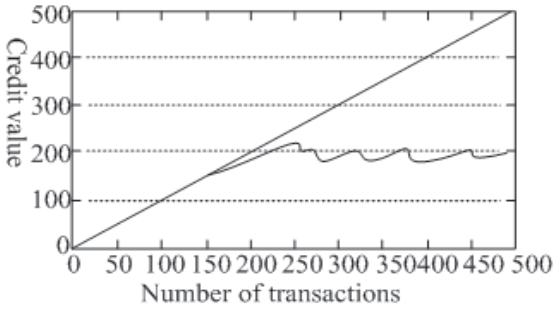

Figure 3. Analysis on credit speculation with deception

As figure 3 for situation (2), it tells that traditional trust evaluation cannot control deception after credit speculation; while advanced curve can clearly detect and crack down on deception after credit speculation.

5. Credit Risk Calculation

5.1 Risk

Generally speaking, risk is objective expectation of probable losses caused by a body who wants to purchase a desired result. Besides, risk possesses two dimensions, loss uncertainty (loss probability) and loss outcome and importance (loss degree), therefore, max risk value of anof information exchange among nodes equals to real value exchanged information. Analysis on informationexchange in P2P network concludes that risks are from the following two aspects.

(1) Information value. Under condition of P2P network environment, real value of information exchanged among nodes decides risk of information exchange.

(2) Service node credit. Even with reasonable credit evaluation system, potential risks also exist because trust degree of consumption nodes to service nodes is presented by credit values which are always accompanied by risks.

5.2 Risk calculation formula

Risk calculation in this paper is based on historical exchange that is divided into three types, namely information exchange without “Worst Behavior” during history exchange, with periodic “Worst Behavior” and with random “Worst Behavior”.

For the first situation, risk calculation should take information value, credit value, credit level, historical mean value and exchange failure threshold into consideration. With longer distance between information value and historical mean value, greater risks will turn up. Within some credit level, greater credit value means less risk, and greater exchange failure threshold is followed by more risks. Calculation formula of credit risk is presented as:

$$R=\begin{cases}k(i), Y_{i-1}<10\\ (k(i)/k_a(i-1))\times(T_j/Y_{i-1})\times\lambda_j, Y_{i-1}\geq 10\end{cases} \quad (1)$$

It can be known that k(i) is the information value of current exchange, ka(i-1) is historical mean value of i-1 preceding exchanges, T_j the upper limit of credit value in j credit level, λ_j the exchange failure threshold in level j, and Y_{i-1} the credit value for i-1 preceding exchanges.

As for calculating credit risks of periodic deception, formula (1) needs modifying. So deception period is introduced. If degrading does not happen, service nodes carry on certain deceptions within a fixed exchange time when reaching some credit level, and the fixed time is called deception period C. on the basis of λ_t ,service nodes do not keep more than $\lambda_t(b\text{-}a)$ deceptions in a deception period. Thus formula (1) can be modified into formula (2).

$$R=(k(i)/k_a(i-1))\times(T_i/Y_{i-1})\times\lambda_i+(i-c)/C \quad (2)$$

In formula (2), c refers to exchange times from last period to last exchange and C is deception period. Obviously, besides general risks due to value and credit, period arrives with risks brought by rules of periodic deception. When period approaches, risks caused by periodic deception occupy more and more percentage with greater exchange risk. How to figure out deception period is presented as follows.

(1) Record the first failed exchange as c(i) where i=1;

(2) Figure out exchange times between following two failed exchanges;

(3) Calculate credit value and level of users after last exchange, select relevant λ_t and figure out failed exchange time threshold w = $\lambda_t \times$ (b-a)

(4) Compare w and c(i): if c(i)>w, it is taken as valid periods that are accumulated to get sum of valid periods (cc) and number of valid periods (cn).

(5) Figure out mean value of valid periods, presenting as C=cc/cn regarded as deception period.

Speaking of the third situation, risks are calculated and evaluated by historical exchange failure rate p according to below formula.

$$R=\begin{cases}k(i), Y_{i-1}<10\\ (k(i)/k_a(i-1))\times(T_j/Y_{i-1})\times p, Y_{i-1}\geq 10\end{cases} \quad (3)$$

The reason for P instead of λ_t is that λ_t is the greatest threshold within which exchanges in this paper are considered as safe and applicable. As for "Good" exchanges, they are expected to come across "Worst Behavior" within error deviation or threshold; but for random deception, λ_t cannot exactly reflect historical exchanges, while p can.

5.3 **Experiment on calculating periodic deception risks**
Matlab is adopted to analyze experiment data, resulting in c(i) = 31, 172, 16, 1, 110, 4, 23, 13, 66, 6, 28, 0, 3, 0 and user credit value Y=148, w=6, cc=57. Speaking from deception period, this set of data faces unstable deceptions. Figure 4 shows the results of historical exchange risk calculation adopting this period.

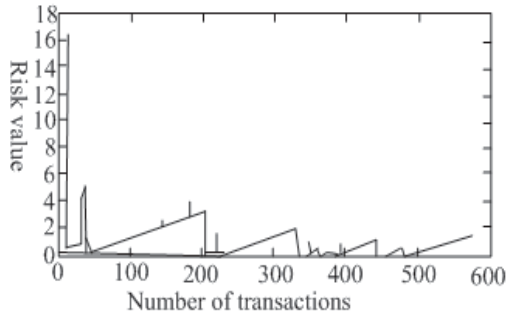

Figure 4. Historical exchange risk analysis

Figure 4 tells that risk value fluctuation basically matches historical exchanges, meaning that it is practicable to use above period to calculate risks.

