Managing Cluster-Based Trust Model for Peer to Peer Networks

U.swath

M.Tech CSE Dept.,
Institute of Aeronautical Engineering,
HYD-500043, AP, India.

Dr.N. Chandra Sekhar Reddy

Professor, CSE Dept.,
Institute of Aeronautical Engineering,HYD-500043,AP,India. .

Abstract- The peer-to-peer approach to design large-scale systems has significant benefits including scalability, low cost of ownership, robustness, and ability to provide site autonomy. Peer-to-Peer network represents a large portion of internet traffic, and becomes fundamental data sources. Because of lacking the security mechanism from third-party, P2P network will face some severe trust problems such as service faking and resource abusing by some malicious peers. The conventional security measures can not be used to cater for this demand, whereas the scenario based on reputation has widely been accepted. According to our model, the trust value of a peer is the probability that this peer sends correct messages to other peers, provided that this probability is at least. Through studying the present reputation, the paper presents a cluster-based reputation model. The model is consisted by reputation mechanism and cluster. In the model, we take the reputation mechanism for realizing the security transaction; and the network topology structure of CBRM adopts the cluster, so efficiency of reputation management is noticeably raised. In order to improve security, reduce the network traffic brought by management of reputation, and enhance stability of cluster, when we select reputation, the average historical online time, and the network bandwidth as the elementary components of the comprehensive performance of node. Simulation results showed that the proposed model improved the security, reduced the network traffic, and enhanced stability of cluster.

Keywords:Reputation model,peer to peer network,confidentiality,clustered based model.

I. INTRODUCTION

Peer- Peer System can be considered as a set of interconnected domains interacting in a peer-to-peerfashion. One goal of such systems is to encourage domain-to-domain interactions and increase the confidence of the domains to share their resources (a) without losing control over their own resources, and (b) ensure confidentiality for other domains. Sharing resources across institutional boundaries creates several issues related to *quality of service* (QoS) and trust. Handling these issues are complicated in NC systems due to distributed ownership, site autonomy, resource provider heterogeneity, and diverse resource clients. Peer-to-Peer (P2P) networks are self-configuring networks with minimal or no central control [1]. It integrates the scattered network resources, improves the capability of resources sharing, and maximizes the utilization of resources. So P2P network gets the fast development. Due to the open, free, and anonymous nature of P2P network, so it is more vulnerable to dissemination of malicious or spurious content, viruses, malicious code, worms, etc. The traditional security techniques developed for their centralized distributed systems are inappropriate for P2P networks by the virtue of the centralized nature. For these problems, one feasible way to minimize the threats is to establish the reputation model. In recent years, reputation has widely been studied in P2P network. Both reputation and trust are different, but also have relations both. Trust is abstract and has the intuitive sense [2], the subjectivity, dynamic; and reputation is metric of trust and easily builds model. Reputation model is based on a network topology and builds the reputation mechanism. Resnick et al. [3] defines the reputation system as “a system that collects, distributes, and aggregates feedback about consumer's past behaviors.” Reference [4], for the problems of self-replicating inauthentic files, presents a distributed and secure method to compute global trust values, based on power iteration. Literature [5], in order to use community-based reputations to help estimate the trustworthiness of peers to minimize threats of communities, presents a reputation-based trust supporting framework. Literature [6], for enabling peers to represent and update their trust in other peers for sharing files, proposes a Bayesian network-based trust model for building reputation based on recommendations in P2P networks. Literature [7], for authentication and recommendation of trust, presents a method for the valuation of trustworthiness which can be used to accept or reject an entity as being suitable for sensitive tasks. Literature [8] poses the reputation model based on reinforcement machine learning from a computer-science perspective. Literature [9], for the problems caused by anonymity in P2P, proposes a self-regulating system where reputation sharing is realized through a distributed polling algorithm. But the present models emphasize particularly on realization of function and take little account of feasibility of application, especially in the aspects of network security, stability, and network traffic. Combined with the existing reputation model and features of the P2P network, the paper proposes the cluster-based reputation model.

