A Credit Mechanism Based on Automatic Audit in P2P File Sharing Systems

Ruixuan Li, Cuihua Zuo, Yuntian He, Zhengding Lu
College of Computer Science and Technology,
Huazhong University of Science and Technology,
Wuhan 430074, Hubei, P. R. China
E-mail: rxli@hust.edu.cn; zuocuihua@163.com;
heyuntian1982@sohu.com; zdlu@hust.edu.cn

Abstract

Peer-to-peer (P2P) network provides an efficient way for resource sharing. However, due to lacking centralized control, free-riding phenomenon becomes a serious problem in P2P network, especially in P2P file-sharing network. This heavily restricts the development of P2P file-sharing systems. Most existing approaches need the manual intervention, such as providing credit scores. This paper proposes a credit mechanism based on automatic audit, which captures malicious behaviors through automatic detection. In this mechanism, peers can detect malicious acts spontaneously without human intervention. The simulation experiments are carried out to evaluate the performance and validity of the credit mechanism in a P2P file-sharing system. The result shows that it is effective to prevent the malicious actions in P2P network.

Keywords*: Peer-to-peer network, credit model, credit mechanism, automatic audit.*

1. Introduction

Since the introduction of Napster in 1999, peer-to-peer (P2P) network has gained quiet great development in recent years. P2P network has been an important application. People have developed various P2P file-sharing systems, and millions of users can share abundant files and data through these systems. It is estimated that there are about 60 million users of P2P systems in the United States [1] and such systems consume up to 80% of the network traffic. However, free-riding [2] [3] phenomenon has become a serious problem which restricts the development of P2P file-sharing systems.

Free-riding phenomenon means that users only expect to get resources from others while never share any resources. As discussed in [4], nearly 90% of peers in Gnutella were either sharing nothing or sharing those files never being wanted by other users. In other words, P2P traffic is entirely concentrated on a few contributors, which results in overload of these contributors and brings bottleneck of the whole system. In order to distinguish contributors from free-riders, trust management mechanism is inducted to P2P systems. The approach of trust is mainly using some algorithm to appraise a peer according to the peer's past behaviors, and sending this appraising value to other peers in P2P network. Through a reward and punishment mechanism, it can make P2P networks gradually achieve a benign development.

However, trust management mechanism of P2P system still has several problems. Some trust models rely on the centralized servers to manage all peers of the P2P network and record the peers' credit and transaction information. This is against of the idea of the pure P2P network and there is the potential risk of single failure. At the same time, some trust management mechanisms need manual intervention to form the trust or reputation value. Besides, existing trust management mechanisms lack of effective resisting measures to some malicious acts, such as juggling peers' information, collusion, slandering and exaggerating. White-washing used by free-riders is also an attack method aiming at credit mechanisms, which repeats joining P2P network with a new identity each time to escape the punishment. Existing trust management mechanism still has no good solutions to resist white-washing attack.

This paper studies a credit mechanism in pure P2P network, which is not relying on man-made intervention and can resist free-riding and other malicious acts effectively. This mechanism is restricted in the environment of P2P network without centralized

978-0-7695-3398-8/08 $25.00 © 2008 IEEE
DOI 10.1109/ICYCS.2008.378

servers or super peers. In this paper, peers can detect malicious acts spontaneously without manual intervention; consequently it can achieve the purpose of resisting malicious acts effectively.

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 details the credit mechanism based on automatic audit for P2P file sharing systems. In Section 4, we evaluate the performance of the proposed scheme with the experiments. Finally, the paper is concluded in Section 5.

2. Related work

The study of security problem of current P2P file-sharing systems mainly focuses on the reputation-based trust management technology. Reputation management system in P2P environment is responsible for searching and analyzing reputation information in order to direct collaboration decision-making among peers in network. Reputation is the evaluation of the peer's acts, including positive and negative aspects. Most of reputation systems only deal with one aspect or seldom take negative aspect into account. There are many works discussing trust and reputation management schemes in P2P network, such as those in [5] [6] [7]. However, most of these schemes only use positive (credible) or negative (not credible) information to build the reputation of entities, and the former is more familiar.

In most of the schemes, two peers who transact with each other only use "satisfaction" or "dissatisfaction" to appraise one transaction, and deduce the reputation of the target peer through collecting its evaluation. In addition, existing reputation management schemes mainly use two storage schemes of the reputation. (i) Evaluation entity maintains the trust assessment records of other entities. (ii) Objective entity maintains the trust assessment records of themselves from other entities.

