2009 International Conference on Communication Software and Networks

Trust Decision Making in Structured P2P Network

CAI Biao[1], LI Zhishu[1], CHENG Yang[1], FU Die[2], CHENG Liangying[1]
1 School of Computer, Sichuan University, Chengdu, Sichuan, P.R.China, 610065
2 Network Management Center, Sichuan University of Art and Science, Dazhou, Sichuan, P.R.China, 635000
nccb130@yahoo.com.cn

***Abstract*—P2P trust systems are essential to against the selfish, dishonest, and malicious peer behaviors. But most previous trust strategies of P2P network have many defaults such as low accuracy, high traffic etc in trust decision. Then we proposed a structured trust P2P network based on DHT (discrete hash table), in which includes peer management and peer locations based on the DHT circle, another, a top-n trust accumulating strategy based on developed and discrete particle swarm optimization (PSO) is proposed too. And effectiveness and practicality of the proposed trust decision have been showed in simulation experiments at the end.**

Keywords-P2P Network; structured topology; peer location; trust accumulating

I. INTRODUCTION *(HEADING 1)*

Peer-to-Peer network is a fully distributed computing application in which peers can directly communicate with others to exchange their information such as Gunnalt and Napstey. In a P2P community, relationship between peers are often established dynamically and they are unknown to each other, so peers themselves have to manage the risk involved with transactions without prior experience and knowledge about cooperators' reliability. One way to address this uncertainty problem is to make use of trust strategies to make peers can only interact with others based on their trust belief. Most existing trust models of e-commercial require central entities for storing and distributing trust information of peers. With characteristics of P2P network such as *self-organizing*, *anonymity*, *dynamic*, *robustness*, and *scalability* etc, how to implement trust strategies in P2P communities is very important.

Because trust model for electronic markets cannot be directly transferred to a self-organizing P2P network, so trust mechanisms that peers can play the same roles and there are no entities that can be taken as a reliable trusted center for P2P network will be essential. PeerTrust [1] model define a general trust metric based on three introduced basic trust parameters and two adaptive factors in computing trustworthiness of peers, which are feedback of a peers receives from others, the total transaction numbers a peer performed, the credibility of peers from feedback received, transaction context factor, and the network environment factor. EigenTrust [2] presents a distributed and secure method to compute global trust value, in which peers choose other peers from whom to interact with based on this global trust value and the trust model performed significantly to decrease the number of inauthentic files in P2P network. PowerTrust [3] aggregate global reputation with significantly and accuracy speed by using a look-ahead random walk strategy, and dynamically selects top-n power peers that are most reputable by using a distributed ranking mechanism. This trust model is robust to disturbance by malicious peers and adaptable to dynamics in peer joining and leaving.

Above mention trust strategies of P2P network have many defaults such as low accuracy, high traffic etc in trust decision. Then we proposed a structured trust P2P network based on DHT [4] (discrete hash table), in which includes peer management, peer locations and a trust accumulating. Simulation shows that the proposed trust decision performed well.

The rest of this paper is organized as follows: Section 2 and Section 3 is the peer management and peer location based on DHT respectively. In section 4 is the top-n trust accumulating strategy based on the developed PSO [5,6]. Section 5 is simulation performance results and the conclusion and future works is organized in section 6.

II. PEERS MANAGEMENT

A. Peer Organizing

In this paper, we organize peers on DHT as Chord; the discrete hash function assigns every peer an *m*-bit identifier using a general hash function such as SHA-1 [7]. A Chord [4] like peer's identifier is chosen by the peer's unique username (such as IP address). We use the term "key" to refer the hashed value of the unique identifier under the hash function. The identifier length *m* must be large enough to make the probability of two usernames hashing to the same key is negligible. Alls peer is organized in a circle according to their keys with increasing order. Peer organizing in such circle is showed in figure 1(a). And the main challenges in implementing trust operation and management in such P2P network are to overcome the three barricades:

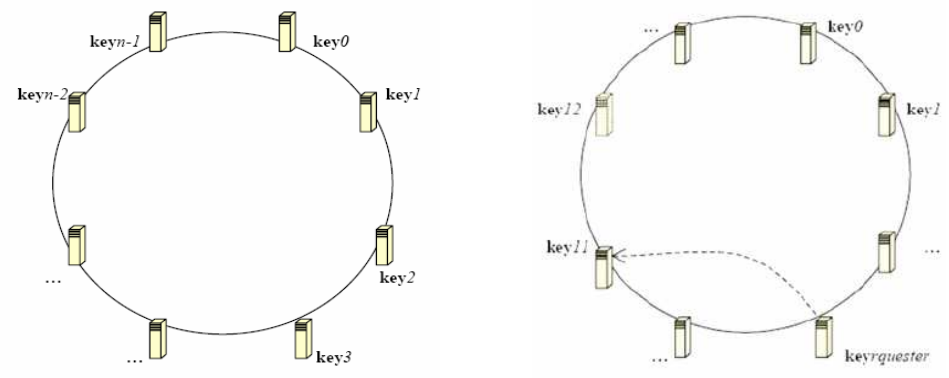
where to store trust information of trustee,
how to implement trust routing decision
and how to accumulate trust score

B. Trust Managemen

To maintain trust management of peers on DHT in the P2P network, each peer will be assigned at least one trust manager to manage identifier and trust information of its own. The trust manager of peer *i* is assigned as follows: if

978-0-7695-3522-7/09 $25.00 © 2009 IEEE
DOI 10.1109/ICCSN.2009.52

peer j is a certain successor of h_i, where h_i is the hash value of its unique identifier of peer i hashed by the predefined hash function, then allocate the peer j as the trust manager to peer i. If other peers want to contact with a trustable peer i, they may issue a lookup on the manager to abstain the identifier information of peer i to get relate to the trustable peer. The key of the manager $h_{m(i)}$ is decided on a predefined constant c and calculated as $h_{m(i)}=(h_i+h_c)\bmod 2^n$, where h_c and $h_{m(i)}$ be hash values of constant c and identifier of the manager hashed by the predefined hash function respectively, and $h_{m(i)}=h_j$. If $m(i)$ isn't in this circle, then $m(i)=m(m(i))$. Zhou and hwang [3] point out that multiple hash functions can be used to against malicious manager reports incorrect trust scores, here, we can adopt different constants instead of different hash functions to implement this purpose.



(a) Peer organization (b) peer 12 is failure

Figure 1: Peers on circle

III. PEER LOCATIONS

As the same as Chord, a small amount of routing information suffices to implement peer locating in a distributed P2P environment. When lookup the routing information of a trustable peer, each peer need only be aware of its successor peer in the routing table to get the IP address of the trustable peer which is stored in management table of its manager. For example, let the bit length in the hashed key of identifier m=4, key of requester equal to 3, key of trustable peer equal to 12, key of the manager is 15. The requester issues a lookup on the manager to query the IP address of the trustable peer, so requester will calculate the intervals of its routing peers to make sure that, which interval will the manager of the trustable peer belongs to, for the case of $(3+2^3)\bmod 2^4-1=11$ and $(3+2^4)\bmod 2^4-1=19$. So the requester locate the lookup at peer whose key equal to 11, recursively, it can access the manager peer whose key is 12, and get the IP address of the trustable peer. After successfully abstain the IP address of the trustable peer, the requester can relate to the trustable peer immediately.

Because the dynamics of that peers can join or leave the network at anytime, an expected peer is not exist in may frequently happen. When the expected peer i cannot be find in this circle, then its first predecessor peer h_i-1 will take the role of this expected peer. For example, if key of the expected peer is 12 doesn't existing, and it is the first successor of peer with key equal to 11 is existing in this circle, because $(11+2^0)\bmod 2^m=12$, then let $h_i=11$ take the role of peer 12, such as in figure 1(b).

IV. TRUST ACCUMULATING

Because peers in P2P network are dynamic and unknown to each other, so trust accumulating of a new peer is a NP complex problem, we employ a developed particle swarm optimization to implement a top-n trust accumulating in P2P network.

A. History Particle Swarm Optimization

Particle swarm optimization (PSO) is an evolutionary computation technology and was introduced by Eberhart and Kennedy [5] in 1995. Standard particle swarm optimization (SPSO) requires every particle in the swarm has two "best-positions" which are personal best position in history (pBest, p_0) and population best position be discovered so far (gBest, p_g). And particles will update their positions and velocity according to the two best positions to find the global optima iteratively.

$$v_j^{i+1}=v_j^i+c_1r_1(p_0-x_j^i)+c_2r_2(p_g-x_j^i) \quad (1)$$

$$x_j^{x+1}=x_j^i+v_j^{i+1} \quad (2)$$

where c_1 and c_2 are constants, j is the j^{th} dimension, x^i is position of i^{th} iteration, v^i is velocity of i^{th} iteration, r_1, $r_2\backsim U(0,1)$, and a parameter v_{Max} is used to constrain the moving scope of particles.