The model is consisted of reputation mechanism and cluster. Reputation mechanism realizes the network security by reputation evaluation. Cluster is a new network topology, its organization structure is flexible, and its management is very convenient. In the model, reputation represents node's credibility. For a node, the higher the reputation of node is, the more credible it is. In the election of super node and transaction between nodes, node of the high reputation will have more priorities or chances, and the low reputation will have more restrictions. Because the comprehensive performance of node considers the average historical online time and network bandwidth, the network flows and stability of cluster are improved.

II. RELATED WORK

The representation of trust model in peer-to-peer Networks, we use this model in later sections to develop several protocols that allow peers to compute the trust values of other peers in their peer-to-peer networks. Our trust model is based on the following three assumptions.

- *Trust Values*: Each peer in a peer-to-peer network has a fixed probability of "telling" the truth. We refer to this probability as the *trust value* of the peer. For example, when a peer p[i], whose trust value is *tr*, is about to send a message or file to another peer p[j] in its network, p[i] either sends the correct message or file with probability *tr* to p[j], or sends any wrong message or any wrong file with probability *(1-tr)* to p[j]. A peer whose trust value is at least 0.6 is called a *good peer*; otherwise it is called a *bad peer*.
- *Sources and Monitors*: A good peer uses a *source discovery protocol* to actively monitor several good peers in its network, and accurately estimate the trust values of each of them. If p[i] monitors a good peer p[j] and accurately estimates its trust value (to ensure that it is indeed a good peer), then p[j] is called a *source* of p[i] and p[i] is called a *monitor* of p[j]. Note that a good peer can have several sources and several monitors, and that its sources and monitors may overlap.
- *The Good Sub-network*: A good peer knows all its sources, all its monitors and the trust value of everyone of its sources. A good peer can send messages only to its monitors and can receive messages only from its sources. Therefore, the good peers form a sub-network, called the *good sub-network*, within the peer-to-peer network. Over the good sub-network, the good peers execute a *source propagation protocol* so that each good peer ends up with the identities and the trust values of all other good peers in the (good) sub-network. Our main focus in this paper is to develop the source propagation protocol over the good sub-network. Some explanations of the three assumptions are as follow. First, if the trust value *tr* of a peer p[i] is at most 0.5, then it is impossible for peer p[i] to effectively communicate even one bit of information to another peer p[j] in the same network. For example, assume that *tr* = 0.4 and that p[i] attempts to communicate a bit *b* to another peer p[j] by sending *b* many times to p[j]. In this case, p[j] receives bit b only 40% of the times, and receives arbitrary bits in the remaining 60% of the times. In particular, p[j] can end up receiving bit *0* half the times and receiving bit *1* half the times, and so p[j] can never determine the value of the sent bit b. On the other hand, if the trust value of a peer p[i] is larger than 0.5 but less than 0.6, then p[i] can communicate information to other peers in the network but it will take p[i] a long time and a very large number of messages to do so. Therefore, peers in a network should avoid receiving information from other peers unless they are certain that the trust values of these other peers are at least 0.6. Second, each good peer p[i] uses a source discovery protocol to identify and keep track of several good peers and accurately estimate their trust values (to ensure that they are indeed good peers and be able to download files from them). The source discovery protocol that p[i] can employ to accurately estimate the trust values of each of these good peers is to periodically request some files, that p[i] already has, from each of these good peers, then determine whether or not each returned file is correct. Third, the topology of the good sub-network can be represented by a directed graph, where each node represents a good peer, and where each directed edge from a node p[i] to a node p[j] indicates that p[i] is a source of p[j] and so p[i] can send messages to p[j]. As mentioned above, we assume that each good peer has already used the source discovery protocol to identify the identities of its sources and accurately estimate the trust values of each of them.

Now, the good peers need to use the source propagation protocol (which is presented below) so that each good peer ends up with the identities and trust values of all the good peers in the good sub-network.

