Chapter 125
Defending Against Whitewashing Attacks in Peer-to-Peer File-Sharing Networks

Weimin Luo, Jingbo Liu, Jiang Xiong, and Ling Wang

Abstract Nowadays, peer-to-peer (P2P) file-sharing networks have been widely applied because of the popularity of P2P software. Complete freedom not only allows for the development of P2P networks but also brings about security risks. Malicious nodes can escape the punishment of reputation mechanisms by performing some attacks such as a whitewashing attack. In this paper, we propose a novel reputation mechanism based on two kinds of reputation so as to resist a whitewashing attack. We analyze the reputation and the capacity of the node corresponding to two different behaviors. The relationship between the behavior, capacity, and reputation of the node is discussed. We give the calculation method of our reputation mechanism and run simulations. The results show that our reputation mechanism could defend against a whitewashing attack effectively.

Keywords P2P networks • Network security • Reputation mechanism • Whitewashing attack

125.1 Introduction

P2P softwares, such as BitTorrent, have been used extensively, and the scale of P2P networks is very large. The advantage of P2P networks, such as anonymity, open, and dynamics, allow nodes to exchange resources freely, which encourages the development of P2P networks but also brings about a variety of security risks to P2P networks. To identify and isolate malicious nodes, many reputation mechanisms have been proposed. Karl et al. [1] discuss and resolve some issues of trust management in P2P networks; nevertheless, when malicious nodes are identified by trust/reputation mechanisms, they can still rejoin networks with different identities by performing whitewashing attacks.

In this paper, we propose a novel reputation mechanism that is capable of effectively defending against whitewashing attacks. The rest of the paper is

W. Luo (✉) • J. Liu • J. Xiong • L. Wang
College of Computer Science and Engineering, Chongqing Three Gorges University, 404000 Chongqing, China
e-mail: weim_luo@163.com

W.E. Wong (ed.), *Proceedings of the 4th International Conference on Computer Engineering and Networks*, Lecture Notes in Electrical Engineering 355,
DOI 10.1007/978-3-319-11104-9_125

organized as follows. Section 2 presents related works. Then we analyze the reputation and capacity of nodes in Sect. 3. Next we propose our mechanism and present the calculation method of the mechanism in Sect. 4. Simulations are run and an analysis of the results is provided in Sect. 5. Finally we give the conclusion of the paper.

125.2 Related Works

Muntasir et al. [2] provide a survey on the incentive mechanisms in P2P networks. They study free rider, whitewashing, and Sybil attacks and present the concept of such attacks and discuss how to defend against them. Michal et al. [3] study free rider and whitewasher attacks in P2P networks; however, the imposition of a penalty on all legitimate newcomers incurs a significant social loss. Pinninck et al. [4] propose a defense mechanism against whitewashing attacks. The key to their mechanism is that the transferred messages are evaluated by intermediate nodes and request messages from malicious nodes are blocked. Sohail et al. [5] study whitewashing attacks in mobile ad hoc networks. They propose a different trust mechanism based on the task completed. The new node joins the network and must complete a series of tasks. The attack cost is increased to prevent a whitewashing attack. Levine et al. [6] describe the process of a Sybil attack and point out that the trust mechanism may detect network attacks from many aspects, such as trusted certification, resource testing, and recurring costs and fees. Marti et al. [7] consider that all nodes are probably malicious, and this treatment could improve defense performance.

We find that most works focus on the trust/reputation of nodes that upload resources in transactions. Nodes that upload resources should be focused on by the trust mechanism [8], but ignoring the nodes that download resources reflects a lack of understanding of such nodes.

125.3 Two Kinds of Reputation

The node in P2P networks is the provider or consumer of resources, so it should have distinct reputation values according to different behaviors. We first define four concepts to facilitate the subsequent description. A node that uploads resources is called an upload node (UN). Whether or not a node is selected to be an UN is determined by its reputation value. Then the reputation is Upload Reputation (UR). A node that downloads resources is called a download node (DN). Whether or not a node is a DN is determined by its reputation value, and this reputation is the download reputation (DR).

