2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

An Efficient Trust Mechanism in P2P Network

Qin Zhenquan, Wang Lei, Li Mingchu, Sun Weifeng*
Department of Network Engineering, Dalian University of Technology
Dalian, Liaoning, China
{qzq , lei.wang , mingchul , wfsun}@dlut.edu.cn

***Abstract*—With the proliferation of P2P application, it is critical to consider how these systems can be run in a trust environment. We present a lightweight time-window based effective dynamic trust mechanism(*Tw-Trust*) considering the peer's local and global trustworthiness. Simulation results show that *Tw-Trust* has the advantages in countering strategic altering behavior and dishonest feedbacks of malicious peers.**

Keywords-Trust model; Tw-Trust; time-window based

I. INTRODUCTION

A peer-to-peer(herein known as P2P) is any distributed network architecture composed of peers that make a portion of their resources directly available to other peers, without the need for central coordination instances[1].

Due to its distributed characteristics, P2P systems provides an easy way to aggregate large amount of resources holding by personal computers with a low cost of system maintenance, but it also brings up many scurity problems. Since there is no centralized peer to monitor the peers' action and to pay penalty to their malicious actions, some peers have an incentive to get better services from other peers but to provide poor quality services for their partners. As a result, the whole network's performance will degrade quickly.

So it is critical to consider how these systems can be run in a trust environment. Many works have been done to secure the P2P systems mainly in two aspects, one is to secure the content transmitted by peers through symmetric or asymmetric cryptography, while the other secures the protocols. However, the above traditional techniques cannot prevent from peers providing variable-quality services or peers that are unknown.

Trust and reputation mechanism, which is a branch in P2P network security, can not only automatically balance the workload of file providers (other peers), but also help peers find trustworthy file providers, in other words, it can be used to help peers distinguish good from bad peers. Trust is a peer's belief of its direct peers in capabilities, honesty and reliability based on its own experience, while reputaton is a peer's belief in another peer's capabilities, honesty and reliability based on recommendations received from other peers. Many works have been done to inspire the peers to act fairly and honestly[2-7].

However, there is still a long way to put them into practice due to their complexity in protocol design[3]. In this paper, we aim to shorten the complexity in protocol design but still to maintain the preciseness during judging the peers' action, and then describes a lightweight trust and reputation mechanism that allows peers to find out peers who meet their individual requirements through individual experience and sharing experience with other peers with similar preferences.

The rest of this paper is organized as follows: section Ⅱ discusses the related works on trust and reputation. Section Ⅲ discusses the characteristics of trust and reputation, and then describes the time-window based trust model(*Tw-Trust*) in detail. The simulations and results are shown in section Ⅳ. In the last section, we present conclusions and directions for future work.

II. RELATED WORKS

Trust and reputation mechanisms in P2P system are essential to evaluate the trustworthiness of participating peers and to eliminate the dishonest, malicious, and selfish peer behaviors. A.Samreen et al. [4] surveyed some proposed schemes and discusssed some open issues to cope as the future research, and then provided solution of some problems such as to detect malicious peers, false rating problem and sudden change in the behavior or peers which can be helpful in designing a novel and robust framework for trust and reputation based incentive mechanism.

There are still a lot of researches on trust and reputation mechanism. Here we just mention some works that are most related to our approach.

Y. Wang et al.[5] proposes a Bayesian network-based trust model and a method for building reputation based on recommendations in P2P networks. Bayesian networks provide a flexible method to present differentiated trust and combine different aspects of trust.

R. Zhou et al.[6] developes a P2P reputation system(named PowerTrust) to leverage the power-law feedback characteristics of eBay transactions. PowerTrust significantly improves global reputation accuracy and aggregation speed by using a look-ahead random walk strategy and leveraging the power peers. what's more, PowerTrust is adaptable to dynamics in peer joining and leaving and robust to disturbance by malicious peers.

EigenTrust is proposed by S. Kamvar et al.[7]. It assigns each peer a unique global trust value based on the peer's history of sharing files, and uses a distributed and secure method to compute global trust values based on Power iteration. In this way, untrustworthy peers can be effectively identified and then isolated from the network.

The above works can inspire the peers to act fairly and honestly, but their protocol designs are still too complex to be used in large network system, and they cannot fully prevent from peers providing variable-quality services. In order to solve these problems, we propose a lightweight

*Corresponding author.