III. CHARACTERISTICS OF THE TRUST MODEL

The trust architecture determines how the trust model is applied to a NC system. By design, trust modeling is necessary and appropriate only for large-scale NC systems. Therefore, the trust architecture should deal with key issues such as heterogeneity, site autonomy, and scalability that are associated with large-scale network computing systems. A straight forward approach to mapping the proposed trust model to a large-scale NC system can result in an inefficient implementation. The trust architecture presented in this section employs various techniques to address these issues. First, the NC system is divided into domains called the NCDs. The resources (RD) and clients (CD) inherit the parameters associated with the NCD. Aggregating the resources and clients into groups increases the scalability of the overall approach. Second, we assume the trust to be a slow varying attribute. If, on the contrary, trust varies much faster, then the overall system is in an unpredictable state and the deployment of a trust model is not viable. If the slow variation assumption is true, it means the trust level is updated based on a significant amount of transactional data and the overhead associated with maintaining the trust model can be amortized over a large number of transactions. Third, by limiting the number of contexts, the fragmentation of the trust space is reduced. In the example model considered in this paper, the contexts are limited to primary service types such as printing, storage, and computing.

III .CLUSTER BASED REPUTATION MECHANISM ALGORITHAM

It is mainly aimed at building reputation mechanism. The goal of reputation mechanism would manage reputation of node and predict the future behavior of node by its past behaviors. Reputation mechanism is consisted of reputation information storage, reputation information aggregation, and reputation stimulation. In order to more accurately predict the future behaviors of node, every time the reputation evaluation of node must store. The commonly used methods store the reputation data in itself or third-party. But these methods will bring a lot of network traffic and the security is low. In CBRM, way of storage is the following. Every node stores own reputation data evaluated by other nodes, the data will be encrypted and prohibited against modifying. Modification of reputation information is operated by its cluster head. Through the improved method, operations of reputation storage are done in cluster inner and by cluster head to which the node belongs, so the new way greatly reduces network traffic and enhances the network security. When a node requests a service, it firstly knows about the reputation information of resource node. Cluster head to which resource node belongs aggregates the reputation information of resource node, and sends result to the request node. The calculation formula of reputation aggregation refers to the above reputation. P2P network is a platform of open and free resources sharing. In the network, every node is equal in status and under no restraint from third-party. In order to make more nodes actively cooperate under no restraint from third-party, stimulation is needed. In CBRM, the description of reputation stimulation is as follows: The higher the reputation is, the more chances the node will get resources. Especially, when cluster is busy or resource is shortage, the higher reputation nodes will have the priorities of obtaining resources.

The initialization of cluster

The main tasks of cluster's initialization are electing the cluster head, and then building cluster. After formation of cluster, cluster head sends invitation of join to the nearby nodes. First of all, the two problems are needed to be considered. One is efficiency of clustering. Because of the dynamic of P2P network, if the efficiency of clustering is too low, and the formation of cluster will cost a lot of time. After the formation, the nearby network may have greatly changed. The other is cost of clustering. In the process of clustering, it will certainly bring a lot of network flows, and that will not be avoided, so we must improve the initialization of cluster and reduce the network traffic. Based on the above two reasons, initialization of CBRM' cluster takes the dynamic clustering, and the realization is as follows:

In the area of no cluster, for a new node which is ready to join the P2P network, first of all, it sends application of join and waits for response. Because of no cluster in the neighborhood, the new node doesn't get any answer. Then, it will calculate its own comprehensive performance. If the result is greater than$C0$, it is to be cluster head, or just waiting the join invitation of the nearby cluster head. In order to reduce the network flows, the waiting node will be limited to do any activity. After formation of cluster, clusterhead will invite the nearby nodes to join.

