

A Scheme of Trust Management System for P2P Network

BinbinLiang^{1,2}, LizeGu^{1,2}, Bin Sun^{1,2}, Yixian Yang^{1,2}

¹Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications

²Key Laboratory of network and information attack & defence technology of MOE, Beijing University of Posts and Telecommunications

liangbinbin@gmail.com

Abstract—P2P network has become an important branch of Internet recently, with the significant advantages of full resource utilization, dynamics, openness and high scalable, which helps it achieve wide applications. But security and trust have also become urgent problems for a P2P network due to its openness and anonymousness. Most of the current schemes rely on some trust models, but the research in systematic managing scheme is scarce. Consequently, we propose a scheme of constructing trust management systems in a P2P network here.

Keywords—Trust management, P2P network, trust certificate, trust policy, trust negotiation, trust agent.

I. INTRODUCTION

P2P is a new technology of network computing, which aims for combining these different computer together on the network, and making full use of the idle resources anywhere on the Internet and the web site. In this network participants are not only resource suppliers (Server) but also resource recipients (Client).

P2P distributed network can eliminate single-point error and isolated point of info caused by centralized system, improve scalability and reduce the bottleneck. However, P2P clients are faced with the issue of client security and trust, while centralized systems have advantages in security. The core of the centralized system includes the control of resources, users and network and safety precautions. The P2P distributed system security is very difficult to achieve. In order to make the system work effectively, security must be embedded into the P2P system, rather than be added to the system as an additional part after the system design was completed. In the past, a part of the attractiveness of P2P systems comes from the freedom and anonymous login. But it is not feasible for business applications which deal with private information or economic exchanges. No matter what the underlying structure is, these applications require the traditional security guarantees.

In view of their respective advantages of the P2P systems and centralized systems, we have adopted a compromise

consideration and proposed a scheme of trust management system for P2P Network based on hybrid structure. The legacy trust framework based on the status or access control can't satisfy the requirement of the security in P2P environment. Blaze and his fellows raised the conception of trust management [1], and studied out the trust management system such as PolicyMaker and KeyNote based on this conception. In this situation, we proposed a new scheme of trust management framework. This systematic scheme likes a reputation system [2]. Reputation is one specific way of establishing trust; it is a risk management technique. Reputation systems provide a way for peers to be able to trust other peers. The main challenge in reputation systems are handling of trust measures, handling dishonest feedbacks, handling malicious attacks on peers and taking care of free riders, those who do not contribute much to the network. Aimed at these problems, the scheme of trust management system is proposed to resolve them.

The network system will be divided into a number of independent Autonomous Systems (AS). A super-node, trust agent (TA), which provides trust service will be assigned in each AS. As the super-node only provides lightweight trust service, it is not a heavyweight server in traditional centralized system. The interaction between nodes is peer-to-peer in each AS. And in order to obtain trusted services and better quality of service, nodes interact with each other with the help of trust services supplied by TA.

II. P2P MODEL STRUCTURE and ITS TRUST MANAGEMENT

According to its network topology, P2P network model can be divided into four kinds: Pure P2P, Central Index P2P, hybrid P2P and Structured P2P. Topology refers to the physical or logical relationship between each unit in the distributed system.

Pure P2P: In a pure P2P model, we can only seek a credible third party by quantitating the credibility of the nodes. The typical example of pure p2p is Gnutella [3]. In this model, there is absolutely no central node, and the relationship between nodes is true peer-to-peer. Each peer has the exactly same functions and responsibilities in two aspects of content sharing and search. All of the peers not only initiate searching but also process the other's searching. The advantage of pure P2P is its

greatest fault tolerance. Gnutella, typical example of such models, uses flooding-based query which is easy to have a great impact in the network traffic and lack of quick search and scalability.

Central Index P2P: In this model, we can attribute a central server to be credible third party. The typical example of pure p2p is Napster [4]. The central server exists in the network and it is high-performance. The server saves shared resources directory of the entire computer in the network. When one peer needs to search a file, it sends a request message to the index server, and the index server responds it after it finds the resource index. The advantage of this model is its high efficiency and it alleviates the peers' load. But it also has disadvantages, and the most important is Single point of failure.