Scheme (i) generally adopts a similar document query scheme to collect the feedback information of special objective's reputation. Query information can only cover part of peers of the whole system, and collect partial transaction records. This scheme is named a scheme based on local recommendation, like P2Prep [7]. In scheme (ii), the objective offers its reputation on its own initiative, such as PRIDE [8] and NICE [9], where each peer maintains its own evaluation records from other peers, and these records can be regarded as the proof of the peer's creditability.

Nowadays, there are some articles and systems studying on resisting free-riding and malicious acts and giving some solutions. Many of these solutions are designing an incentive mechanism to change the uncooperative state. Most incentive mechanisms in P2P network employ the differentiated service scheme based on reputation system. The essential idea is giving the active and virtuous peers differentiated services with faster download speeds or higher priority access to servers to promote cooperation among peers in resource consumption in P2P network.

3. Credit mechanism based on automatic audit

3.1. Credit model

In P2P file-sharing system, each peer has its credit value. We use C_{i} to denote the credit of peer i. In order to record the change of credit value in consecutive time and design the audit mechanism, each peer has a timer. We check the credit value of peers in a period of time, and use $C_{\mathrm{i}}(t)$ to denote the credit value of peer i in a period time t.

In order to evaluate the ability of the contribution and consumption of the peers, we induct two variables $B_{\mathrm{Ii}}(t)$ and $B_{\mathrm{Oi}}(t)$, where $B_{\mathrm{Ii}}(t)$ denotes the whole downloads of peer i from other peers in a period time t, and $B_{\mathrm{Oi}}(t)$ means the whole uploads from peer i in a period time t. Then, credit value $C_{\mathrm{i}}(t)$ is the value of the downloads subtracted from uploads as shown in formula (1).

$$C_i(t) = \sum_{u=0}^{t-1} (B_{Oi}(u) - B_{Ii}(u)) \tag{1}$$

However, there is an obvious shortcoming in the above formula. In order to calculate the value of $C_{\mathrm{i}}(t)$, we should get all transaction information from the first period to the t-1 period. Thus, we need an unpredicted huge amount of space to store the transaction information of peers with the passage of time. We amend formula (1) as shown in formula (2) which only use the latest m periods to calculate $C_{\mathrm{i}}(t)$, where m is a uniform constant.

$$C_i(t) = \sum_{u=t-m}^{t-1} (B_{Oi}(u) - B_{Ii}(u)) \tag{2}$$

In order to encourage peers to share their resources, we introduce the concept service threshold LIM into P2P file-sharing system, which is a positive constant and the lowest limitation of service provision. In other words, when the credit value of a peer is less than the threshold LIM, request from the peer will be refused. Peers can obtain enough credit value by sharing their resources to achieve the condition for obtaining service from other peers. This restriction method can restrain white-washing effectively and encourage sharing resources in P2P network.

However, the above method will induce another problem - system deadlock. For example, at the start of running time in the network, all peers' credit value is zero which is lower than the threshold of LIM. So any node could not obtain resources from other peers, consequently deadlock appears. Even though the system has been running and some peers can consume resources, but if only few peers has enough credit value to bear their consumption, the system is still in a state of "hunger", since a large number of poor peers have no consuming capacity. In this exceptional state, only when rich peers consume on poor peers, the situation will be alleviated.

In order to solve the above problem, we introduce the concept of valid service threshold LIMe. In each peer, we set up LIMe which is the lowest value of service provision as shown in formula (3). As described above, the service provider *p* can not obtain service from other peers if *p*'s credit value C_p is lower than LIM. In LIMe scheme, even though a peer *i* whose credit value is lower than LIM, it can obtain the service from peer *p* if its credit value C_i is no less than the valid service threshold LIMe of service provider *p*.

$$LIM_e = \min(LIM, k_{LIM} \cdot \max(C_p, 0)),$$
$$0 < k_{LIM} < 1 \qquad (3)$$

In this way, it can solve the deadlock and "hunger" problem to some extent at the start running time. Nevertheless, it can only solve the "hunger" problem in a certain period of time and can not completely solve the problem that poor peers have low credit value. Possibly, even though a peer has transactions in a long time, its credit value is still lower than LIMe of other peers. Therefore, to induct LIM to credit model, a principle should be obeyed: we should assure the credit value of the contributors larger than the LIMe of some peers, including those peers whose downloads are a little larger than uploads.

