A Group-Based Trust and Reputation Model in Peer-to-Peer Networks

Chuan Kong, Qingxian Wang

School of Software, UESTC, Chengdu 611731, China

jerry925@163.com

Abstract: In P2P networks, peers must interact with unknown or unfamiliar peers without the benefit of trusted third parties or authorities to mediate the interactions, the quality of service can not be guaranteed, so it is very important to establish a good trust and reputation mechanism in P2P system. We present a novel group-based trust and reputation model in which the trust relationships between entities are classified into two tiers: the trust relationship between groups, and between peers. This model deals with these two kinds of trust relationships in the different way, it can reduce the impact of whitewashers and malicious peers, and make good peers happy with the high ratio of the success query. Both performance analysis and simulation show that this new model is more effective.

Keywords: p2p; group-based; trust and reputation model

1 Introduction

Network development shows a new trend towards large scale content distribution, global computing, and global storage. Meanwhile, the networking system has been shifting from Client/Server model to the Peer-to-Peer model. Oram gives a simple definition of peer-to-peer (P2P) networks as: “P2P is a class of applications that take advantage of resources storage, cycles, content, human presence available at the edges of the Internet”.

With the rapid development of P2P technology, it has been widely used in file-sharing applications, distributed computing, e-market and information management [1]. According to the research of the running P2P applications [6], a lot of drawbacks of the real P2P systems have been disclosed that performance of the most P2P systems can’t reach or even be proximal to the expectation of users and system designers. The major reason is lacking of the effective cooperation mechanism inherently in the P2P systems, so not all participators can be encouraged to take part in the systems actively and honestly. The open and dynamic nature of the peer-to-peer networks is both beneficial and harmful to the working of the system. Problems such as whitewasher and malicious users could lead to serious problems in the correct and useful functioning of the system. Such as a P2P user tries to download a file from another user in the same application, he may worry about the virus or attack embedded in that file; the user shares resources with others but who do not; and so on. All of these risks destroy the trust among the system users, so that the users will remind themselves more careful when they take actions in the system full of hazards, which holds back the users’ footstep to cooperate with others.

A good trust model is the key to assure high quality service which is provided by the P2P system and inspire users to cooperate each other effectively. At present, there are a lot of research on the trust model based on P2P system and mainly can be divided into the following categories [3] [4]: (1) Digital signature model. This method doesn't pursue the credibility of nodes, but emphasizes the credibility of the data. However, this method can only be applied for data sharing application, and can't prevent mass fraud, namely, malicious group of nodes all make signatures for inauthentic data. Currently popular file sharing applications are using this method. (2) PKI-based [7] trust model. There exist a small number of central nodes which are responsible for the supervision of the entire network and announce illegal nodes in the regular time. The legitimacy of central nodes is guaranteed by certificates issued by the CA. This kind of system usually relies on the center and has scalability and single node failure issues. (3) Global credibility model. This kind of model obtains the global credibility of nodes by using mutual satisfaction iteration among the neighbor nodes. (4) Local recommendation-based trust model. A node obtains the credibility of a certain node by asking for limited other nodes in this kind of system.

In this paper, we present a novel group-based trust and reputation model for P2P systems, which is a local

recommendation-based trust model. Within this system a peer can reason about trustworthiness of other peers based on the available local information which includes past interactions and recommendations received from others, and finally choose a peer for trading with two tiers of trust value (the trust value between peers, and global trust value). As a result, the new mechanism we proposed can get rid of dishonest and malicious peers effectively in a P2P environment where more complex malicious strategies are introduced.

The rest of this paper is organized as follows: In the second section, the related works are presented. The group-based reputation system is defined in the third section. In the fourth section, an analysis of the proposed model is followed. The conclusion is in the final section.