Hybrid P2P model: In hybrid model, the super-peer can play the role of credible third party. It has possessed of advantages of the above two model. The peers which have higher performance are selected as super-peer. And these super-peers constitute a forward layer with higher performance. Its main advantage is well supported to network-scalable. Compare to Pure P2P, it can decrease the amount of the transmitted query-messages. The query-messages merely transmit between super-peers. Compare to Central Index P2P, it reduces the impact to the whole P2P network caused by Single point failure.

Structured P2P: This model uses DHT (Distributed Hash Table) protocol to route, e.g. CAN [5], Chord [6] and Pastry [7]. In this model, we can set native trust-database and make use of it for DHT routing.

III. COMPUTE and UPDATE TRUST VALUE

A. Generate Trust value

This Trust Management System includes two type of trust value: static and dynamic. Static trust value is measured with the static info of the peer and trust policy. And the dynamic trust value is computed based on the dynamic info of transaction result between peers and the trust model we designed. Moreover, dynamic trust value depends on static trust value to some degree.

The computation of static trust value happens during the register of peers. And the static trust value is created according to the register info submitted by peers and system's trust policy. This task is completed by Static Trust Value Creating Function.

There are two ways of generating dynamic trust value.

1) Real time: when operation was completed, and the initiator and participator in the operation reported evaluation result info of the operation performing to the Trust Agent which updated the trust value of relevant peers according to the result info.

2) Timing: Trust agent read data from operation result database table, and sum up the total event and these performing results occurred during some time, and then update the trust value of relevant peers according to these info.

B. Update trust value

We can take two ways to update trust values: time drive and event drive. Event drive update executes when the next time trust evaluation occurs. While Time drive update performs after an interval of time.

If taking the way of event drive to update trust values, we can reflect the trust relationship between peers exactly and in time. But it will cause a great lot of system spending if the event occurs in high frequency. While Time drive mode can make full use of the adjustable time interval. This mode will bring delay to some degree, but it is lighter system load.

If we take mixed time and event update policy, the contradiction above will be resolved effectively. The work processes of this mixed update method are below: when trust estimate occurs each time, the Trust agent evaluates the trust estimate. If it impacts the trust relationship of relevant peers more, we will take event drive update method. Otherwise, we will choose time drive update method. The mixed type holds the advantages of both event and time drive update, and it can reflect the trust relationship between peers exactly and in time without increasing system load.

IV. TRUST MANAGEMENT SCHEME

In order to achieve trust between peers in P2P network, it is necessary to import Trust Agent Super Peer which focuses on providing trust management services. This model takes hybrid structure and divides P2P network into a number of independent Autonomous Systems (AS) according to the organization and physical location of the peer. Every AS includes a Trust Agent Super Peer and some common peers. The Trust Agent connects each other between each AS. In this way, the system problems that include trust problem in each AS, scalable capability, autonym capability and isomorous capability, will be well and easy resolved. Figure 1 shows the system topology.

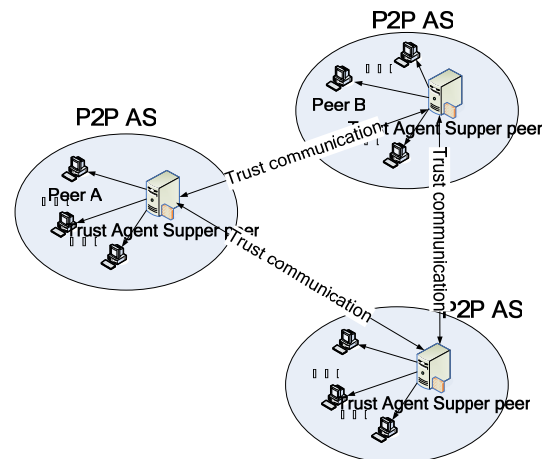


Figure 1. Hybrid P2P Trust Management Scheme

In our model, we assign Trust Agent in each AS. These supper nodes themselves don't participate in the resources sharing, and they only provide function of trust management for generic peers, hence, it is hard to attack the network.