978-0-7695-4222-5/10 $26.00 © 2010 IEEE
DOI 10.1109/IIHMSP.2010.185

time-window based trust mechanism*(Tw-Trust*). *Tw-Trust* contributes to the trust and reputation issues by proposing a trust assessment process with the following features:

- Introduce a penalty factor β during computing the local trust to restrict the peer's behavior,once a peer makes a malicious deal, its trust will decrease more quickly than that of increase.
- Introduce a weight factor N during computing the final trust to differentiate the importance of the trust given by high or low trust peer.
- Introduce an aging factor α to prevent from peers providing variable-quality services.

III. TIME-WINDOW BASED TRUST MODEL

A. Role and relationship of peers

Trust and reputation mechanisms have been proposed in many P2P based systems. However, there is no universal agreement on the definition. In this paper, we adopt the following working definitions of the role and relationship of peers.

Based on the role of peers participated in the deal, peers can be divided into three kinds:

- **Good peer**: peer provides honest service with high probability.
- **Malicious peer**: peer provides honest service with low probability.
- **Normal peer**: peer provides honest service between good and malicious peer.

According to the process of peer deal, deals can also be divided into three kinds:

[*Definition 1*]Deal: an interaction between two peers is called a deal. Such as a download action in a file sharing network.

- **Honest deal**: peer A requests a deal from peer B, and peer B provides the service matching the required content.
- **Malicious deal**: the deal is finished but the service provided by peer B dose not matching the required content.
- **Selfish deal**: peer interrupts the deal before the deal is finished.

B. Process of computing the trust value

This section defines the formulas using in computing trust value and updating. Considering that peer A wants to make a deal with peer B, it must computes the trust value of peer B in order to determine to trust peer B or not.

- Compute the Sum of deal between two peers

$$I(A) = \sum_{B \in P, B \neq A} I(A,B) \quad (1)$$

Where I(*A,B*) is the sum of deals between A and B. I(*A*) denotes the sum of deals between A and other peers.

- Compute the Satisfaction

$$Sat(A,B) = I(A,B) - UnSat(A,B) \quad (2)$$

Sat(A,B) and UnSat(A,B) denote the sum of satisfaction or dissatisfaction of B given by peer A from the past deals between A and B, respectively.

- Compute the local trust based on penalty factor

$$C(A,B) = \frac{Max(Sat(A,B) - UnSat(A,B) \times \beta, 0)}{\sum_{B \in (neighbor\ of\ A) \& (B \neq A)} Max(Sat(A,B) - UnSat(A,B), 0)} \quad (3)$$

Where β(β>0) denotes the penalty factor using to enlarge the penalty to malicious behavior. Once a peer makes a malicious deal, its trust will decrease more quickly than that of increase. Therefore, peer receives a high trust only by the accumulation of trust deals. The bigger the factor β is, the severer the penalty is. It will inspire the peers to act honestly. C(A,B) is the local trust of B given by A.

In normal network environment, the denominator can guarantee to be positive, unless a peer is surrounded by malicious peers without a good peer.

- Compute the global trust

$$Cr(A,B) = \sum_{j \in (Deal\ peer\ of\ A)} C(A,j) \times C(j,B) \quad (4)$$

Cr(A,B) is the global trust of B given by A. With the increase of deals between peers, a peer's behavior can be predicted more precisely by other peers through sharing their local trust among them.

- Compute the final trust

$$T(A) = \frac{\sum_{B \in (neighbor\ of\ A) \& (B \neq A)} Sat(A,B) \times [Cr(A,B)]^N}{\sum_{B \in (neighbor\ of\ A) \& (B \neq A)} I(A,B)} \quad (5)$$

Where T(A) is the final trust from the whole system. N denotes the weight factor, the N-th power of global trust Cr(A,B) shows the importance of high trust peer. It differentiates the importance of the trust given by high or low trust peer and also inspires the peers to act honestly.

- Improve the precision of T(A) based on aging factor

$$T_{CURRENT}(A) = (1-\alpha) T_{OLD}(A) + \alpha T_{CURRENT}(A) \quad (6)$$

Where α ($\alpha \in [0,1]$) is the aging factor, it can change the weight of different period and prevents from peers providing variable-quality services.