2 Related Works

Many literatures try to exactly define the concepts of reputation and trust. Due to the universality of the concepts, the understandings to them appear diversity. According to the ITU-T X.509, trust is defined as follows: “Generally an entity can be said to ‘trust’ a second entity when the first entity makes the assumption that the second entity will behave exactly as the first entity expects.” That means, trust is an indicator of credibility to content, and it is comparable. Another very similar concept is reputation. According to a formal definition of reputation given by Wilson [9], together with P2P environment, it is “a characteristic or attribute ascribed to one peer (or peers) A by another person (or peers) B". On the other hand, the reputation is also considered as a service provider which can be formed by means of a collection of ratings by different users, each such rating is intuitively equivalent to user satisfaction.

There are some new reputation systems in P2P in recent years. They provide different approaches to evaluate reputation.

Kamvar S. [5] proposed EigenTrust to calculate a global trust value for every peer based on their behavior history. Dou W. [3] presented a similar trust model where pre-trusted peers are unnecessary while these peers’ existence is the basic assumption of EigenTrust. Mekouar L. [8] proposed a reputation management scheme RMS PDN for partially decentralized P2P networks to enable every super-peer to maintain the contribution of its leaf peers and calculate their global trust value. Most of the reputation systems enable peers to calculate a local trust value for a given peer with shared information. Credence is a subjective, independent and local reputation mechanism based on Gnutella. It defines polling mechanism, which let users vote for whether the sharing file matches the file description or not. PowerTrust is a global, robust and scalable reputation system based on power-law. It uses trust overlay network (TON) model to analyze the power-law distribution of peer feedbacks.

3 A Group-Based Trust and Reputation Model

To improve the cooperation between users and reduce the impact of malicious peers, we propose a group-based trust and reputation model for P2P networks. This model can be used to deal with trust relationship between the entities in peer-to-peer environment and help peer-to-peer entities make trust choice. In this model the trust relationship is classified into two tiers: the trust relationship between groups, and between peers. Groups establish their direct trust relationship based on the cooperation between them. A group evaluates the credibility of members according to their behavior history of proving services with other peers. The system selects a node whose performance is the optimal as a super-node in each group of nodes. Trust and reputation information of nodes and groups is stored in super-nodes. There is a lot of this kind of groups in the whole peer-to-peer structure, and super-nodes in each group are connected in the form of the pure peer-to-peer structure in the overall structure. This model can evaluate the trust relationship between the entities more accurately, thus can solve security issues more effectively in.

3.1 Mechanism of the model

As showing in the Fig.1, in the group-based trust and reputation architecture, all the users are organized into groups. In simplicity, we assume that one user belong to only one group (in the case of the user belonging to more than one group, the user can be looked as joining the different group with different identity). Each group is assigned a unique identity called group id (GId), and each user in each group is also assigned an unique identity locally called member id (MId), so every user can be iden-

978-1-935068-01-3 © 2009 SciRes.

tified uniquely by combining his MId with GId.

In each group, all the members contribute a part of their storage to cooperatively store and maintain the trust and reputation information set which consists of group id (GId), member id (MId), number of action, trust value for each node that have ever cooperated with, threshold value of trust (TVT). The number of action is used to determine whether the user is new user or old user. The trust value is the extent of trustable for other nodes. The reputation value is the indication of the user's reliability. This trust and reputation information can be located in the common storage through the distributed hash table (DHT). There is only one super-node in each group, and the super-node holds a table including group id (GId), other groups' reputation value, each member's id, each member's global trust value, the threshold value of trust (TVTG) for kicking node out of group.

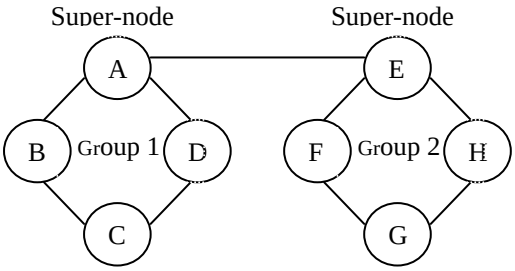

Fig.1 Group-based peer-to-peer structure

(1) When a node B wants to select node F for a service, he firstly checks the trust value of cooperator through his storage information, and then compares with TVT, finally determines whether to do. The threshold value of trust is set by group member own, and the node only cooperates with other node whose trust value overtops his TVT. After the service, node B update the trust value of node F ($T_{b,f}$), and sends $T_{b,f}$ to super-node E, then super-node E calculates global trust value of node F (GT_f).