Based on the above considerations, this paper proposes a credit model inducting LIM as shown in formula (4). In (4), there are two parameters K_C and K_O, where K_C is a constant larger than 1 and K_O is a positive constant.

$$C_i(t) = \sum_{u=t-m}^{t-1}(B_{Oi}(u) - B_{Ii}(u)) + \min(k_C \cdot LIM, k_O \cdot \sum_{u=t-m}^{t-1} B_{Oi}(u)),$$
$$k_C > 1,\ k_O > 0 \qquad (4)$$

There are several advantages in this design. Firstly, two positive parameters will assure all contributors are able to gain premium of credit. Secondly, it can resist the acts of free-riding and white-washing. If a peer's download is larger than upload, the peer's credit value will fall into a minus and it can not obtain services from other peers ultimately. At the same time, it can restrain the whiter-washing action of peers with changing their identity frequently. Thirdly, it will assure the total credit value is a positive number, and the system can achieve persistent development with its running. Lastly, though download of a peer is a little larger than upload at the beginning phase, its credit value will still increase slowly and exceed LIM finally.

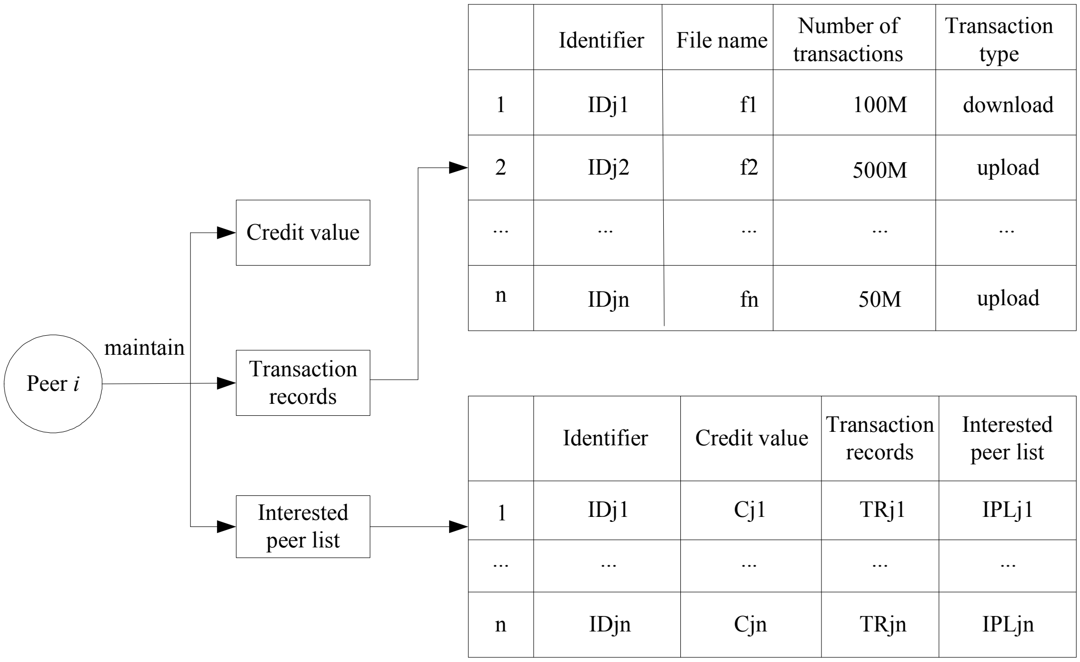
3.2. Automatic audit mechanism

After applying credit model into the system, peers in P2P network do document uploading and downloading according to the above credit model. Each peer maintains a credit table including three kinds of dynamic information: credit value, transaction records and interested peer list as shown in Figure 1.

3.2.1. Synchronization strategies. In this paper, we use the audit mechanism that is automatically launched among peers in the P2P network. Its purpose is maintaining the information integrality of the credit table of the peers. In this mechanism, we assume that each peer can hold the latest information of its interested peers. At the same time, its latest information can be known by its interested peers in time. Hence, each peer needs to issue its latest information to its interested peers, and assure the information of these peers is new. Taking the characteristics of P2P networks into account, each peer may be frequently online or offline. Therefore, we need design a Synchronization strategy to maintain the information updates. The proposed concrete synchronization strategies are as follows.

Strategy 1. At ending time of each period of peer *i*, *i* adds information timestamp into its credit value, transaction records and interested peer list. Then, *i* signs and issues this information to its interested peers who are online. The peers who receive the signed messages of peer *i* validate the signature and update their credit table information about the peer *i*.

Strategy 2. In some period of peer *j*, peer *i* and peer *j* have a transaction. Peer *i* updates its credit value in the local credit table and creates a new transaction record including identifier of peer *i*, sharing file name, the number of transactions and transaction type. Then, peer *i* signs and issues this information to its interested peers who are on-line. The peers who receive the signed messages of peer *i* validate the signature and update their credit table information about the peer *i*. The same process happens on peer *j* and its interested peers online.