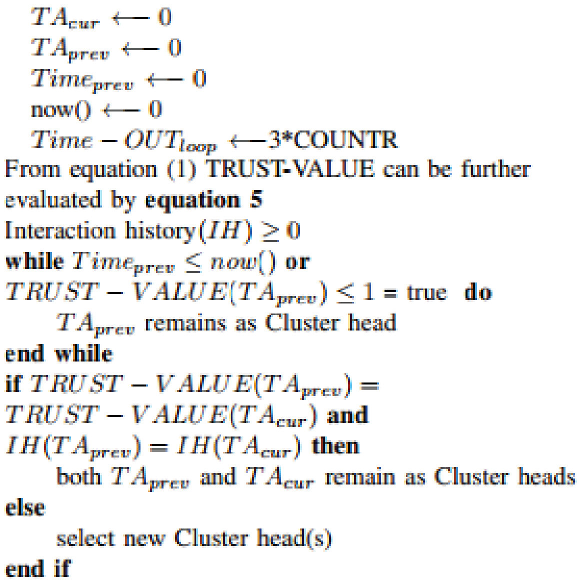
Node join

After the formation of cluster, the nearby nodes will join it. New node firstly sends the join application, after getting the join permission from nearby cluster, and both formally starts to establish communication. After communicating, the cluster head calculates C of the new node and decides its identity. For a new node, its identity may be one of the following three kinds:
1) Cluster head: C of the new node is greater than the current cluster head's.
2) Gateway: C of the new node is greater than the current gateway's, or it is the second node meeting$C0$ in the cluster.
3) Common node: in addition to above two cases, the node can be only the common member. In order to enhance stability of cluster, for the node join, the paper proposes the concept of virtual backup. Its definition is as follows: After generating the gateway, cluster head and gateway mutually store the management information of the other party in order to quickly restore when occurring the exception.

Node leave

Because of freedom, dynamic, abnormality, node frequently leaves. Node leave may be normal and abnormal. The basic principles which handle the node leave are as follows: For the normal, node must apply before leaving. But, for the exception, cluster head must communicate with its members at regular internals, if detecting its members which abnormally left, and timely handle. After node leaving, members of cluster may need adjusting. Let C denote the comprehensive performance of node, principles of adjustment are as follows: 1. If the quantity of nodes meeting $C > C0$ is greater than 2, the greatest one is cluster head and the greater one is gateway; if equal to 1, the node is cluster head and also serves as gateway; less than 1, cluster will disintegrate.

Algorithm
Cluster Based Trust Algorithm



```
  $TA_{cur} \longleftarrow 0$
  $TA_{prev} \longleftarrow 0$
  $Time_{prev} \longleftarrow 0$
  now() $\longleftarrow 0$
  $Time - OUT_{loop} \longleftarrow$3*COUNTR
From equation (1) TRUST-VALUE can be further
evaluated by equation 5
Interaction history$(IH) \geq 0$
while $Time_{prev} \leq now()$ or
$TRUST - VALUE(TA_{prev}) \leq 1$ = true  do
    $TA_{prev}$ remains as Cluster head
end while
if $TRUST - VALUE(TA_{prev}) =$
$TRUST - VALUE(TA_{cur})$ and
$IH(TA_{prev}) = IH(TA_{cur})$ then
    both $TA_{prev}$ and $TA_{cur}$ remain as Cluster heads
else
    select new Cluster head(s)
end if
```

The disintegration of cluster

When cluster doesn't have nodes meeting more than$C0$, the left nodes don't meet requirements in the aspects of reputation, the average historical average online, and network bandwidth. In order to reduce the network traffic, we will limit activities of these nodes and let them wait for the join invitation of cluster.

Reputation management strategy of cluster

In CBRM, reputation management is realized by cluster head. Main contents are as the following:

1) For choosing the cluster head, C of node must meet $C0$. When transacting between nodes, the requested node firstly considers R of the resource node, and next is$C$.

2) Cluster head manages the reputation information of its members, including such as query, update, etc. Before transaction, cluster head of service node aggregates its reputation data, and sends result to request node. After transaction, in according to reputation evaluation of request node, cluster head modifies reputation information of service node. For evaluation of malicious behavior, the request node must also offer evidence in order to prevent malicious slander.

3) When node serves as cluster head or gateway, it will be prohibited from providing service of resources sharing, but it can enjoy resource services and have more priorities of getting resource, especially when shortage of resources. For cluster-based reputation management, all operations are carried out in cluster inner, so management is very convenient, operation is very simple, and network flows brought by management will greatly reduce.