(2) If node B wants to select node F for a service, but there is no trust value of node F in his storage information, he will ask super-node A for some information. Super-node A sends a message to super-node E, and super-node E gives GT_f back. When node B receives GT_f, he compares with his TVT and determines whether to do.

(3) If node B wants to select a node for a service, but nobody's trust value overtops his TVT in the storage information, then he asks super-node A for recommendation. Super-node A checks every group's reputation value, and then chooses a best one for a message. The super-node's reputation value represents his group's reputation value. Suppose the best one is group 2, the super-node E recommends node G for a service. When node B receives recommendation, he sends a request to node G. After the transaction, node B updates the trust value of node F ($T_{b,g}$), super-node E updates global trust value of node G (GT_g), and system updates the reputation value of super-node E.

3.2 Trust and reputation value calculation

The trust value calculation of the model is divided into calculation between nodes and global. Each group has only one reputation value. The trust value is a discrete value between -1 and 1. The results of evaluation are more near to 1, namely the node obtains the more satisfactory services, or the opposite. The reputation value is a value between 0 and 1. The reputation value of a node more near to 1 means he is more reliable.

- **Trust value calculation between nodes**

Let Tij denote the trust value between node i and j, which is calculated by the past direct behavior between nodes, and Tij is defined:

$$T_{ij} = \frac{Sat_{ij} - Dissat_{ij}}{Sat_{ij} + Dissat_{ij}} * \theta(t - t_{ij}) \qquad (1)$$

Where $Dissat_{ij}$ represents the number of dissatisfied trades between node i and j. Faked files, virus and interrupting downloads will lead to dissatisfaction. Sat_{ij} represents the number of satisfied trades. In the time decay function $\theta(t-t_{ij})$, t_{ij} represents the time of the latest trade between node i and j.

- **Calculate the global trust value of node**

Let T_i denote the global trust value of node i, which is calculated by the past direct behavior with other nodes, and T_i is defined:

$$T_i = (1-\alpha)T_{i0} * \alpha T_{ij} \qquad (2)$$

Where T_{i0} is the original global trust value of node i, and α represents the importance proportion of direct trust to the global trust.

- **Calculate the reputation value of group**

As the super-node's reputation value represents his group's reputation value, so we only calculate the reputation value of super-node. Suppose node u in group B wants to select a node for a service, the super-node k of group C recommends his group member node j to node u for a transaction. Let T_j denote the global trust value of node j, T_{kj} denote the trust value between node k and j, and R_k denote the reputation value of super-node k.

(1) The trade is successful.

If T_{kj} near to T_j, it means super-node k provides a reliable recommendation, the reputation value of super-node k should be improved; if T_{kj} far from T_j, it means super-node k provides an unreliable recommendation, the reputation value of super-node k should be decreased.

(2) The trade is failed.

If T_{kj} far from T_j, it means super-node k provides an unreliable recommendation, the reputation value of super-node k should be decreased; if T_{kj} near to T_j, it means super-node k provides a reliable recommendation, the reputation value of super-node k should be improved.

R_k is calculated by using the following formula:

The trade is successful:

$$R_k = \begin{cases} R_k / 2 - - - (|T_{kj} - T_j| > 0.5) \\ R_k - - - (0.2 < |T_{kj} - T_j| < 0.5) \\ R_k + 0.1 - - - (|T_{kj} - T_j| < 0.2) \end{cases} \quad (3)$$

The trade is failed:

$$R_k = \begin{cases} R_k + 0.1 - - - (|T_{kj} - T_j| > 0.5) \\ R_k - - - (0.2 < |T_{kj} - T_j| < 0.5) \\ R_k / 2 - - - (|T_{kj} - T_j| < 0.2) \end{cases} \quad (4)$$

When R_k overtop 1, gets 1 as the reputation value.

