Whitewash-Aware Reputation Management in Peer-to-Peer File Sharing Systems

Xiao YU[1] **and Satoshi FUJITA**[1]
[1]Department of Information Engineering, Hiroshima University
Higashi-Hiroshima, 739-8527, Japan

Abstract— *In this paper, we propose new schemes for the reputation management in P2P applications which discourage whitewash while encouraging good behaviors. The basic idea of the schemes is to design update rules for the reputation scores to satisfy the following requirements: 1) the score of a peer is strictly greater than the initial score at any point in time if it conducted at least one good behavior, 2) the score gradually increases if it conducted a good behavior while it rapidly decreases if it conducted a bad behavior, and 3) the strength of penalty is refined by allowing the system to give a penalty for several consecutive rounds.*

1. Introduction

Peer-to-Peer systems (P2Ps, for short) are autonomous distribute systems which have been used in many applications such as file sharing, video streaming, IP phone, and others. Different from traditional Client/Server (C/S) systems which rely on few dedicated servers, services in P2Ps are provided by each computer participating in the system in a "peer-to-peer" manner. In other words, each computer in P2Ps, called **peer** hereafter, plays the role of a client and a service provider at the same time. Such a remarkable property of P2Ps enables the designer of distributed systems to increase the scalability and the fault-tolerance of the constructed system, because it effectively removes the single point of failure existing in C/S systems as well as the service bottleneck.

However, such a distributed nature of P2Ps would cause several critical issues, such that a malicious peer can provide wrong, devastating services to the client peers, the quality of the services is not guaranteed by any authority, and the security of transactions could not be retained. In this paper, we focus on P2P reputation systems as a way of resolving such issues. In typical reputation management systems, each recipient of a service can *evaluate* the quality of the service and a collection of such evaluations will be disclosed to all participants so that it could be used to select safe and appropriate services in the next time. Examples of reputation systems include [2], [3], [4], [12], [13], [14]. A key idea of such reputation systems is to share information on past transactions among all participants to the system, i.e., if a transaction conducted by peer i is observed by peer j and another transaction conducted by i is observed by peer k ($\neq j$), by merging those two observations, we will have a more reliable evaluation concerned with the transactions conducted by peer i than the case in which each peer individually keeps such an evaluation.

In many P2P applications, a peer to have a high reputation will be granted to access high quality services such as the broader communication bandwidth and the video streaming in HD quality. On the other hand, the reputation of a peer rapidly becomes worse if it conducted malicious actions, such as an intentional provision of low quality services and the distribution of malwares such as spyware and computer viruses. In other words, the reputation system works as an incentive mechanism for the participants to conduct good behaviors. However, such an effect of reputation systems can be significantly reduced if a peer with a bad reputation could become a new participant by changing its identifier (ID) after leaving the system. Such a malicious behavior of peers is known as **whitewash**, and it has been recognized as a crucial issue in many distributed applications with reputation management [6], [5], [9].

In this paper, we propose new schemes for the reputation management in P2P applications *which discourage whitewash while encouraging good behaviors*. The basic idea of the schemes is to design update rules for the reputation scores to satisfy the following three requirements: 1) the score of a peer is strictly greater than the initial score at any point in time if it conducted at least one good behavior, 2) the score gradually increases if it conducted a good behavior while it rapidly decreases if it conducted a bad behavior, and 3) the strength of penalty is refined by allowing the system to give a penalty during several consecutive rounds.

The remainder of this paper is organized as follows. After overviewing related works in Section 2, Section 3 describes the model of P2P reputation systems. Section 4 proposes basic update rules for reputation scores, which is extended in Section 5. Section 6 proposes several reputation management schemes based on the extended update rules. Finally, Section 7 concludes the paper with future work.