V. EVOLUTION

The evaluation is to use the *success ratio* metric to examine the effectiveness of the proposed Cluster management architecture model . To test effect of the improved model, the paper performs simulation experiments. Simulation tool uses the PeerSim [13] which is specially designed to simulate the P2P network. PeerSim is the cycle-based engine, to allow for scalability, use some simplifying assumptions, such as ignoring the details, the transport layer, etc. Through the three indices, namely, security, stability, and network traffic, we perform experiments. Let S denote the rate of effective download (RED) and it represents the proportion of security transactions in total transactions; $N1$ is the times of security transactions; N is the total times of transactions, then calculation formula of S is as the following:

$S = N1 / N$

The greater S is, the more security the system is. Because cluster head is manager of cluster, so the average historical online time of cluster head represents the stability of cluster. When choosing cluster head in simulation, we also consider the average historical online time, so we can test the stability of the cluster by calculating the online time of cluster head in simulation. Let T denote the average online time of all cluster head (AOT); N is the quantity of cluster head; ti is the online time of cluster head i . Then calculation formula of T is as the follows:

$$T = \sum_{i=1}^{N} t_i \ / N$$

The greater T is and the more stable the system is. Let F denote the network traffic (NT). NT is determined by data packet which includes query request, response message, file download, connection request, etc. The smaller F is, the less the network flows are.

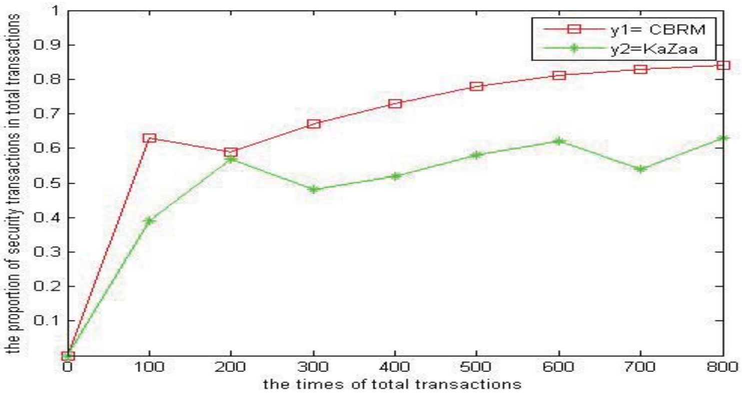


Fig1. Rate of the download

the Goodwill nodes account for 70%, the Selfish for 20%, and the Malicious for 10%. At the beginning, RED of CBRM is showing the fluctuation, which is mainly caused by the behaviors of selfish and malicious, but the selfish behaviors are restricted and malicious behaviors are quickly punished, so RED is steadily growing. Because of reputation mechanism, for malicious nodes, the reputation is difficult to restore in short time, so RED of CBRM keeps comparatively stable. For KaZaa [14], RED is relatively low and frequently fluctuates, and that is mainly caused by lacking the security mechanism. the stability verification. In Fig.2, AOT of CBRM is steadily increasing, owing to do some improvements such as considering the online time when electing the cluster head, and adding the virtual backup, etc. For KaZaa, because of just considering the limited factors when choosing super-node, so AOT of KaZaa is less than CBRM's.

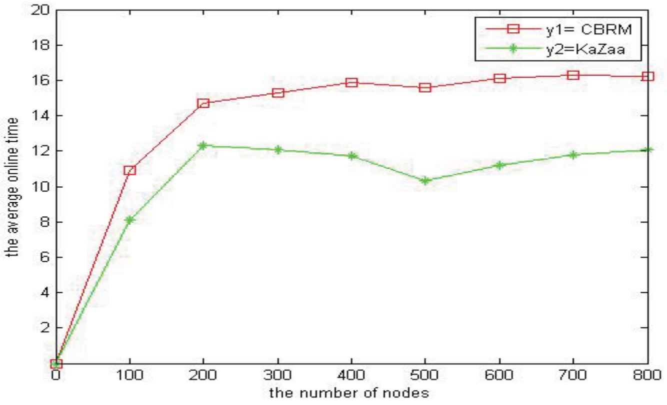


Fig2. Average time of the cluster head.

the test of network traffic. In the figure, the NT of CBRM is obviously better Because of improving on node join, node leave, disintegration, so after the formation of cluster, the cluster is comparatively stable. These improved measures reduce a lot of network flows.