Based on SPSO, we developed a fast convergence particle swarm optimization (fPSO) strategy [6] whose particles update their positions only according to p_0 and p_g instead of p_0, p_g and v_j^i in SPSO as follows:

$$x_j^{i+1}=c_1r_1(p_0-x_j^i)+c_2r_2(p_g-x_j^i) \quad (3)$$

In a P2P network, when a new population best position is find, this peer do not know where other routing message will be, so other message are not know there is new gBest. Let peers that routing messages arrived keep in attach each other can resolve this problem, but it obviously is illegitimate that it will produce much unnecessary traffic by these communications. To overcome these challenges, we define a new history PSO (hPSO) algorithm based on fPSO as follows:

$$x_j^{i+1} = c_1 r_1 (p_1 - x_j^i) + c_2 r_2 (p_2 - x_j^i) + \cdots + c_k r_k (p_k - x_j^i) \quad (4)$$

where p_l is the l^{th} best position of history of this particle in decreasing order.

B. Discrete hPSO for Trust Accumulating

However, this method can only be used to solve continuous problem, while peers in network are discrete contribution, so this equation cannot be directly transferred to P2P network. The operational components in (4) can discrete as follows:

Positions: peers in P2P network x_j^i.

Subtractive operation between two positions: this operation is peers routing in P2P network, we mark peer A routing on peer B as $\Re = A \Theta B$.

Multiplicative operation between real number and peer routing: this operation is a routing decision operation when make a routing selection, we mark a real number r multiplies a routing decision $\Re(j)$ as $r \otimes \Re(j)$, where r is decided by a random number as follows:

$$\begin{cases} r = 1 & \text{int}((n+1)random) = j \\ r = 0 & \text{int}((n+1)random) \neq j \end{cases} \quad (5)$$

where n is the number of trustable peers of top-n.

The routing decision of trust accumulating algorithm for a new peer in the network can be present as follows:

$$x_j^{i+1} = \sum_{l=1}^{k} r \otimes \Re(l) = \sum_{l=1}^{k} r \otimes (x_j^i \Theta p^l) \quad (6)$$

In this top-n trust accumulating, the new peer will send trust query message to peers in its routing table, and every routing peer will make decision peer will be the next hop iteratively, until yhe top-n trustable peers have been found or remain hops *rh*=0. Then, the top-n trust accumulating algorithm for a new peer can be present as algorithm 2:

Algorithm 2: top-n trusts accumulating
Begin
Initial the trust vector of trustor
for *every routing neighbor*
do
send query message to routing neighbors
while (*TTL>0* or *condition isn't satisfied*)
routing decision based on routing decision as (6)
else
return IP address of the trustee to trustor
endwhile
enddo
End

V. Simulation Experiment

A. Simulation Setting

a) Experiments in this section are simulated in Matlab 7.0. Trust score of peers is produced randomly. Network topology is constructed as follows: another connection matrix C=c(i,j) *is constructed randomly, if* c(i,j)*>0.9, then there is a connection between peer* i *and peer* j. *Because hash function can make peers in the circle balance arrangement, so we suppose key of peers are uniformly distributed with increasing order in this circle.*

B. Effectiveness of Trust Routing Decision

We evaluate the effectiveness of this trust routing decision on trust location and trust accumulating, and suppose there isn't malicious peers in the experiment. We compute the average path hops (APH) of 20 runs. The lower APH indicates the higher effectiveness performed. The APH is defined the number of peers between the trustor and trustee in the network.

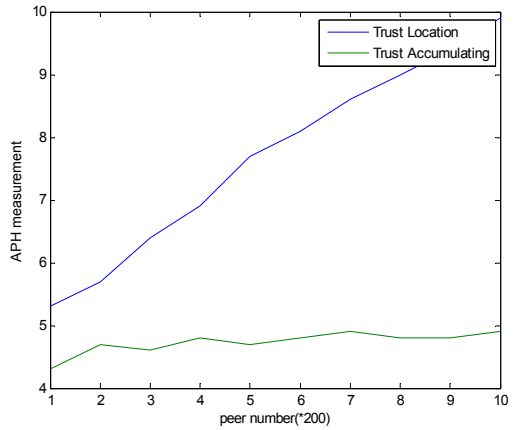
We plot the APH against different number of peers in a stationary network in Fig. 2(a). The default trusts score is 0.5. Figure 2(a) shows the APH on every number of peers in trust location is equal to value that in theorem 1 approximately. And with about a fix number of hops 5, the trustable peers can be found to the trustor. Figure 2 (b), we set a dynamic network with 10% peers join in or leave out. A random number implements the dynamics of 10%. When a routing message arrived on a certain peer, this peer will produce a random number *r*, if *r*>0.9, it will implement requirement of this message, otherwise, keep on muting. The result shows that in trust location, the greater the number is, the more APH will be. But in trust accumulating, there is a little variation between the two networks.