2. Related Work

There are few proposals on whitewash-aware reputation management in spite of the importance of the problem. Pinninck *et al.* proposed a scheme which increases the

resistance of trust assessment schemes against whitewash attacks with the aid of social networks [7]. This scheme assumes that all interactions among peers are conducted according to the following simple protocol: 1) the initiator peer p chooses a set of potential partner peers S_p and evaluates the trust of all members in S_p; 2) p selects a peer q in S_p and sends an invitation message to q, 3) if q accepts the invitation, it starts an interaction with p, 4) after completing the interaction, q sends a feedback about the interaction to p. The key idea of the scheme is to use a social network in which each peer must be adjacent with a set of contact peers. Invitation messages are routed to the receivers through such contact peers, so that any peer wishing to interact with other peers must know at least one contact peer in the social network. Such a restriction makes a simple whitewashing meaningless, since if it changes ID, contact peers do not recognize the peer any more, so that the invitation message will not be routed to any receiver (note that the scheme could not completely prohibit whitewash if each peer can have several temporary IDs and tries to connect the network through a permanent ID among them).

Chen *et al.* proposed a scheme to identify whitewashers in P2P file sharing systems using the notion of observation preordering [1]. This scheme is based on an assumption such that actions conducted in our daily life are *habitual* so that it is hard to change even under different situations. Whitewashers are no exceptions. Namely, even after re-entering the system with a different ID, a whitewasher should contact similar peers to download files in a similar category. Observation preordering is a data structure to record the history of actions concerned with a peer, which is observed and recorded by another peer during the interaction with the target peer. Thus, for example, after interacting with peer j, peer i stores (or updates) the observation preordering concerned with j in its local storage. Suppose that j is malicious and conducts a whitewash to acquire new ID k ($\neq j$). By the assumption described above, peer k should contact peer i again to download files, and such an action is observed by i which will be stored as an observation preordering concerned with k. Thus, peer i could identify that k is likely to be j by comparing observation preorderings concerned with j and k, and if it concludes that k is j, it recognizes k as a malicious peer and degrades the reputation score of k accordingly.

How to encourage peers to conduct collaborative actions is another important issue in realizing practical incentive systems. Tseng and Chen proposed a free-rider aware reputation scheme for P2P file-sharing systems [11]. In this scheme, peers and files are divided into five levels depending on the reputation score, and the incentive mechanism is designed in such a way that a peer which does not share its files with the other peers can not access files at a higher level; i.e., in order to access files at a higher level, it needs to share its files with the other participants. This scheme also provides a penalty mechanism such that: 1) if a peer tried to share harmful files with the other peers including malwares and inauthentic files, and if such a malicious behavior is reported by the other peers, the reputation of the peer is reduced according to the penalty function (hence the level of the peer would also degrade accordingly), and 2) if a peer shares no files with the other peers, the reputation score gradually decreases as the elapsed time increases.

3. Model

In this section, we describe the model of P2P systems considered in this paper. The model of malicious actions of peers and the basic framework of reputation management will also be described.

3.1 System Model

In this paper, we consider P2P file sharing systems consisting of a number of peers which play the role of a client and a service provider at the same time. Each peer holds several files which can be shared with the other peers. Each peer, which wishes to acquire a copy of a file, firstly sends an inquiry message to the system so that the inquiry message will be delivered to peers holding the requested file [8], [10], [15]. The requesting peer will receive a response from several peers holding the requested file, and the receiver conducts the selection of a peer from the set of candidate peers according to the *reputation* of the candidates; e.g., high reputation peers are likely to be selected as an uploader compared with low reputation peers. Download of the requested file is conducted merely from the selected peer.

After completing the download, the downloader evaluates the transaction and gives a score to the uploader so that it reflects the *degree of satisfaction* of the downloader concerned with the transaction. In other words, the score is given for each transaction even if such transactions are provided by the same uploader. Such scores are aggregated to a central manager which keeps the reputation scores of all peers in the system, and if a peer conducts an evaluation of another peer, the outcome of the evaluation is immediately notified to the central manager.