4 Performance analyses

When the node calculates the trust value, it not only considers transaction histories of the local records, but also asks for recommendations of super-nodes in the group. If small numbers of nodes fail, it doesn't have too much effect on the entire trust value calculation, so the reliability of the model is greatly improved. Because the local stores are only transaction records participated in by their own, and recommending to other nodes is more reliable, thus making the accurate judgment to the trust value is guaranteed.

The group based architecture can improve the management of nodes and the cooperation between them; it is an effective strategy to limit the whitewasher's behaviors and reduce the impact of them. If a node often shows poor performance in his group, the trust value of this node will under the threshold value of trust, and then he will be kicked out of his group. When this happens, it is difficult for the node to find another group. So the mechanism makes users cherish their trust relationship between others, and inspires users to have a good performance when cooperating with others.

Trust values are stored in the node itself in this model and need not other nodes participate in the management, so it prevents the trust value from being altered, forged or deleted by malicious nodes, thus the integrity of the trust value is guaranteed.

5 Conclusions

In this paper, we propose a novel group-based trust and reputation model based on the super-node network architecture. The structure of this model is very simple. The model is very easy to be accepted by users and can suit for many kinds of peer-to-peer application environment. The group–based mechanism make users cherish their prestige, and the trust and reputation mechanism cause users make a better choice for cooperating with others. As a result, good peers can be distinguished from malicious ones. Therefore, choosing the download source based on the trust value and recommendation makes good peers happy with the high ratio of the success query and the high satisfaction level under malicious collusive attacks with front peers.

References (参考文献)

[1] Oram, A.: Peer to Peer: Harnessing the power of disruptive technologies[M]. ISBN 0-596-00110-X, 2001

[2] Damiani E., di Vimercati D. C., Paraboschi S., et.al.:A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks[A]. In: Proceedings of the 9th ACM conference on Computer and communications security[C]. Washington.DC, USA: ACM Press, 2002. 207-216.

[3] W. Dou, H.M. Wang, Y. Jia, A recommendation-based peer-to-peer trust model[J]. Journal of Software, 2004, 15 (4), 571-583.

[4] F. Comelli, E. Damiani, S. D. C. Vimercati, Choosing reputable servents in a P2P network[A]. In: Proceedings of the 11th International World Wide Web Conference[C]. Hawaii, USA: ACM Press, 2002. 376-386.

[5] Kamvar S D, Schlosser M, and Garcia-Molina H, Eigenrep: Reputation management in p2p networks[A]. In: Proceedings of

978-1-935068-01-3 © 2009 SciRes.

the 12th International World Wide Web Conference [C], Budapest, Hungary: ACM Press, 2003. 41-47.

[6] K.P. Gummadi, S. Saroiu and S.D. Gribble, “A Measurement Study of Peer-to-Peer File Sharing Systems”[A], In: Proceedings of Multimedia Computing and Networking[C]. San Jose, USA: ACM Press, 2002(MMCN’02).

[7] SD. Kamvar, MT. EigenRep Schlosser, Reputation management in P2P networks[A], In: Proceedings of the 12th International World Wide Web Conference[C]. Budapest, Hungary: ACM Press, 2003. 123-134.

[8] Mekouar L., Iraqi Y., and Boutaba R.: A Reputation Management and Selection Advisor Schemes for Peer-to-Peer Systems[A]. In Lecture Notes in Computer Science[C]. Berlin:Springer-Heidelberg, 2004. 208-219.

[9] Wilson, R.: Reputation in games and markets[A]. In: Roth, A. (ed.) Game-theoretic models of bargaining[C]. New York: Cambridge University Press, 1985. 65–84.

[10] Indranil G,Ken B,Prakash L,et al.Kelips: Building an efficient and stable P2P DHT through increased memory and background overhead[A]. In: Proceedings of 2nd International Workshop on Peer-to-Peer Systems[C]. New York: ACM Press, 2003. 37-45.