C. Traffic Load

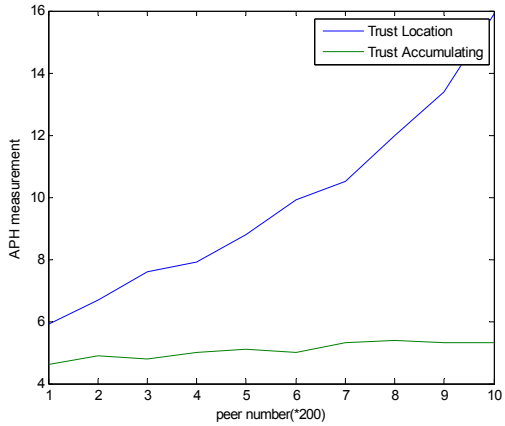
We evaluate the traffic load of this trust routing decision on trust location and trust accumulating, and suppose there isn't malicious peers and 20% malicious peers in the experiment respectively. We compute the average number of message (ANM) of 10 runs. The lower ANM indicate the smaller waste of resource in the procedure. The ANM is defined as the messages number of transactions fly in the network. Peers with trust score no more than 0.2 will be isolated from the network.

We plot the ANM against different number of peers in a stationary network in this simulation. The default trusts score is 0.5. Figure 3(a) shows the ANM of a trust decision in an honest network, figure 3(b) shows the ANM of a trust decision in a dishonest network with 20%malicious peers. Malicious peers of 20% is present by it trust score. If trust score *ts*>0.2, this peer is taken as an honest peer, otherwise, take it as a dishonest peer. The result shows that the ANM of trust accumulating in a dishonest network with 20% malicious peers is about 2 times than that of in an honest network or dishonest network. While either in a dishonest network or honest network, the ANM of Gunnalt like trust

management is about hundreds or thousands times to that of trust accumulating and trust location this paper.