125.3.1 Behavior and Reputation

In most P2P networks, the DN can freely and without limit download any resource from an UN and need not be chosen or evaluated by the UN. Thus, many studies only focus on URs, which is shortsighted.

Once a node uploads incorrect or malicious resources, the UR of the node will decrease. At the same time, if the node downloads and gives correct evaluations of the UN, then the node is a good DN and a bad UN. Other nodes will tend to choose the node to be a DN instead of an UN.

Once a node uploads good resources but gives bad evaluations to the UN after downloading, then the node is a bad DN and a good UN. It causes other nodes to choose the node to be an UN instead of a DN.

Two different scenarios indicate that the reputation of one node varies and is complicated. Whether one node is worth interaction or not, it is determined only by a single aspect will lead to an error.

125.3.2 Relationship Among Reputation, Behavior, and Capacity

A node's reputation should reflect the level of reputation and the behavior capacity. The behavior capacity can be divided into two types: download capacity and upload capacity. The download capacity determines the size of the resource the node can download from an UN in a single transaction. The upload capacity determines the size of the resource the node can upload to a DN in a single transaction.

The relationship among reputation, behavior, and capacity is complicated. We elucidate the relationship from the following three aspects:

1. Reputation can be influenced by behavior. A node should be responsible for its behavior. Good behavior leads to an increase in reputation and bad behavior leads to decrease in reputation. The value of a DR should be decreased if the node does not correctly evaluate the UN after the transaction. Accordingly, the value of an UR should be reduced if the node refuses to upload resources.
2. Reputation and capacity influence each other. When the DR of a node decreases, its download capacity should be reduced to prevent the node from giving a bad evaluation. When the UR of a node is reduced, the upload capacity should be reduced too.
3. The reputation and capacity of an upload or download influence each other. A change in the DR should affect both the download capacity and the upload capacity, as do changes in the UR. For simplicity, when a node's DR or UR changes, two kinds of capacity of the node will be affected.

125.4 Trust Mechanism Based on Two Kinds of Trust

Our reputation mechanism is based on two kinds of reputation, DR and UR, and takes the capacity into account. In our mechanism, the DN must evaluate the UN. At the same time, the UN also evaluates the DN, but this action will be performed automatically by the P2P system. The evaluation value is the value that DN i assigns to UN j after i has finished the number k transaction, which is defined as

$$E_{i\to j}^{k} = \begin{cases} 1 \\ -1 \end{cases}, \tag{125.1}$$

where 1 represents that DN is satisfied by the service of the UN and -1 represents that DN is not satisfied. Furthermore, the final evaluation should take into consideration both the resource size and the DR of the DN in order to avoid a rapid accumulation of UR. In this sense, the final evaluation value is calculated as follows:

$$E_{i\to j}^{k} = e^{-1/\left(S_{i\to j}^{k}\times R_{i}^{k}\right)} E_{i\to j}^{k}, \tag{125.2}$$

where $S_{i\to j}^{k}$ is the resource size in the number k transaction between DN i and UN j, R_i^k is the DR of DN i when the number k transaction occurs and $\lim_{S_{i\to j}^{k}\to+\infty, R_i^k\to+\infty} e^{-1/\left(S_{i\to j}^{k}\times R_i^k\right)} = 1$. This means that the final evaluation value is equivalent to the original one in order to avoid a rapid accumulation of UR by increasing the resource size or the DR of the DN.

The evaluation is given by the UN to the DN when the transaction is finished. Later it is revised by Eq. (125.2). When the final evaluation has been given, the related UR and DR will be calculated accordingly. The calculated value will be normalized and let UR and DR be in the range (0,1).

Different URs indicate different upload capacities, while the relationship between the DR and the download capacity is the same. We divide reputation and capacity into separate levels in Table 125.1.

Ipoque points out that the size of 81.49 % of files shared in P2P networks are less than 92 MB, and the size of 9 % of files shared are larger than 700 MB [8]. In our mechanism, the new node gets an initial UR of 0.25 and a DR of 0.5. The initial DR of 0.5 is enough to attract new users to acquire resources. The initial 0.25 UR is given so that new users can upload most resources. But the UR will decrease to a lower level rapidly when whitewashers upload malicious resources. The increase in the UR or DR will not cause them to exert an influence on each other. This indicates that the only way to increase the UR or DR is to finish related transactions; but when a decrease in the UR or DR reaches a lower level, the DR or UR will also decrease to a lower level.