C. Process of peer deal

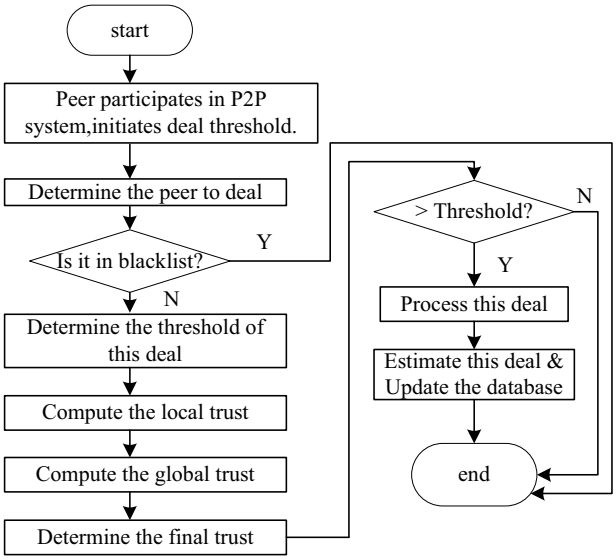

Fig. 1 Trust assessment and peer deal process

Fig.1 shows the trust assessment and peer deal process in a P2P system. A peer first checks its deal peer whether in the black list built by previous deals. If the deal peer in the black list, it will abandon this deal, if not, it will compute the deal peer's trust through the formula introduced in the last section. And then it will determine whether to process this deal by comparing the final trust and the threshold, and finally it will update the database according to the result of this deal so that it can estimate its deal peer for the next time.

IV. SIMULATIONS AND RESULTS

In order to evaluate the proposed trust mechanism, we built a simulation experiment in a P2P network. The system is developed on the Netbeans. For the sake of simplicity, each node in our system plays only one role at a time.

Our experiments involve 1000 peers, the proportion of good peer, normal peer and malicious peer is 0.7, 0.2 and 0.1. Each configuration has 1000 deals among the peers. We run each configuration for 10 times and use means for the evaluation criteria.

A. Determine the Impact Factors(α ,β,N)

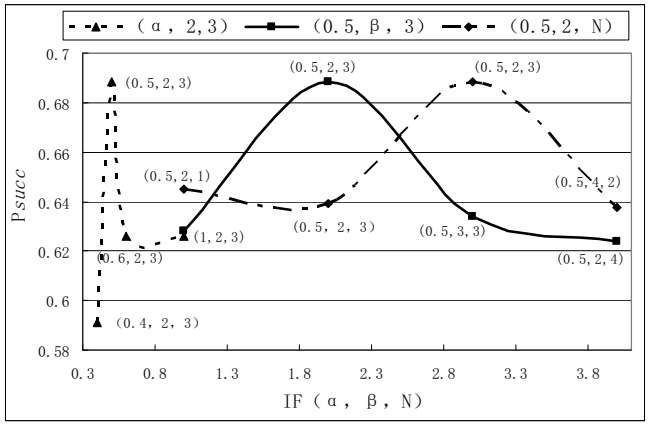

Fig. 2 Determine the Impact Factors (α , β, N)

The choice of impact factors relates to the deal success ratio of the trust mechanism. There are three impact factors involved in our *Tw-Trust* trust mechanism which are aging factor α used to prevent from peers providing variable-quality services, penalty factor β used to control the malicious behavior of peers and weight factor N used to prominent the importance of high trust peer. The last two factors can inspire the peers to act honestly.

In our experiment, the alternative value of aging factor α is 0.4, 0.5, 0.6 and 1. The alternative value of penalty factor β and weight factor N is 1, 2, 3 and 4, respectively. As shown in Fig. 2, the deal success ratio **P*succ*** varies as the combination of (α , β, N) changes. **P*succ*** reaches its maximum when the combination of (α , β, N) is (0.5, 2, 3). This combination will be used in our following experiments.

B. Effectiveness

Effectiveness denotes that the deal success ratio Psucc should be improved with the increase of deals and much higher than that without trust mechanism.