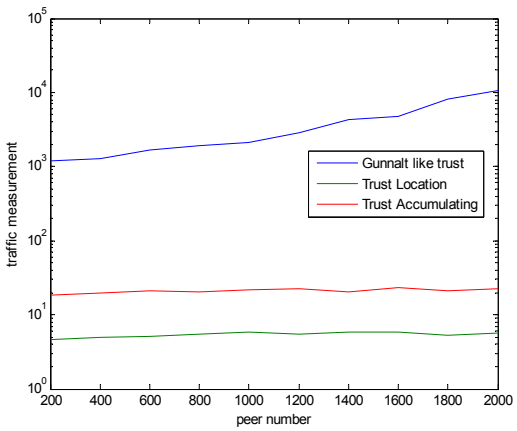


(a) Stationary network

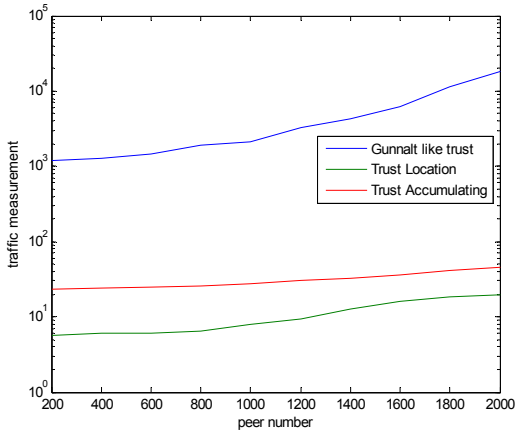


(b) With 10% dynamic peers network

Figure 2: Effectiveness on APH

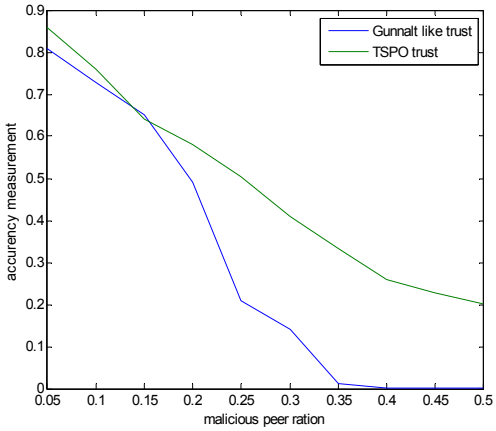


(a) Without malicious peers

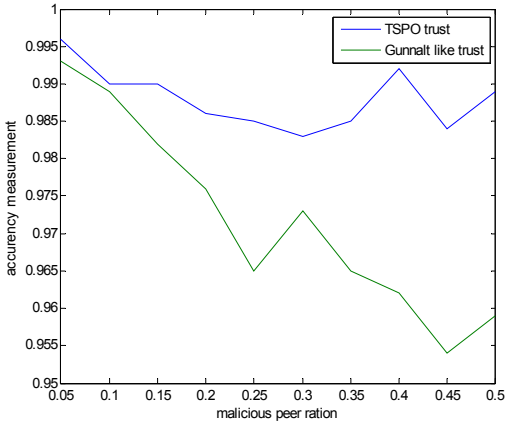


(b) With 20% malicious peers

Figure 3: Traffic performance on ANM



(a) Do not isolate malicious peers



(b) Isolate malicious peers

Figure 4: Schedule accuracy

D. Schedule Accuracy

We evaluate the schedule accuracy of this trust routing decision between Gunnalt routing like and trust routing mechanism with structured peer organization proposed this paper (TSPO). Suppose there are 20% malicious peers in the experiment. We evaluate the average value of schedule accuracy (ASA) of 10 runs. Malicious peers of 20% is present by it trust score as the same as that of section 5.3.

We plot the schedule accuracy against different ration of peers in a stationary network in this simulation. Figure 4(a) shows the accuracy of a trust decision in the network in which malicious peers are not be isolated, figure 4(b) shows network in which malicious peers are isolated. The result shows that without isolation of malicious peers, Gunnalt like trust performed very poor than that of TSPO proposed in this paper. If isolate all malicious peers of the network, both the two trust decisions can perform satisfactory result with schedule accuracy more than 90%.

VI. CONCLUSIONS

In this paper, we proposed a structured trust P2P network based on DHT (discrete hash table). Peer management includes peers organization, trust storing and data-tables. Based on Peer management, the peer locations based on the DHT circle and top-n trust accumulating strategy based on developed particle swarm optimization (PSO) is proposed too. The effectiveness and practicality of the proposed trust decision have been showed in simulation experiments end. The next work of this paper should to construct a rational trust computation model [8,9] and transfer this trust strategy to a network simulator or real network environment future to test and improve the trust decision.

REFERENCES

[1] [1] L. XIONG and L. LIU, "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," *IEEE Trans. Knowledge and Data Eng*, vol. 16, no. 7, 2004.

[2] [2] Sepandar D. Kamvar, Mario T. Schlosser, Hector Garcia Molina. The EigenTrust Algorithm for Reputation Management in P2P Networks. *In ACM proceedings of WWW2003*, *May* 2003.

[3] [3] Runfang Zhou, Kai Hwang. PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing, *IEEE Transactions on Parallel and Distributed System*, Vol.18, 4.2007

[4] [4] Ion Stoica_, Robert Morris, David Karger, et al. Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications, *In ACM proceedings of SIGCOMM'01*

[5] [5] Kennedy J, Eberhart R.C. Particle Swarm Optimization. In *Proceedings of the IEEE Conference on Neural Networks*, IV., 1995,1942−1948

[6] [6] CAI Biao, LI Zhishu, FU Die et al. Mutated Fast Convergence Particle Swarm Optimization and Convergence Analysis. Accepted by *ICINIS'08*, will publish in Nov 2008

[7] [7] FIPS 180-1. Secure Hash Standard. U.S. Department of Commerce/NIST, National Technical Information Service, Springfield, VA, Apr. 1995

[8] [8] CAI Biao, Li Zhishu, Lin Xun. PRN: a Novel Trust Model. *In proceedings of International Symposium on Data, Privacy, and e-commercial'07* Dec.2007 361-366

[9] [9] Ali Aydin Selpk, Ersin Uzun, Mark Regat Pariente. A Reputation-Based Trust Management System for P2P Networks *In Proceedings of International Symposium on Cluster Computing and the Grid' 04*

[10] [10] Antony Rowstron and Peter Druschel. Pastry: Scalable, decentralized object location and routing for large-scale peer-to-peer systems. In proceedings of IFIP/ACM International Conference on Distributed Systems Platforms (Middleware 2001)

[11] [11] Yunhao Liu, Li Xiao, and Lionel M. Ni. Building a Scalable Bipartite P2P Overlay Network. *IEEE Transactions on Parallel and distributed systems*, Vol. 18, NO. 9, Sep 2007