	Identifier	File name	Number of transactions	Transaction type
1	IDj1	f1	100M	download
2	IDj2	f2	500M	upload
...	...	...	...	...
n	IDjn	fn	50M	upload

	Identifier	Credit value	Transaction records	Interested peer list
1	IDj1	Cj1	TRj1	IPLj1
...	...	...	...	...
n	IDjn	Cjn	TRjn	IPLjn

Figure 1. The structure of the peer's credit table

Strategy 3. After peer *i* is online, it needs to update the information of its interested peers in the local credit table. For example, when peer *i* wants to update the information of its interested peer *j*, *i* will sign and issue update request to all online peers among peer *j*'s interested peers (except *i*). After validating the signature, these peers sign and return the information which they know about peer *j* to *i*. Then, peer *i* validates the signature of return information, compares the timestamps of the returned information, and uses the information with the latest timestamp to update peer *j*'s credit table information. If peer *i* finds all peer *j*'s interested peers offline, peer *i* will issue updating request to peer *j* directly and operate just like the above process.

These three strategies apply to different situations and they ensure the detection of malicious acts in P2P system with automatic audit mechanism.

3.2.2. Audit strategies. Through the above synchronization strategies, the credit table information of each peer will be maintained on its interested peers dynamically. So each peer can automatically initiate the audit and detect the actions of other peers. We can audit the credit table information from different point of view, such as credit value, transaction records and interested peer list.

Strategy 4. audit the credit value. This is the basic audit method for credit table information. It will happen in two situations. One situation is as follows. The interested peer *j* of peer *i* initiates the audit of peer *i*'s credit value. It selects some online peers in the interested peer list of peer *i* with the probability P_C (e.g. peer *k*, not including itself) and asks peer *i* about the credit value $C_i(t)$ in a certain period of time *t*, then it compares this credit value $C_i(t)$ from peer *i* with the value $C_i(t)$ from peer *k*. If they are inconsistent, peer *j* asks peer *k* to send him the credit value $C_i(t)$ signed by *i* as the evidence of malicious acts of peer *i*.

Strategy 5. audit the transaction records. The audit of transaction records is initiated by peer *j* which is one of the interested peer of peer *i*. Concretely, within a certain period of time *t*, the interested peer *j* of peer *i* initiates the audit of transaction records with the probability P_T. Peer *j* selects some peers in the interested peer list of peer *i* with the probability P_{TS} (e.g. peer *k*), then it asks peer *k* about the transaction record between *i* and *j*, and the transaction record *i* and *k*, and checks whether the results are consistent. If they are inconsistent, peer *j* will inform peer *k* to send the transaction records to peer *j* as the proof of malicious acts of peer *i*.

Strategy 6. audit the interested peer list. The audit of interested peer list is initiated by peer *j* which is one of the interested peer of peer *i*. Concretely, within a certain period of time t, the interested peer j of peer i initiates the audit of interested peer list with the probability P_I. Peer j selects some peers in the interested peer list of peer i with the probability P_{IS} (e.g. peer k), then it asks peer k about the interested peer list of peer i and checks whether it is consistent with the interested peer list of peer i in peer j. If they are inconsistent, peer j asks peer k to send the interested peer list of peer i to peer j as the evidence of malicious acts of peer i.

Besides, the peers should obey the following two rules when initiate the automatic auditing. i) When peer i receives the updating information of the credit table from other peers, it initiates the audit to the source peer issuing the updating information. The updating actions will complete only after the audit is passed. ii) At the ending time of each period of peer i, it automatically initiates the audit to some peers in its interested peer list.

4. Performance evaluation

Through observing the simulation experiment in a certain time period, we get the relationship between the detecting rate of malicious peers and the probability of audit as shown in Figure 2 and Figure 3. We set the period of time t to 10 minutes. The number of latest records m is 12 and LIM is 10. The running time is 20 periods. The number n of interested peers for each peer is 50.

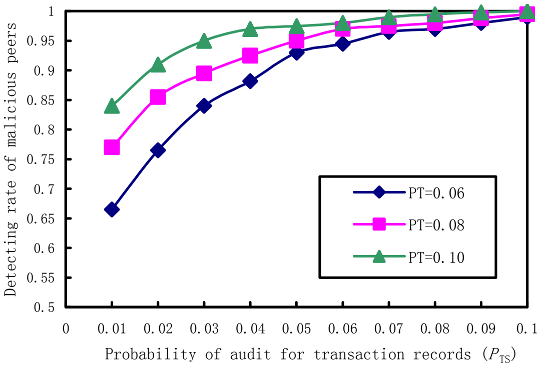


Figure 2. The relationship between the detecting rate of malicious peers and the probability of the audit for transaction records

From the above figures, the detecting rate of malicious peers increases with the increase of the probability. In Figure 2, when P_{TS} achieves at 0.05, its corresponding detecting rate will be up to larger than 0.9. That is, 90 percent malicious actions can be found in the P2P network. At the same time, in Figure 3, when P_{IS} reaches at 0.06, its corresponding detecting rate will be up to larger than 0.8. That is, 80 percent malicious actions can be detected in the network.