As shown in Fig. 3, we can conclude the follows:

- At the beginning, the deal success ratio **P*succ*** increases both in *Tw-Trust* and *non-Trust* mechanism because the number of malicious participating in deal is small which will not influence the deal success ration very quickly.
- With the increase of deals, **P*succ*** using *Tw-Trust* is much higher than that without trust mechanism because the number of malicious participating in deal increase. *Tw-Trust* can improve the trust of honest peer and decrease the trust of malicious peer as well which make the malicious peer can not participate in deal if its trust is small than threshold and thus improve the deal success ratio.
- With the increase of deals, **P*succ*** using *Tw-Trust* increases smoothly and converges to 0.7 while **P*succ*** without trust mechanism decreases quickly.

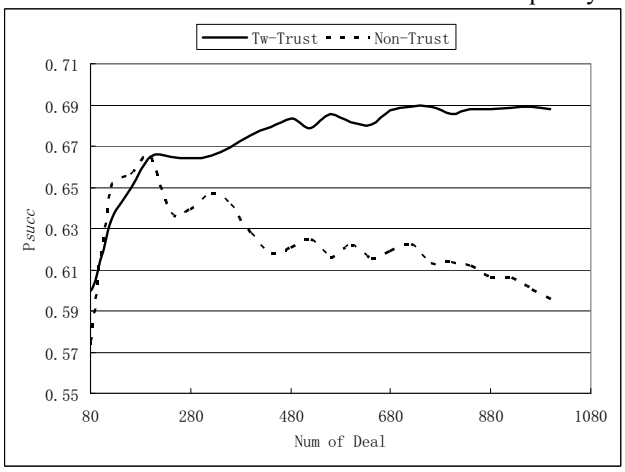

Fig.3 Analysis of effectiveness

C. Feasibility

Feasibility denotes that good peer should achieve a higher trust than malicious peer after a certain number of deals.

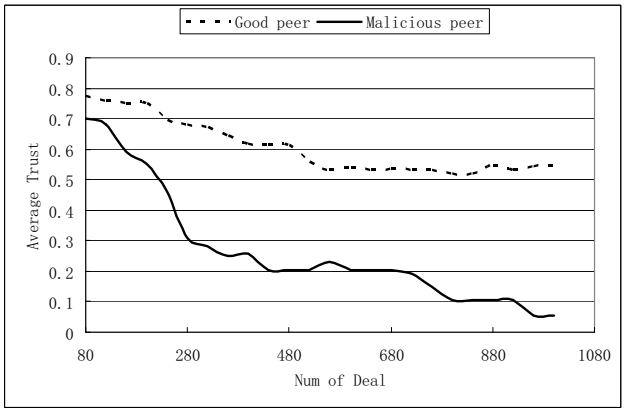

Fig.4 Analysis of feasibility

As shown in Fig. 4, we can conclude the follows:

- With the increase of deals, the average trust of good peer and malicious peer decreases simultaneously. But the trust of good peer decreases smoothly and

converges to 0.53 while the trust of malicious peer decreases quickly and almost reaches 0.

- The different performance of good and malicious peer verifies the effects of penalty factor β and weight factor N which inspire the peers to act honestly. The peer will be punished severely once it makes dishonest behaviors which leads to its failure in the next deal.

D. Robustness to malicious peer

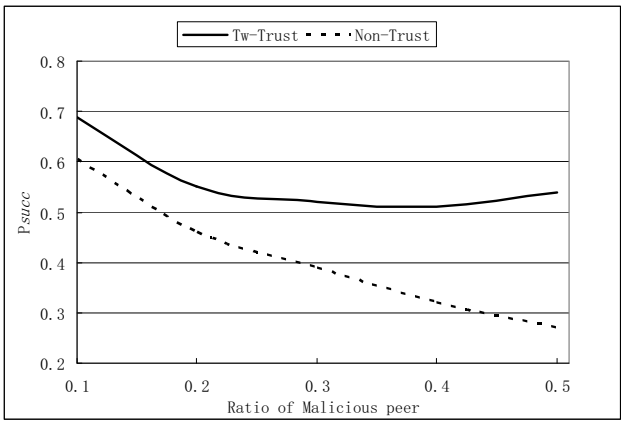

Fig.5 Analysis of robustness to malicious peer

This experiment is used to show the robustness of *Tw-Trust* under different ratio of malicious peers.