Table 125.1 Relationship between reputation and capacity

UR or DR	Upload or download capacity (MB)
>0.75 and <1.00	>500
>0.50 and ≤0.75	>100 and ≤500
>0.25 and ≤0.50	>10 and ≤100
>0.10 and ≤0.25	>0 and ≤10
>0.00 and ≤0.10	0

Our mechanism does not punish nodes that only upload resources. However, a node will be punished when it only downloads resources. Its UR and DR will decrease to a lower level. Correspondingly, the capacity of the UR and DR will decrease. We introduce P to describe the trend of the behavior of a node and define T_k as the time consumed by the node for uploading resources at time k. T_k is calculated as

$$T_k = \begin{cases} e^{-1/(N_k \times S_k \times T_{\text{online}})} T^k_{\text{upload}} & N_k \neq 0, \\ 0 & N_k = 0, \end{cases} \tag{125.3}$$

where T^k_{upload} is the real time consumed by the node for uploading resources at time k, N_k indicates how many times the node uploads resources at time k, S_k is the resource size uploaded by the node at time k. Then P is calculated as

$$P = \frac{T_{k+1}}{\sum_{k=1}^{n} T_k / n}. \tag{125.4}$$

If P is less than 0.5 and stays at that value for at least three consecutive transactions, the mechanism will consider the possibility that the node is a whitewasher and let UR and DR of the node decrease to the next lowest level.

125.5 Simulations

We use *PeerSim* to implement and evaluate our mechanism. The network topology is obtained from *Brite*, including 1,000 peers, and satisfies a power law. There are 5,000 files distributed randomly to the normal nodes. In the simulations, the size range of 80 % of the files is (0,100], and the size range of the remaining files is (100,1,000]. In each cycle, each node downloads a random resource and issues an evaluation following the transaction. Twenty percent of the nodes are whitewashers in the network. Each experiment is run ten times, and the average of the results is taken as the final data.

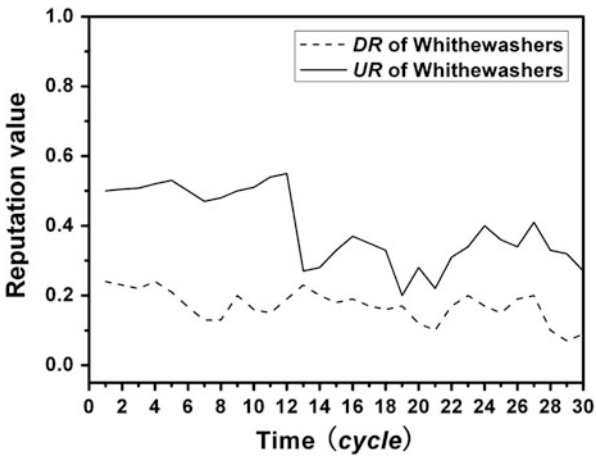

Fig. 125.1 Change of DR and UR of whitewashers

125.5.1 Whitewashers Download Resources Only

Whitewashers do not attack other normal nodes and only download resources. Here whitewashers are similar to free riders. From Fig. 125.1 we see that the DR of the whitewashers increases initially and their UR does not change. Later, their UR begins to decrease because whitewashers do not upload files, and the DR also decreases to the lowest level. This means that whitewashers have been identified and could not download or upload resources any longer.

125.5.2 Whitewashers Perform Slander Attacks

Whitewashers usually perform slander attacks. They try to undermine the UR of normal nodes and destroy the effectiveness of the trust mechanism. As shown in Fig. 125.2, the UR of normal nodes is affected by a slander attack but does not decrease rapidly because the transaction evaluation given by the whitewashers is restricted by many factors; furthermore, the DR of whitewashers will decrease rapidly, as shown in Fig. 125.1, because they only perform slander attacks and do not upload resources.