While a peer joins trust system, it will find the nearest Trust Agent. When a peer submits transaction resources, such as shared files and computing resources, TA will check these resources and save these indexes of them. Whereas, TA will delete these indexes while the peer take away these transaction resources. If the peer log out, TA will mark its resources unavailable.

Consider the Single point of failure, we provide a spare neighbour peer for each TA. The spare peer has the same topology and trust info with TA. In this way, when one certain TA is not able to work, the spare one can substitute its job of trust-providing services such as backup, timing send and update info etc. Thanks to the exchange-info is not complex, the network spending is limited.

V. TRUST AGENT

Structure of Trust Management Scheme is shown as figure 2 below.

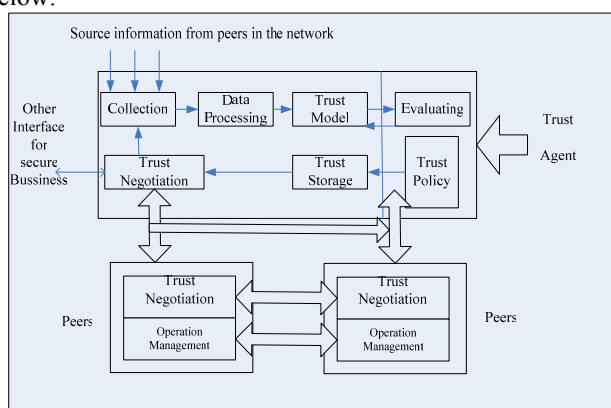


Figure 2. Structure of Trust Management Scheme

The core of the Trust Management System is the design of Trust Agent. In order to implement the Trust Management Scheme, Trust Agent needs to complete these functions, such as, the interaction of the inner and outer trust system, the maintenance of the trust database and trust certificate, the update of trust value etc. Generally, we will require Trust Agent to complete functions which include searching trust info, formalization, computing trust value, generating and maintaining trust certificate, and in the same time, it is needed to fulfill functions including updating and initializing trust value, dealing with trust request and completing the trust management and interaction in the whole P2P network environments. Then, we will introduce the main functions of TA.

A. Trust storage

Trust storage module is a important part of Trust Management System. This module mainly storages and manages the static and dynamic trust value of the peers, the operation result info, trust policy info, trust certificate info, the trust histories of peers, the operation histories of peers and etc.

As we mentioned above, the static trust value reflects the original ability of the peer, including the capability of CPU,

memory, cache, bandwidth and etc. While the dynamic trust value reflects the credit standing of the peer in the system real time, and in the same time, it is the main info for generating trust certificate.

We maintain a database table to save trust certificate info, and update the info of the table while update the certificate. While updating peer's trust value, we will save the last time peer's trust value into the trust history record table. In this way, peer's history trust info is formed for audit. When one transaction between peers is completed, each peer will report the result of it and the evaluation to each other to TA. And the trust storage module will save the evaluation to the relevant database table, and notify the trust update module to execute the event drive update.

B. Trust Certificate

Traditional certificate includes identity certificate and attribute certificate. Identity certificate binds name and public key of the main body, while attribute certificate binds name and right limit of the main body. Generally speaking, the two kinds of certificate above are both static during a period of time, and the info of identity and authorization are changeless. Moreover, the process of authentication is not change with the entity's behaviour and the time went by.

Nevertheless, trust is dynamic and closely related to the subject's concrete behaviour. Thus, we use the concept of Trust Certificate. Trust Certificate is a kind of digital certificates which can be used in the trust management system [8]. It is the objective evaluation of one entity to another, and it can reflect an entity's trust degree objectively. Trust certificate contains the relative entity's trust information such as trust value, trust validity, applied types of trust certificate and so on. TABLE 1 shows the format of trust certificate clearly.

Trust Certificate is closely related to the entity's behaviour and the time, thus its update cycle is fast and life cycle is short. It is issued by Trust Authority and it binds name and trust info of the entity. In our model, it can also be issued by Trust Agent which is authorized by Trust Authority via Proxy Signature. The most important information in trust certificate is the trust value. It directly reflects the subject's trust degree by the public's evaluations. For example, entity A will get the trust certificate of entity B from Trust Agent before it transactions with B. It can gain an objective appraise to B in aspect of trust degree and decides whether transact with B.

