Reliable P2P File Sharing Service

Jung-Hwa Shin[1], Weon Shin[2], and Kyung-Hyune Rhee[3,⋆]

[1] Department of Computer Science, Pukyong National University,
599-1 Daeyeon 3-Dong Nam-Gu,
Busan, 608-737, Republic of Korea
shinjh@pknu.ac.kr

[2] Department of Information Security, TongMyung University,
535 Yongdang Dong Nam-Gu,
Busan, 608-711, Republic of Korea
shinweon@tu.ac.kr

[3] Division of Electronic, Computer and Telecommunication Engineering, Pukyong National University
khrhee@pknu.ac.kr

Abstract. A P2P service is a popular for sharing various information through direct connection among two or more peer entities. This service which does not require a dedicated server can be used for finding and exchanging information freely. P2P file sharing systems have become popular as a new paradigm for information exchange. All users who use file sharing service can use shared files of each other freely by equal access privilege. Therefore, P2P file sharing service can suffer from free rider that only downloading without sharing on file. Also, some users can provide malicious files such as virus, worm. Recently, reputation information has been used to solve these problems. Hence, we propose the reliable P2P file sharing service model that can restrict a "free rider" and guarantee the reliability of shared files and users using reputation information.

1 Introduction

A P2P network is a computer network that does not have fixed clients and servers but a number of peer nodes that function as both clients and servers to the other nodes in the networks. By the nature of its architecture, a P2P file sharing systems provide an open and unrestricted environment for content sharing. However, this openness also makes it an ideal environment for attackers to spread their malicious contents. Also, P2P networks introduce a range of security threats, as they can be used to spread malicious software, such as viruses and Trojan horses, and easily bypass firewalls. And, there is also evidence that P2P networks suffer from free riding. Reputation systems are well suited to fight these problems. Reputation-based systems are widely used to establish trust among the members of on-line communities where the parties have no prior

[⋆] Corresponding author.

S. Joseph et al. (Eds.): AP2PC 2006, LNAI 4461, pp. 143–150, 2008.

knowledge of each other [1]. A user can evaluate the party it dealt with after a transaction, and the accumulation of such evaluations makes up a "reputation" for the involved parties. By these records of earlier transactions, a new user is able to distinguish the trustworthy parties from untrustworthy ones. In this paper, we can decrease the impact of free rider using trust value based on reputation information. Also, we can restrict use of shared files against users that provide harmful files such as virus or worm, low quality file, or file whose contents have no connection with the title. The rest of this paper is organized as following: In section 2, we describe the concept of P2P, the considerations in P2P file sharing service, and reputation-based file sharing systems. In section 3, we describe a reliable P2P file sharing service model using trust value. In section 4, we analyze the proposed model and conclude in section 5.

2 Related Works

2.1 Peer-to-Peer

P2P computing is a novel Internet-based computing paradigm which is being studied widely in recent years. In P2P systems, peers are acting as service consumer and provider simultaneously. Two main architectures of P2P networks are available today, the pure P2P model and the hybrid model [2][3]. Pure P2P models are decentralized without any central server. This kind of system is built on participating peers only, connected to each other. No central administrator unit will be involved to distribute information within the community. The network environment will be formed automatically when peers log into the system and establish connections to other peers. Hybrid P2P models are centralized in the sense that they depend on some central server. This model have the one-point failure problem. The server is not holding any data itself, it is mainly used to organize the network. According to system function, current P2P systems can be classified to three categories : file sharing, distributed processing and instant messaging. In this paper, we focus on the file sharing service.

2.2 The Consideration in P2P File Sharing Service

In P2P file sharing, the balance between resource providers and consumers must be considered. Like their counterparts in the real world, P2P communities depend on the presence of a sufficient base of communal participation and cooperation in order to function successfully. But, in the P2P context, this might mean downloading files but not sharing any for upload, or initiating queries without forwarding or answering queries from others. At best, such behavior just means increased load for everyone else; at worst, it can significantly harm the functioning of the system. A recent study on Gnutella file sharing system shows that as many as 70% of its users don't share any files at all [4]. This means that these users use the system for free. This behavior of an individual user who uses the system resources without contributing anything to the system is the first form of the Free Riding problem. Such users are referred to as free riders. Free riders use the resources available in the P2P network, but do not make any resources available. Free riding reduces the availability of information as well as the level of network performance [5][6]. Reputation can be used to solve the "free riding" in P2P file public ownership service as file or information that can display believability about user. It collects and aggregates the feedback of participants' past behaviors, which is known as reputation, and publishes the reputations so that everyone can view it freely. The reputation informs the participant about other's ability and disposition, and helps the participant to decide who to trust. Furthermore, reputation system also encourages participant to be more trustworthy and discourages those who are not trust worthy.