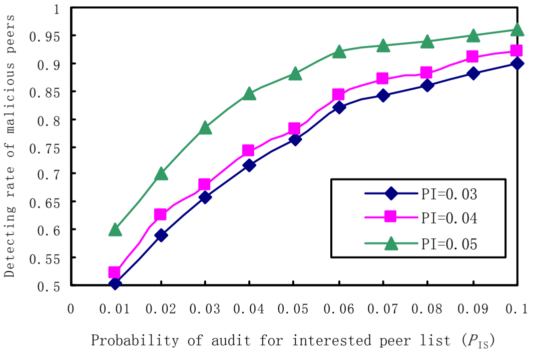


Figure 3. The relationship between the detecting rate of malicious peers and the probability of the audit for interested peer list

5. Conclusion

This paper analyzes the characteristic and shortage of existing algorithms and designs a credit model. Based on this, an automatic audit mechanism is designed. In this mechanism, each peer has the information of its interested peers and detects the date integrity of its maintenance information of credit table in some probability. Consequently, malicious actions will die out in P2P network. Through carrying out the experimental simulations, the validity of the proposed credit mechanism is proved.

The results of research in this paper show that the credit mechanism can detect malicious acts effectively and restrict the actions between transaction peers. It makes the good peers gain the ability of persistent survival and consumption. In addition, the proposed credit mechanism does not need servers or human intervention absolutely.

Acknowledgment

This research is partially supported by National Natural Science Foundation of China under grants 60403027, and 60773191, National High Technology Research and Development Program of China under grant 2007AA01Z403, Natural Science Foundation of Hubei Province under grant 2005ABA258.

References

[1] R. Stern, “Napster: a walking copyright infringement?”, IEEE Micro, 2002, 20(6): 4-5.

[2] E. Adar and B. Huberman, “Free Riding on Gnutella,” First Monday, Oct., 2000.

[3] L. Ramaswamy and L. Liu, “Free riding: A new challenge to peer-to-peer file sharing systems”, In: Proceedings of the 2003 Hawaii International Conference on System Sciences (HICSS 2003), Hawaii, 2003, pp. 220-230.

[4] N. Coleman, “The riaa and the music piracy debate”, Washingtongpost.com, Oct 2003.

[5] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “The EigenTrust Algorithm for Reputation Management in P2P Networks”, In: Proceedings of the 12th International World Wide Web Conference (WWW 2003), Budapest, Hungary, May 2003, pp. 640-651.

[6] L. Xiong and L. Liu, “A Reputation-Based Trust Model for Peer-to-Peer eCommerce Communities”, In: Proceedings of the 2003 IEEE International Conference on E-Commerce Technology (CEC'03), Newport Beach, CA, USA, 2003, pp. 275.

[7] E. Damiani, D. C. di Vimercati, S. Paraboschi, et al, “A Reputation-based approach for Choosing Reliable Resources in Peer-to-Peer Networks”, In: Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002), Washington, DC, USA, 2002, pp. 207-216.

[8] D. Prashant and D. Partha, “PRIDE: Peer-to-Peer Reputation Infrastructure for Decentralized Environments”, In: Proceedings of the 13th International World Wide Web Conference (WWW 2004), New York, 2004, pp. 480-481.

[9] S. Lee, R. Sherwood, and B. Bhattacharjee, “Cooperative Peer Groups in NICE”, In: Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, April 2003, pp. 523-544.

[10] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, “Incentives for Combatting Freeriding on P2P Networks”, In: Proceedings of the International Conference on Parallel and Distributed Computing (Euro-Par 2003), Klagenfurt, Austria, June 2003, pp. 145-149.

[11] R. T. B. Ma, S. C. M. Lee, J. C. S. Lui, et.al, “An Incentive Mechanism for P2P Networks”, In: Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS 2004), Tokyo, Japan, March 2004, pp. 516-523.

[12] Q. Sun, and H. Garcia-Molina, “SLIC: A Selfish Link-based Incentive Mechanism for Unstructured Peer-to-Peer Networks”, In: Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS 2004), Tokyo, Japan, March 2004, pp. 624-633.