Table 1 shows the format of trust certificate clearly.

Table 1. The format of trust certificate

Version	An integer, "1" means the certificate's version is 1.
Serial Number	The unique identifier of the certificate, it's an integer.
Issuer	The name of the issuer.
Signature Algorithm	The signature algorithm used in signing this certificate.
Subject	The name of the Subject.

Validity	Not Before	The start time of the certificate's validity.
	Not After	The end time of the certificate's validity.
Trust Value	The trust value of the subject. Generally, one entity's trust degree is fuzzy, and it can't be described and disposed with the normal precise logic. Thus we should not express it with 0 or 1 simply, and we can induct the fuzzy theory to construct the trust value calculate model to calculate the trust value. Here, we restrict the interval of trust value in 0 to 1. 1 means the best trust degree.	
Applied Types	The applied types of this certificate. This attribute defines where this trust certificate can be used.	
Extension	(optional) Define some additional trust information or the manage ability of the certificate.	
Issuer's Signature	Algorithm	The signature algorithm.
	Encrypted	The signature to this certificate.

C. Trust Policy

Trust Policy is a profile of the whole system, and its function is specifying dynamic trust attributes which include trust value relevant policy and trust certificate relevant policy.

The trust value relevant policy mainly consists of attenuation policy and initialization policy. As we mentioned above, trust value is change with time went by, if peer is long-term inactive in trust system, its trust value will slump with time went by. In this way, a inspirit mechanism is formed in trust system. In order to keep well credit standing, peer will often participate in operation. So it can avoid the common free riders phenomena in P2P system. Furthermore, the slumping of the trust value is not linear but exponential. In this way, it can be avoided that peer's trust value slumps unlimited, and its trust value will keep at a lower level when peer is long-term inactive.

The ways of initializing trust value include indistinctive initialization, sorted initialization, initialization based recommendation and dynamic initialization with auto adaptive. Initialization of trust value has a great influence on trust's objectivity. So it should be selected carefully according to the actual demand of the system. In our model, we adopt sorted initialization according to the capability of the peer.

The trust certificate relevant policy mainly includes the definition of update cycle and period of validity of trust certificate and so on. Because trust certificate have dynamic performance comparing to identity certificate and attribute certificate, we take its update cycle and period of validity into the trust policy. In this way, we can adjust them dynamically and conveniently so as to fit the demand of concrete business.

D. Trust Negotiation

Trust Negotiation is a series of processes of interactions between Trust Agent and peers. The interaction mainly includes the initiation of peers, reporting state of peers, the interaction between TA and initiator of operation, and the interaction between TA and participator of operation. And the format of the interaction adopts customized XML.

1) Initiation of peers: The operation-peer submits its basic info to Trust Agent. Trust Agent initiates the original trust value, trust certificate and other trust info of the operation-peer according to submitting basic info. And then, Trust Agent will store the initialization registered info into the relevant database tables. Finally, Trust Agent will signal back the operation-peer to confirm it.

2) Reporting state of peers: After the operation-peer joins the system, it will send timing-signal to Trust Agent in the form of heartbeat. In this way, Trust Agent can be aware of peer's online-state.

3) The interaction between TA and initiator: Firstly, the initiator will send message to Trust Agent to request resources. Then, Trust Agent will parse the message and confirm the request parameters. After dealing with it, Trust Agent will send back the relevant resource lists and their trust certificate to the requestor. The operation-peer gets these resources and completes the operation according its local operation policy. When the operation is accomplished, the initiator will report the result of the operation and the evaluation. Finally, after receiving the result info, Trust Agent will signal back the initiator to confirm it. Figure 3 shows the flow of the process.