2.3 Reputation-Based File Sharing System

Reputation, a summary of a peer's past behavior, is a powerful tool for predicting the peer's future action. The reputation scheme helps to build trust among peers based on their past experiences and feedback from other peers. The reputation values will be used as selection criteria among peers. The goal of reputation is to maximize user satisfaction, and decrease the sharing of corrupted files.

Kazaa [7] defines a participation level for each peer based on the Mbytes it transfers and the integrity of the files it serves. Each user rates the integrity of the files it downloads as excellent, average, poor, or delete file. Based on the ratio of Mbytes uploaded and downloaded and the integrity rating of the files, the peers are assigned to three categories: low, medium, and high. The participation level score varies between 0 and 1000. A new user starts at a medium participation level of 100. The participation level score is used in prioritizing among peers during periods of high demand. The security aspects in peers modifying their locally stored participation level values are not addressed.

EigenRep [8] is a reputation management system for P2P networks. Each peer locally stores its own view of the reputation of the peers it does transactions with. The global reputation of each peer is computed by using the local reputation values assigned to it by other peers, but weighted by the global reputation of the assigning peers. This method of reputation inference rules out the possibility of malicious peers maligning the reputation of other peers.

3 Reliable P2P File Sharing Service Model

Our model based on hybrid P2P model. We intend to solve the "free riding" problem and guarantee the reliability of shared files and users using trust value based on reputation information. Also, we can restrict use of shared files against peers that provide harmful files. In our model, the server manages the trust value and shared file list on peers. When any peers query about specific files to the server, the server notifies a peer list and trust value on peers. File requester refers to their trust and select a target peer and request the file download to selected peer. File provider can permit or deny downloading by comparing the trust value of itself with the trust value of provider.

3.1 Notations

- MS : Management Server
- P_X : the identity of peer
- f_i : shared file list
- r_{old} : the latest reputation value
- r_{new} : the new reputation value
- fn_{old} : a number of shared files before transaction
- fn_{new} : a number of shared files after transaction
- GR_{old} : the sum of good reputation before transaction
- GR_{new} : the sum of good reputation after transaction
- BR_{old} : the sum of bad reputation before transaction
- BR_{new} : the sum of bad reputation after transaction
- TP_X : trust value of peers
- dn : the speed of download
- α_X : the ratio of shared files

3.2 Operations

The proposed scheme consists of four steps. At the first step, peers log in the server and register list of sharing files into the server. The second step is a query and response. Peers query to obtain a file and received a response from the server. The third step is download on the file and final step is evaluation on the file and update of the reputation and trust value.

[Step 1] Login and Registration

1. $P_i ... P_n \rightarrow MS$: Login, $MS \rightarrow P_i ... P_n$: Success
   Peers log in the server and the server identifies a correct user, and then sends the message that login is successful.

2. $P_i ... P_n \rightarrow MS$: Register $(f_i ... f_n)$
   Peers receive a response message from the server and register the file list that they want to share with other peers. The server maintains following information on peers.

$$\langle P_i ... P_n, f_i ... f_n, TP_i ... TP_n \rangle$$

[Step 2] Query and Response

1. $P_i \rightarrow MS$: Query(f)
   The P_i sends a query to obtain a file to the server.

2. $MS \rightarrow P_i$: Info$((P_i, TP_i), ..., (P_n, TP_n))$
   The server sends the peer list and their trust value.