3.2 Reputation Score

The **reputation score** of a peer is a sum of scores given by the downloaders. In this paper, we assume the existence of an appropriate incentive mechanism so that a peer with high reputation score will be granted a right to access high quality services, such as the higher priority while conducting a download from service providers and a wider bandwidth when it uses shared communication channels. Thus, it is natural to assume that *every rational peer should try to increase its reputation score*. If it is an honest peer, such an increase of the score will be attained by providing satisfactory transactions to the downloaders, but if it is dishonest, it tries to cheat by conducting malicious actions,

such as the issue of incorrect report to decrease the score of other peers, refusal of given requests, and provision of low quality services instead of providing requested services.

In general, to encourage honest actions of the peers, reputation scores should be managed in such a way that: 1) the score of a peer increases if it conducted collaborative actions to increase the satisfaction of downloaders (e.g., to increase the score by Δ^+), and 2) the score decreases if it conducted adversarial actions to decrease the satisfaction of downloaders (e.g., to decrease the score by Δ^-). As the strength of the penalty increases, i.e., as the value of Δ^- increases, each peer would likely to conduct collaborative actions without conducting adversarial actions, i.e., an incentive to encourage collaborative actions works well. However, if it was too strong, a peer which conducted an adversarial action would select a (malicious) way such that it quits the system once and re-enters the system as a new participant. Such a malicious behavior of a peer is called **whitewash** which is known to degrade the effectiveness of the underlying incentive mechanisms. In fact, to discourage whitewash, Δ^- must not be too large, but if it is not too large, the force to encourage honest actions should become weak.

4. Basic Update Rule

In this section, we propose a collection of update rules of the reputation scores which discourage whitewashes but encourage honest actions. The proposed rules are designed to satisfy the following requiremenrs:

1) The reputation score of a peer increases if it conducts a collaborative action, while it decreases if it conducts an adversarial action.
2) The reputation score is strictly larger than the initial score at any point in time, if it conducted at least one collaborative action.

The second requirement intends that a peer conducted collaborative actions becomes harder to be penalized even if it occasionally conducts adversarial actions.

4.1 Update Rules

Let $R_i \in (0, 1)$ denote the reputation score of peer i. R_i is initialized to R_0 at the time of participation. Suppose that peer j downloaded a file from peer i, and j is satisfied with the transaction. Then, peer j notifies the result of such a positive evaluation to the central manager, and after receiving it, the central manager updates the reputation score of i as follows:

$$R_i \;:=\; \alpha R_i + (1 - \alpha) \tag{1}$$

where α is a parameter in range $(0, 1)$. The above update rule indicates that as the value of R_i increases, the "amount of increase" gradually decreases even if it repeatedly conducts collaborative actions, e.g., if $R_0 = 0$, a sequence of collaborative actions monotonically increases the score as

$$0 \to (1 - \alpha) \to (1 - \alpha^2) \to (1 - \alpha^3) \to \cdots .$$

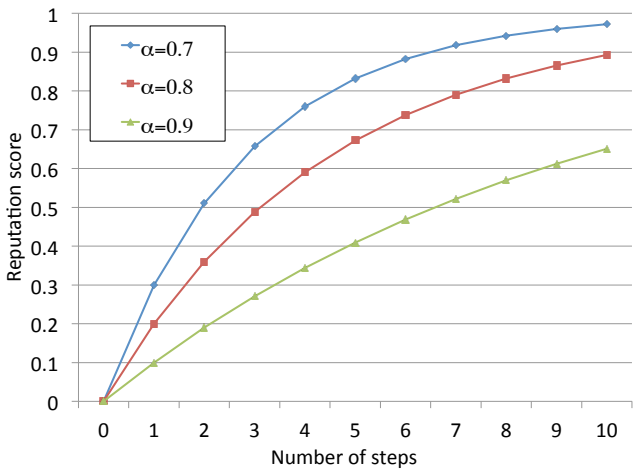


Figure 1: Increase of the reputation score along with collaborative actions ($R_0 = 0$).