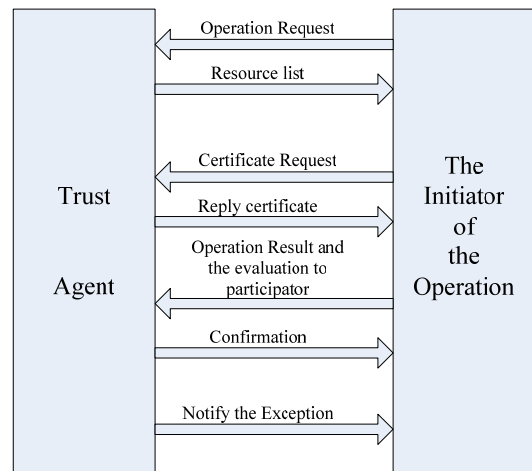


Figure 3. The interaction between TA and initiator

4) The interaction between TA and participator: Firstly, the participator will submit the accepted info of the operation to Trust Agent after it receives and accept the operation request. Then, Trust Agent will signal back the participator to confirm it. Finally, the participator should also report the result of the operation and the evaluation. Figure 4 shows the flow of the process.

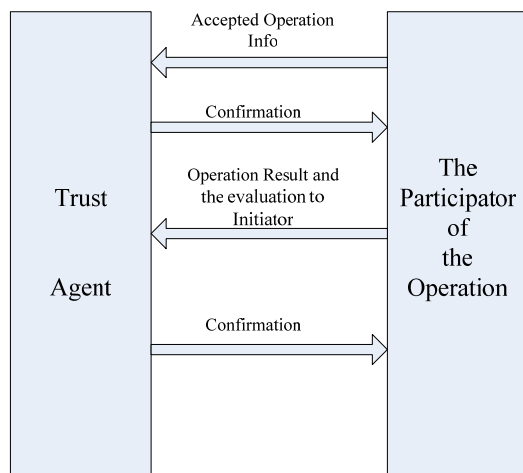


Figure 4. The interaction between TA and participator

5) **TA's job:** During the processes of interaction with peers, the main job of Trust Agent is dealing with info of trust relevant and providing trust services. In the same time, Trust Agent watches the online-state of the peers via heartbeat of the peers. If it finds peers exceptional offline, Trust Agent needs to send exception messages to the initiator of the operation.

VI. RESULTS AND DISCUSSION

We evaluated this trust management system for P2P transactions by comparing the failure rate of transactions with the help of this system against that without the help of it.

In the simulation, we have 100 total number of nodes. Among them, 20 nodes are malicious. We assume the initiate trust value of peers is stochastic. We do simulation of two cases. The first case is that peers transact with each other in the common environment. In this case, it is trust unaware and peer randomly selects peers to transact. If there is a malicious node, the transaction will fail. The second case is that peers transact with each other in this trust management system. In this case, it is trust aware and peer selects peers to transact according to the trust value of the peers, which is maintained by the trust management system. In both cases, we simulate 10, 50, 100, 200, 500, 1000 transactions respectively, and compare the result of them.

From Figure 5, we conclude that the number of failure rate of transactions in this trust management system is lower than the transactions not in this system. Since peers do not use this trust management system, they do not pay attention to the past transaction history of the resource selected. Even though the resource continuously not service well, if it has the highest rank, it will be selected repeatedly in the trust unaware transactions, which leads to higher failure rate.

However, the failure rate of transactions with the help of this system becomes lower along with the number of transactions increasing. That is because, in this trust management system, if one peer has an attack behaviour, the Trust Agent will catch and deal with it. And the trust value of the peer will be reduced by TA according the trust policy. If

someone attacks on many occasions, its trust value will reduce rapidly, and it will no longer be chose when the value plays down under the base line of the resource users.