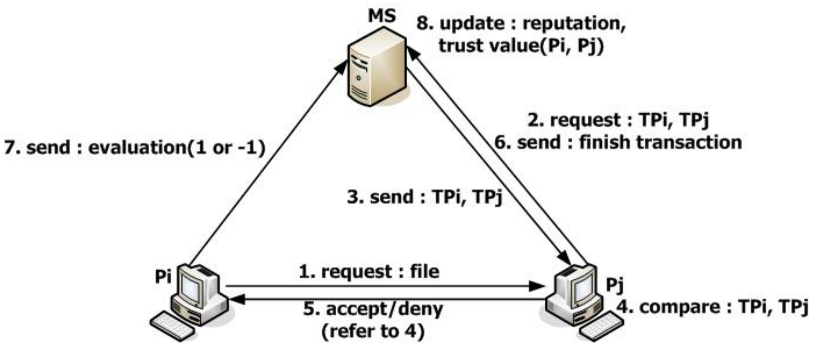
MS
8. update : reputation, trust value(Pi, Pj)
2. request : TPi, TPj
6. send : finish transaction
7. send : evaluation(1 or -1)
3. send : TPi, TPj
Pi
1. request : file
5. accept/deny (refer to 4)
Pj
4. compare : TPi, TPj

Fig. 1. Download and Evaluation

[Step 3] Download

Fig. 1 depicts the operation of download and evaluation on file.

1. The P_i chooses a peer by referring to trust value of peers and requests information for connection to the peer.

2. $MS \rightarrow P_i$: Send(IP_{P_j}, pn_{P_j})
   The server sends the message including IP address and port number of the P_j.

3. $P_i \rightarrow P_j$: Request(f)
   The P_i sends the message about file download to the P_j using the information received from the server.

4. $P_j \rightarrow MS$: Request(TP_i, TP_j)
   Before the P_j permit downloading to the P_i, he requests the trust value of the P_i and P_j to the server.

5. P_j : Compare(TP_i, TP_j)
   The server sends the trust value to the P_j and P_j compare itself trust value with the trust value of P_i.

6. $P_j \rightarrow P_i$: download accept/deny
   If the trust value of the P_i is greater than the trust value of the P_j, the P_j permit the downloading, else denies it.

$$TP_i \geq TP_j : \text{permit downloading request}$$
$$TP_i < TP_j : \text{deny downloading request}$$

By the trust value is the value that reflect on good reputation and bad reputation, peer can select the target peer by means of verification of the trust value and he decides the download request through the comparison of trust value.

[Step 4] Evaluation and Update

1. Since it can happen the situation that the P_i does not send the reputation value on the P_j, after the download is finished, the P_j notifies the finish of transaction to the Server.

2. $P_i \rightarrow MS$: Send(r_{P_j} : 1 or -1)
   After the P_i executes and verifies the downloaded file, sends the reputation on the P_j. If the file is executed correctly and is identical with the requesting file, the P_i sends 1, otherwise -1. The server receives the transaction finish message from the P_j. And then, if the server does not receive the reputation value of the P_j for a specified period of time, he increased the bad reputation value of the P_i by the ratio of shared files.

3. $MS : Update(GR_{P_i}, BR_{P_i}, TP_i, \alpha_{P_i}, GR_{P_j}, BR_{P_j}, TP_j, \alpha_{P_i})$
   The server updates the reputation value and trust value of the P_j using evaluation value received from the P_i. We can divide update method into four state according to reputation value received from latest reputation and current reputation of the P_j. Table 1 depicts the update of reputation value on file provider.

Table 1. Reputation update of the file provider

r_{old}	r_{new}	GR	BR
1	1	$GR_{old} + \lvert r_{new} \rvert * \alpha$	BR_{old}
1	-1	GR_{old}	$BR_{old} + \lvert r_{new} \rvert$
-1	1	$GR_{old} + \lvert r_{new} \rvert$	BR_{old}
-1	-1	GR_{old}	$BR_{old} + \lvert r_{new} \rvert * \alpha$

If the P_j received the good evaluation from latest transaction and current transaction, we increased by α the good reputation of the P_j. On the other hand, if the P_j received the bad evaluation from latest transaction and current transaction, we increased by α the bad reputation of the P_j. If peers received different evaluation value from latest transaction and current transaction, we reflect on evaluation value received from current transaction.

By the α is the ratio of shared files, we use to give peers incentive. The computation of α is as follows.

$$\alpha = \frac{fn_{old}}{fn_{new}}$$

The computation of the P_j's trust value based on good and bad reputation is as follows.

$$TP_j = \frac{GR_{new}-|BR_{new}|}{GR_{new}+|BR_{new}|} *dn_{P_j}$$

The reputation value of file requester(P_i) is computed as follows.

$$\begin{aligned} GR_{new} &= GR_{old} * \alpha \\ BR_{new} &= BR_{old} + \alpha \end{aligned}$$

If the P_i sent the evaluation on the P_j, we decrease by α the good reputation of the P_i. If the P_i does not send the evaluation, we increase the bad reputation of the P_i. Therefore, the trust value of the P_i decreases.