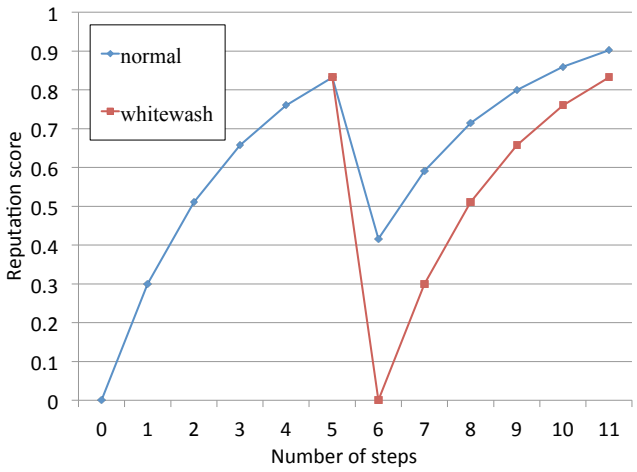


Figure 2: Badness of the reputation score under whitewash.

Figure 1 illustrates the increase of the reputation score along with collaborative actions, for different α's. On the other hand, if j is not satisfied with the transaction, j sends a negative notification to the central manager, and after receiving it, the central manager updates the reputation score of i as follows:

$$R_i \;:=\; \frac{R_i - R_0}{\beta} + R_0 \tag{2}$$

where β is a parameter greater than 1. The reader can easily verify that the second condition described above is certainly satisfied for any selection of $\beta > 1$. In fact, once $R_i > R_0$ holds, this inequality remains to hold even after any number of applications of the second update rule.

4.2 Analysis

In the last section, we observed that by conducting a whitewash, the reputation score becomes worse than the score *immediately before* the whitewash. In this section, we extend this simple argument. More concretely, we prove that by conducting a whitewash, the reputation score always becomes worse than the case without whitewash for any sequence of collaborative and adversarial actions. Let S be a ternary string representing a sequence of actions, where 0 and 1 indicate collaborative and adversarial actions respectively, and 2 indicates whitewash. Let $R(S)$ denote the reputation score of a peer after conducting an action sequence S.

We can prove the following claim.

Remark 1: Let $S = a_1, a_2, \ldots, a_n$ be a sequence of actions conducted by a user starting with a collaborative action, and S' be a sequence of actions which is obtained from S by inserting a whitewash after the i^{th} action for some $1 \leq i \leq n$. Then, $R(S) > R(S')$.

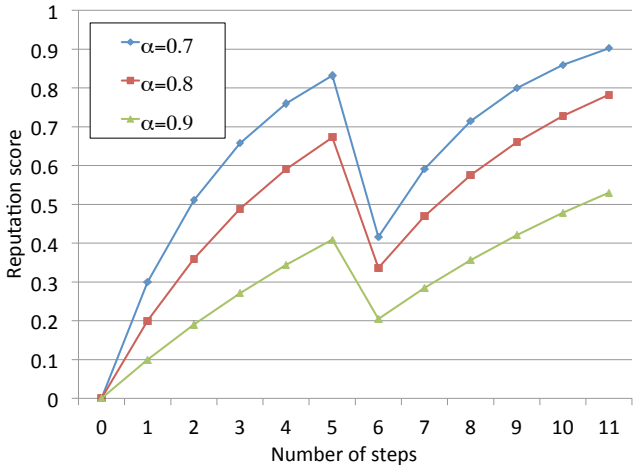
Proof: Suppose that a whitewash is inserted after the i^{th} action, i.e., it divides S into two parts $S_1 = a_1, a_2, \ldots, a_i$ and $S_2 = a_{i+1}, \ldots, a_n$. Since a whitewash initializes the reputation score, $R(S') = R(S_2)$. By the second condition described above, since it is assumed that S_1 contains at least one collaborative action, $R(S_1) > R_0$. By the definition of update rules, as the initial score R_0 increases, the resultant score monotonically glows. Hence the claim follows. ■

The badness of whitewash with respect to the reputation score is illustrated in Figure 2.