In this experiment, the ratio of malicious peers will change from 0.1 to 0.5 and the step is 0.1. Accordingly, the ratio of good peers will decrease at the same proportion.

As shown in Fig. 5, we can conclude the follows:

- With the increase of malicious peers, the deal success ratio **P*succ*** without trust mechanism decreases quickly and reaches 0.4 when the ratio of malicious peer increases to 0.23. While deal success ratio **P*succ*** using *Tw-Trust* decreases smoothly and converges to a stable value.
- The different performance of the two mechanisms verifies the effects of penalty factor β and weight factor N which inspire the peers to act honestly. The peer will be punished severely once it makes dishonest behaviors which leads to its failure in the next deal.

E. Robustness to dynamic network

This experiment is used to show the performance under the situation of dynamic network.

In this experiment, for the sake of simplicity, we only assume that the ratio of malicious peers will change dynamically every 100 deals in the scope of 0.2 and 0.4. Accordingly, the ratio of good peers will change at the opposite proportion.

As shown in Fig. 6, the deal fail ratio **P*fail*** using *Tw-Trust* decreases quickly and reaches a small value, we believe that it is the effects of aging factor α which prevents from peers providing variable-quality services. The peer will be punished severely once it makes dishonest behaviors which leads to its failure in the next deal.

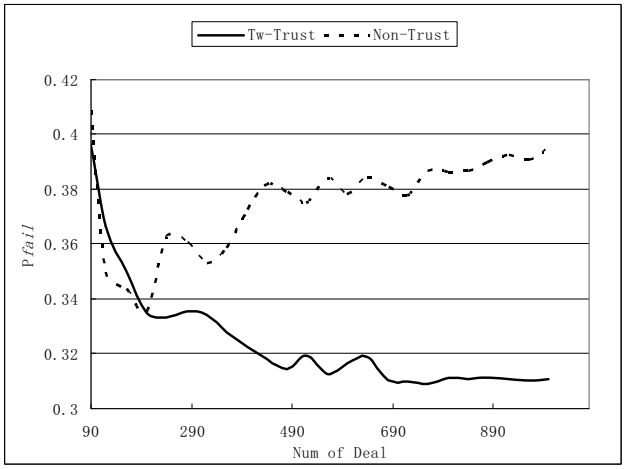

Fig.6 Analysis of robustness to dynamic network

V. CONCLUSIONS

It is very important to enable peers to build trust and reputation among themselves in P2P system, where trust and reputation mechanism can prevent peers from malicious behaviors and then build an effective network environment. In this paper, we propose a lightweight time-window based effective dynamic trust mechanism(*Tw-Trust*). Simulation results show its power in different aspects. However, there are still many works to do, such as how to ensure the correctness from other peers, how to let this mechanism work in practical environment, etc.

REFERENCES

[1] Rüdiger Schollmeier. "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications". In Proceedingsof the IEEE 2001 International Conference on Peer-to-Peer Computing (P2P2001), Linkping,Sweden, Aug. 2001,pp.101–102.

[2] P. Rodriguez, S. Tan, and C. Gkantsidis. "On the feasibility of commercial, legal p2p content distribution", ACM SIGCOMM Computer Communication Review, Vol. 36, No. 1, Jan. 2006, pp. 75–78.

[3] M. A. M. Gupta and M. Ahamad, "Trade-offs between reliability and overheads in peer-to-peer reputation tracking," Computer Networks,Vol. 50, No. 4, 2006, pp. 501–522.

[4] A.Samreen,S.Hussain. "Trust management and incentive mechanism for P2P networks: Survey to cope challenges", Multitopic Conference(INMIC 2008), Karachi, Dec. 2008, pp.301-306.

[5] Y. Wang, J. Vassileva. "Trust and Reputation Model in Peer-to-Peer Networks". Proc. of The Third IEEE International Conference on Peer-to-Peer Computing,Sep.2003,Sweden. pp.150-155.

[6] R. Zhou, Kai Hwang. "PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing," IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 4, pp. 460-473, Apr. 2007, doi:10.1109/TPDS.2007.1015

[7] S. Kamvar, M. Schlosser, and H. Garcia-Molina. "The eigentrust algorithm for reputation management in p2p networks," The 12th International World Wide Web Conference. Budapest, Hungary. May 2003. pp.640-651.