4 Analysis

In this paper, we can solve the "free riding" problem using trust value based on reputation information. Also, we can restrict use of shared files against users that provide malicious file including virus or worm, low quality file, or file whose contents have no connection with title. Therefore, we can guarantee the reliability of shared files and peers. We have performed experiment to show the effect of the proposed scheme on change of trust value on peers. Simulation parameters are as follows. a number of peers : 7, a number of shared files : 100, upload rate (100%, 80%, 60%, 40%, 0%), initial reputation and trust value : 1. Fig. 2 depict the change of trust value on peers through simulation.

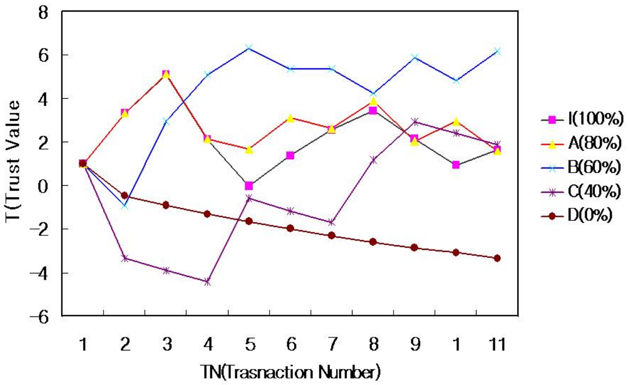

Fig. 2. The change of trust value on peers

If peers upload the file and receive the good reputation continuously, their trust value increase. On the other hand, if peers upload the file and receive the bad reputation from many peers, their reputation value decrease gradually.

Therefore, we can know that when peers provide the file and received the good reputation,their reputation increase.

Our model manages the reputation and trust value of peer using the server. Therefore, peer can not manipulate the reputation and trust value themselves and can trust the reputation and trust value that is provided by the server. Also, if a peer does not send the evaluation on the file provider after the transaction, the server decreases the reputation value of the file requester.

5 Conclusion

In this paper, we diminished the impact of free riders and malicious users by comparing the trust value of peers. In our model, if peers do not share files, they can not obtain download authority for the shared files of other peers with low trust value. Also, if peers share harmful files, they received a bad reputation from file requester and restricted download authority. Therefore, we can improve the reliability on shared files among peers and restrict the participation of free rider and malicious user by referring to the trust value of peers.

Acknowledgement

This research was supported by the Program for the Training of Graduate Students in Regional Innovation which was conducted by the Ministry of Commerce Industry and Energy of the Korean Government.

This work was supported by grant No. R01-2006-000-10260-0 from the Basic Research Program of the Korea Science and Engineering Foundation.

References

1. Selcuk, A.A., Uzun, E., Pariente, M.R.: A Reputation-Based Trust Management System for P2P Networks. In: IEEE International Symposium on Cluster Computing and the Grid, 2004, pp. 251–258 (2004)
2. Aslund, J.: Authentication in peer-to-peer system, Undergraduate thesis, Linkoping University (2002)
3. Milojicic, D.S., Kalogeraki, V., Lukose, R., Nagaraja, K., Pruyne, J., Richard, B., Rollins, S., Xu, Z.: Peer-to-Peer Computing, HP TechReport HPL-2002-57 (2002)
4. Adar, E., Humberman, B.: Free Riding on Gnutella,TechRept:SSL-00-63,Xerox PARC (2000)
5. Oram, A.: Peer-to-Peer:Harnessing the Power of Disruptive Technologies. O'Reilly, Sebastopol (2002)
6. Golle, P., Leyton-Brown, K., Mironov, I., Lillibridge, M.: Incentives for sharing in peer-to-peer networks. In: Fiege, L., Mühl, G., Wilhelm, U.G. (eds.) WELCOM 2001. LNCS, vol. 2232, pp. 75–87. Springer, Heidelberg (2001)
7. Kazaa, http://www.kazaa.com
8. Kamvar, S.D., Schlosser, M., Garcia-Molian, H.: EigenRep:Reputation Management in P2P Networks. In: Proceedings of the 12th International World Wide Web Conference, pp. 123–134. ACM Press, New York (2003)