125.5.3 Whitewashers Upload Malicious Programs

As the initial UR is low in our mechanism, whitewashers will accumulate their URs initially. We see in Fig. 125.3 that the UR increases at first when whitewashers upload normal resources; nevertheless, the UR decreases rapidly when they upload

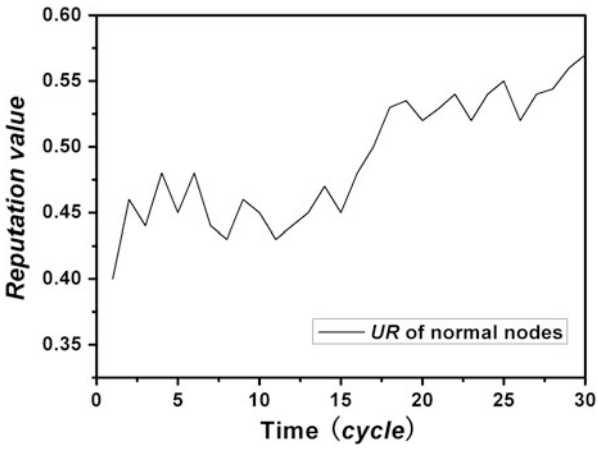

Fig. 125.2 Change in UR of normal nodes

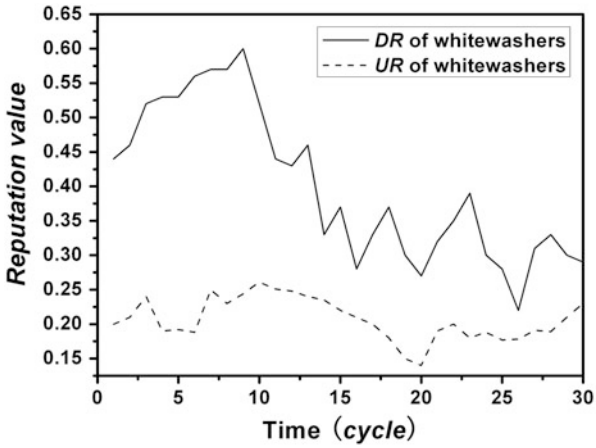

Fig. 125.3 Change of DR and UR of whitewashers

malicious resources for the bad evaluations given by other nodes. At the same time, the decrease in the UR results in a decrease in the DR.

Conclusion

In this paper, we propose a novel reputation mechanism based on two kinds of reputation with a consideration of the drawbacks of traditional reputation mechanisms in P2P networks. We discuss two kinds of node reputation along with the relationships among behavior, reputation, and capacity. The reputation mechanism is presented and the calculations given. Simulations are carried out, and the results show that our proposed mechanism can be applied to defend against whitewashing attacks.

References

1. Karl A, Zoran D. Managing trust in a peer-2-peer information system. In: Proceedings of the 10th International Conference on Information and Knowledge Management; ACM, Atlanta; 2001. p. 310–17.
2. Rahman MR. A Survey of incentive mechanisms in peer-to-peer systems, CS-2009-22. Waterloo: University of Waterloo; 2009.
3. Feldman M, Papadimitriou C, Chuang J, Stoica I. Free-riding and whitewashing in peer-to-peer systems. Sel Areas Commun. 2006;24(5):1010–9.
4. de Pinninck AP, Schorlemmer M, Sierra C, Cranefield S. A social-network defence against whitewashing. In: Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems; ACM, Toronto; 2010. p. 1563–64.
5. Abbas S, Merabti M, Llewellyn-Jones D. Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks. In: Proceedings of the 2010 IFIP Wireless Days; IEEE, Venice; 2010. p. 1–6.
6. Levine BN, Shields C, Margolin NB. A survey of solutions to the Sybil attack, 2006-052. Amherst: University of Massachusetts Amherst; 2006.
7. Marti S, Garcia-Molina H. Identity crisis: anonymity vs reputation in P2P systems. In: Proceedings of the 3rd International Conference on Peer-to-Peer Computing; IEEE, Piscataway; 2003. p. 134–41.
8. Ipoque. P2P survey 2006. http://www.ipoque.com/sites/default/files/mediafiles/documents/p2p-survey-2006.pdf. 2007.