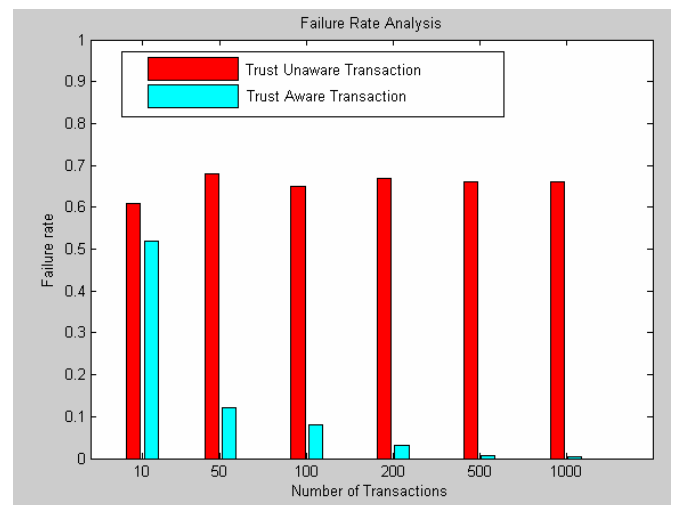


Figure 5. Failure Rate Analysis

Figure 6 shows the trend of failure rate of transaction in both cases. The failure rate of transaction in under ordinary circumstances is holding a high failure rate at about 66% no matter how many number of transactions. It maintains a stable trend. And the failure rate of transactions in this trust management system circumstances quickly drops to almost 0 along with the number of transactions increases. This is attributed to this trust management system, because it does a lot of works including maintenance trust value and trust certificate, the implementation of trust policy and etc. In this system, it adopts a strict reward and punishment mechanism. If peer attacks, its trust value will be dropped a lot. With the help of this system, the malicious peer will be isolated rapidly. Hence, the trend of failure rate of transaction in this system will drop rapidly with the increase of the number of transactions.

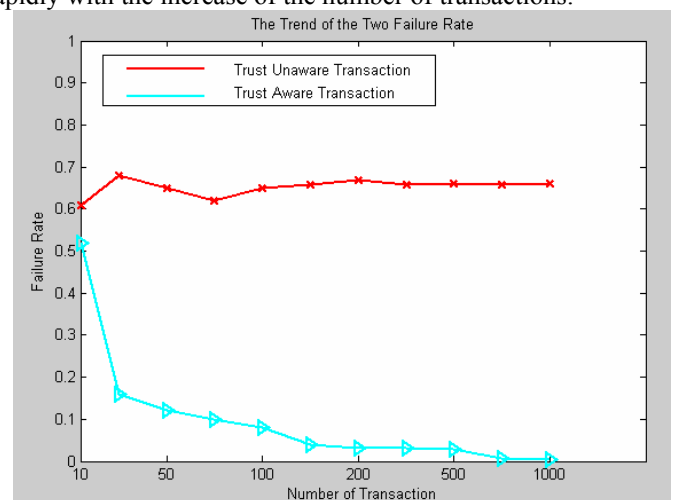


Figure 6. The Trend of The Two Failure Rate

VII. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented a systematic scheme of trust management for p2p networks, and our team members are trying to complete the prototype of it. As we say, most of the current schemes rely on trust models, but the research in systematic managing scheme is scarce. Our works emphasize the whole frame of trust management, and we can use the best suited trust model in our system. We future go ahead and consummate the scheme and do its detail work.

ACKNOWLEDGEMENTS

This work is supported by National Basic Research Program of China (973 Program) (No. 2007CB310704), National Natural Science Foundation of China (No. 90718001, U0835 001)

REFERENCES

- [1] Yuan Shi-jin. The Research on Key Technologies of Trust Management. The discourse of doctor's degree of Fudan University.
- [2] Resnick, P., Zeckhauser, R., Friedman, E., and Kuwabara, K. "Reputation systems." *Commn. of the ACM*, 43(12), 2000, 45-48.
- [3] Gnutella, <http://www.gnutella.com>.
- [4] Napster website: <http://www.napster.com>.
- [5] RATNASAMY S, FRANCIS P, HANDLEY M, et al. "A Scalable Content-addressable Network [A]." *Proceedings of ACM SIGCOMM 01[C]*, San Diego: California, 2001: 161—172.
- [6] STOICA I, MORRIS R, KARGER D, et al. "Chord: a Scalable Peer-to-peer Lookup Service for Internet Applications[A]." *Proceedings of ACM SIGCOMM 01[C]*, San Diego California, 2001: 35—89.
- [7] FREDRIK B, LARS A. "Performance of Pastry in a Heterogeneous System[A]." *Proceedings of the 4th International Conference on Peer to Peer Computing(P2P' 04)[C]*, Switzerland: Zurich, 2004: 32~37.
- [8] David Chadwick. *Understanding X. 500 — The Directory*. University of Salford. UK. ISBN 185 0322 813.1996