VI. CONCLUSION

According to our measure, the trustvalue of a peer is the probability that this peer sends correct messages (or files) to other peers in its network. the security problems of P2P network, the paper proposed the cluster-based reputation model. The model uses the reputation mechanism to realize the security of transaction; it adopts cluster as the network topology; for the comprehensive performance of node, we select reputation, the historical average online time, the network bandwidth as the basic components; at the same time, the model improved on the cluster's initialization, node join, node leave, and the cluster's disintegration, and also posed the virtual backup. The results of simulation showed that the proposed model improved the system security, reduced the network traffic, and enhanced the stability of system. Eventually, each good peer ends up with a large list of good peers and their correct trust values, even though many of the exchanged messages between the good peers are arbitrarily wrong.

VII. FUTURE WORK

Initialization of CBRM cluster takes the dynamic clustering so attack the malicious peers.so avoid these problem using some others techniquesare to avoid attacking .enabling peers to represent and update their trust in other peers for sharing files,proposes a Bayesian network based trust model.

REFERENCES

[1] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The eigentrustalgorithm for reputation management in p2p networks," in WWW'03,May 2003.

[2] S. Lee, R. Sherwood, and B. Bhattacharjee, "Cooperative peer groupsin nice," in IEEE INFOCOM, 2003.

[3] L. Xiong and L. Liu, “Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities,” IEEE Transactions on Knowledgeand Data Engineering, vol. 16, no. 7, July 2004.

[4] E. Damiani, D. C. di Vimercati, and S. Paraboschi, “A reputation-based approach for choosing reliable resources in peer-to-peer networks,” in CCS’02, October 2002.

[5] N. Curtis, R. Safavi-Naini, and W. Susilo, “X2rep: Enhanced trust semantics for the xrep protocol,” in Applied Cryptography and Network Security, June 2004.

[6] F. Cornelli, E. Damiani, S. D. C. di Vimercati, S. Paraboschi, and P. Samarati, “Choosing reputable servent in a p2p network,” in WWW’02, 2002.

[7] M. G. Gouda and Y. Li, “The truth system: Can a system of lying processes stabilize?” 9th International Symposium on Stabilization, Safety, and Security of Distributed Systems(SSS’07), November 2007.

[8] Y. Li and M. G. Gouda, “Sources and monitors: A trust model for peerto-peer networks,” The University of Texas at Austin, UTCS TechnicalReport TR-07-60, 2007.

[9] Y. Chawathe, S. Ratnasamy, L. Breslau, N. Lanham, and S. Shenker,“Making gnutella-like p2p systems scalable,” in SIGCOMM’03, August 2003.

[10] Mingxiao Hu, Jianli Li,Building a bybrid trust model for P2P systems,Computer Apllications, Vol.28 No.12, 2008.

[11] Li Jiang feng, Zhou Xingming, Zhang Zhenxi, Peer-to-Peer network with three tier topology based on anto clustering, Computer Science, Vol.36.No2,PP68.

[12] Royer E M, Melliar-Smith P M, Moser L E, An analysis of the optimum node density for Ad Hoc mobile networks[C], ICC. Helsinki: IEEE, pp:857-861, 2001.

[13] G D.Caro, F.Dueatelle, P.Heegaard, et al. Evaluation of basic serviees in ahn, P2P and grid networks [EB/OL]. http://www.es.unibo.it/bison/deliverables /D07.Pdf, 2005.

[14] KaZaA file sharing network [EB / OL] . http : / / www . kazaacom/ ,2002.

[15] D. Dumitriu, E. Knightly, A. Kuzmanovic, I. Stoica, and W. Zwaenepoel,“Denial-of-service resilience in peer-to-peer file sharing systems,” in SIGMETRICS’05, June 2005.

[16] J. Liang, N. Naoumov, and K. W. Ross, “The index poisoning attack in p2p file sharing systems,” in IEEE INFOCOM, 2006.

[17] K. Walsh and E. G. Sirer, “Experience with an object reputation system for peer-to-peer filesharing,” in NSDI’06, May 2006.

[18] M. Srivatsa, L. Xiong, and L. Liu, “Trustguard: Countering vulnerabilities in reputation management for decentralized overlay networks,” in WWW2005, May 2005.