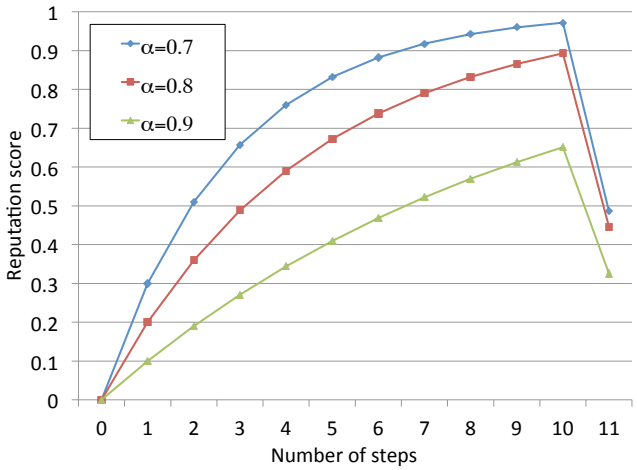
5. Extension

5.1 Motivation

In the above scheme, each peer who conducted an adversarial action is penalized by "uniformly" reducing the reputation score to $1/\beta$. Although it certainly penalizes adversarial actions of malicious peers, those rules give a penalty exactly once. In other words, after reducing the reputation score, the system "allows" the peer and treats him as an honest peer in the succeeding rounds. Thus, it could not effectively work as a *deterrent for addicts* of adversarial actions of malicious peers particularly when they repeat a sequence of actions consisting of an adversarial action and few collaborative actions. For example, if $\alpha = 0.5$, $1/\beta = 0.6$, and $R_0 = 0$, by repeating three collaborative actions after the participation, the score of the peer becomes $1 - 0.5^3 = 0.875$, and by conducting an adversarial action at that time, the score reduces to $0.6 \times (1 - 0.5^3) = 0.525$, but it is slightly larger than the score after the first collaborative action. In other words, one penalty is weaker than two collaborative actions in this case. On the other hand, the penalty seems to be too strong for the peers which have repeated many collaborative actions. For example, if it repeats 1000 collaborative actions in the above example,



(a) Adversarial action at the sixth step.



(b) Adversarial action at the 11th step.

Figure 3: Difference of the impact of adversarial actions to the reputation score.

the penalty for (only) one adversarial action is heavier than 998 collaborative actions. Figure 3 shows the change of the reputation score according to the difference of the position of an adversarial action in a sequence of collaborative actions, assuming $R_0 = 0$ and $1/\beta = 0.5$. When an adversarial action occurs at the sixth step, it "cancels" three or four collaborative actions conducted before it (Figure 3 (a)). However, if it occurs at the 11th step, it cancels 6 steps for $\alpha = 0.9$ and 8 steps for $\alpha = 0.7$ (Figure 3 (b)), which is larger than the case of the sixth step.

Such an unbalance on the number of consecutive collaborative actions which are comparable to one adversarial action should be overcome by reducing β as small as possible (i.e., the difference becomes small by decreasing β), and by introducing an additional mechanism for the penalization. The time transition of the reputation score for different β's is illustrated in Figure 4. It could be observed that the reduction

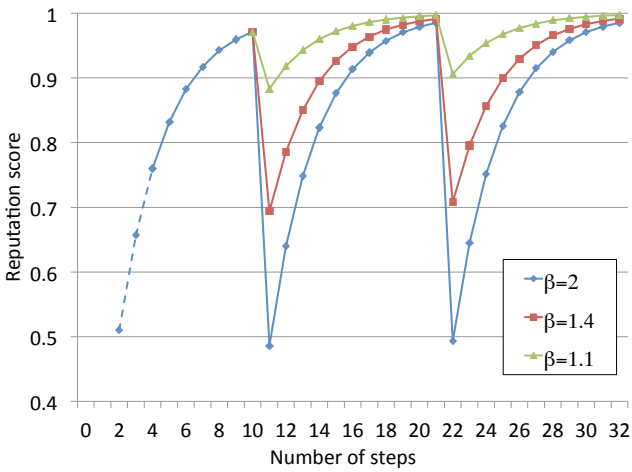


Figure 4: Time transition of the reputation score for different β ($\alpha = 0.7$ and $R_0 = 0$).

of the score significantly decreases as β approaches to one.