Another experiment on periodic deception risk calculation is shown below, which has more stable periods. The simulation results in c(i)=102,2,67,2,66,1,76,0; C=77.8, and Y(330)=118 and w=6. Besides, the last failed exchange turns up in the 324th exchange. Figure 5 presents results of the experiment adopting C=77.8 and formula (2).

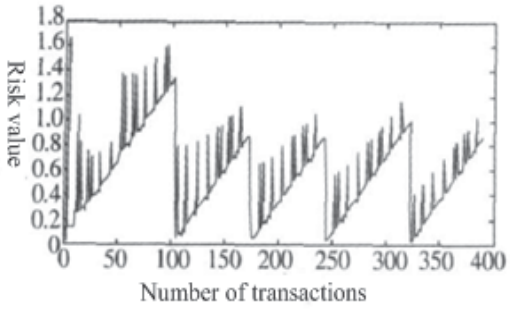

Figure 5. Stable periodic deception risk calculation

5.4 Calculation experiment on credit speculation risks
It can be known from 2.3 that credit speculation leads to two outcomes, and one of them is speculation without deception which can be calculated by formula (1). Primary data from figure 2 are calculated again, leading to results shown in figure 6. In addition, experiment on periodic deception after credit speculation is carried on as that in 2.2.

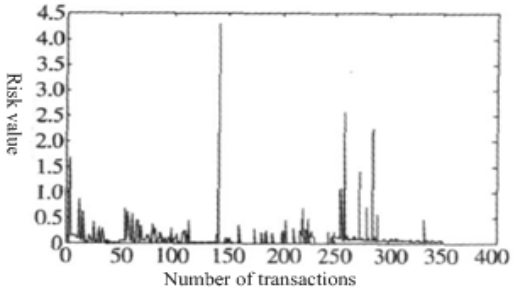

Figure 6. Credit speculation risk calculation

Figure 6 tells that exchanges in the beginning suffer more risks. But with credit speculation, meaning credit value reaching 100, exchange risks mainly come from value. If credit value raises, information with same value faces less risks than early stage.

6. Conclusion

To date, researches on dynamic trust and risk evaluation pointing at information exchange in P2P environment are still in process [11, 12]. So this paper, based on information exchange among nodes, comes upon an advanced trust evaluation model to evaluate changes of credit offered by service provider during information exchange. Experiments prove anti-credit speculation and anti-periodic deception of the model. Analyzing relationship between risk and trust in P2P information exchange environment, this paper proposes risk calculation on the condition of information exchange in P2P environment; and analyzes information exchange risk when credit speculation and periodic deception happen.

Novel credit risk evaluation method put forward in this paper leads to significant experiment effects. For future study, more focus should be put on trust relationship, especially relevant nature of dynamic trust relationship, trust expression and measurement rationality, which is the key factor for and the basis of trust relationship modeling. Meanwhile, performance of the trust evaluation method needs more assess. Due to dynamics and complexity of P2P environment, when calculating deception period, information exchanges in simulation experiment are somehow different from those in real P2P environment. Moreover, this paper does not account sudden failure of information exchange nodes in P2P environment, so this needs to be solved in future researches.

References

[1] Li, X., Ling, L. (2004). Peer trust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans on Knowledge and Data Engineering*, 16 (7) 843-859.

[2] Chang, E.,Thomson, P., Dillon, T., et al (2005). The fuzzy and dynamic nature of trust. *Lecture Notes in Computer Science*, 3592 161-174.

[3] 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.

[4] Su, J.X., Guo, H.Q., Gao, Y. (2008). Recommendation mechanism based on web of trust. *Journal of South China University of Technology (Natural Science Edition)*, 36 (4) 98-103.

[5] Walter, F.E., Battiston, S., Schweitzer, F. (2008). A model of a trust-based recommendation system on a social network. *Journal of Autonomous Agents and Multi-Agent Systems*, 16 (1) 57-74.

[6] Shreedhar, M., Varghese, G. (1996). Efficient fair queuing using deficit round-robin. *IEEE/ACM Transactions on Networking*, 4 (3) 375-385.

[7] Das, A., Islam, M.M. (2012). Secured Trust: a dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*, 9 (2) 261-274.

[8] Liao, X., Tang, H.W. (2003). An evidential reasoning approach for partner selection in dynamic alliance. *Computer Integrated Manufacturing Systems*, 9 (1) 57-62.

[9] Sun, Q., Ye, X.Q., Gu, W.K. (2000). A new combination rules of evidence theory. *Acta Electronica Sinica*, 28 (8) 117-119.

[10] Fang, H.Q., Zeng, Y. (2004). Empirical study and comparative analysis of bank credit risk evaluation method. *Journal of Financial Research*, (01) 62-69.

[11] Liu, W.Y., Yan, G. (2011). Exploration of P2P network credit problem in China. *Northern Economy*, (11) 63-67.

[12] Miao, X.Y. (2012). Network P2P credit risk and prevention. *Gansu Fiance*, (02) 20-23.