5.2 Scheme

Our main idea for the improvement of the basic scheme is to reduce the amount of increase of the reputation score during n consecutive rounds after detecting an adversarial action, where n is a parameter determined later. More concretely, we use the following rule instead of Equation (1) during n consecutive rounds after encountering an adversarial action:

$$R_i \ := \ \gamma R_i + (1 - \gamma) \tag{3}$$

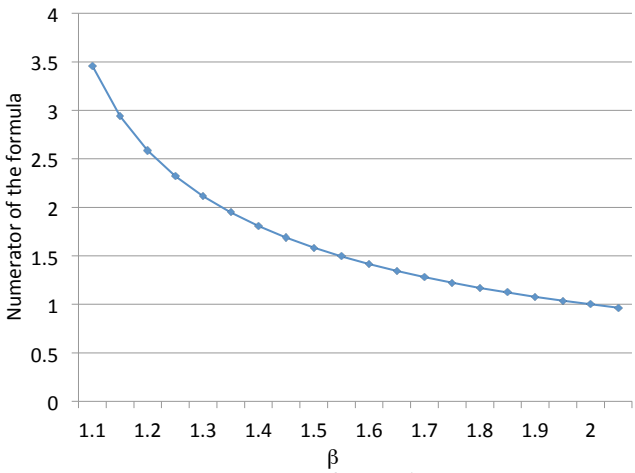
for some $\gamma > \alpha$. The reader should note that if n is too small, it does not effectively frighten peers to conduct adversarial actions, whereas if n is too large, it will encourage adversarial peers to conduct a whitewash. Thus an appropriate value of parameter n should be calculated carefully, which should depend on parameters α, β, γ, and the value of R_i at the time of encountering an adversarial action.

5.3 Analysis

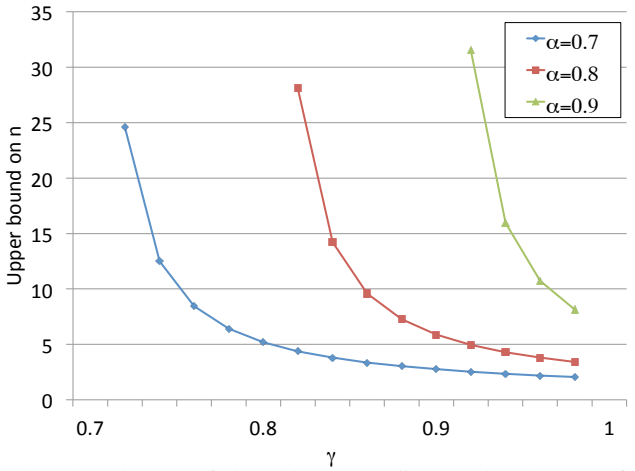
In this section, we derive an upper bound on parameter n in the sense that if it exceeds the value, it works as an incentive to conduct a whitewash. Recall that $R(S)$ denotes the reputation score after conducting an action sequence S which is represented by a ternary string in such a way that 0 and 1 indicate collaborative and adversarial actions respectively, and 2 indicates whitewash.

The following claim is easy to prove since the effect of whitewash will be maximized if it is conducted immediately after an adversarial action.

Remark 2: Let $S = a_0, a_1, a_2, \ldots, a_n$ be a sequence of actions such that $a_0 = 1$ and $a_i = 0$ for $1 \leq i \leq n$, S' be a sequence of length $n + 2$ which is obtained from S by "inserting" a whitewash at the second position. Note that in



(a) Numerator of Equation (4).



(b) The change of the value according to the change of parameters α and γ ($\beta = 2$).

Figure 5: Upper bound on n.

sequence S, n consecutive actions are penalized by reducing the increase of the reputation score. Then, the extended scheme does not encourage whitewash if $R(S) > R(S')$.

Let x be the score before conducting action sequence S. Then, we have

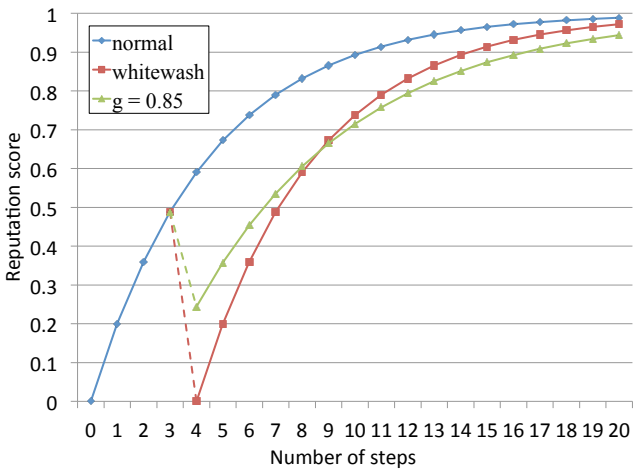
$$R(S) \ = \ \gamma^n \times \left(\frac{x - R_0}{\beta} + R_0 \right) + 1 - \gamma^n$$

and

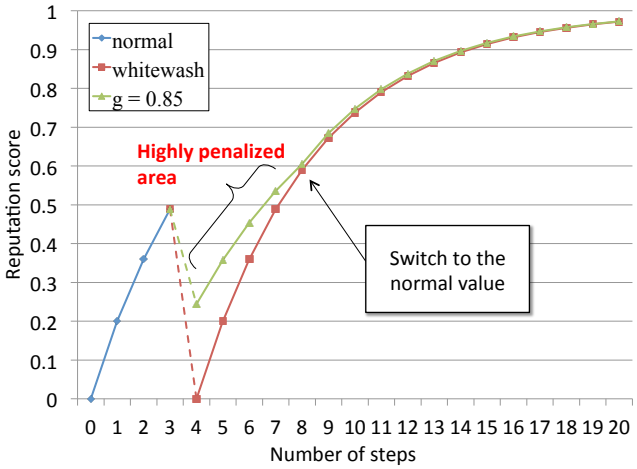
$$R(S') \ = \ \alpha^n \times R_0 + 1 - \alpha^n$$

Thus, in order to satisfy $R(S) > R(S')$, we should have

$$\gamma^n \times \left(\frac{x - R_0}{\beta} + R_0 - 1 \right) \ > \ \alpha^n \times (R_0 - 1)$$



(a) When it does not switch to Rule (1).



(b) When it switches to Rule (1) after four times of repetitions.

Figure 6: The role of parameter n.

that is,

$$\left(\frac{\alpha}{\gamma}\right)^n > \frac{1 - R_0 - \frac{x - R_0}{\beta}}{1 - R_0} = 1 - \frac{x - R_0}{\beta(1 - R_0)} > 1 - \frac{1}{\beta}$$

where the last inequality is due to $x < 1$. By taking a logarithm, we have

$$n \log(\alpha/\gamma) > \log(1 - 1/\beta)$$

Since $\alpha < \gamma$, $\log(\alpha/\gamma) < 0$. Thus,

$$n < \frac{\log \beta - \log(\beta - 1)}{\log \gamma - \log \alpha}. \quad (4)$$

The numerator of Equation (4) gradually decreases as β increases, as is shown in Figure 5 (a). In addition, for a fixed α, the right hand side of the formula decreases as γ increases from α, as is shown in Figure 5 (b) (in this figure, we fix β to two). By this figure, we can see that we could apply Rule (3) at most six times if parameters are determined as $\alpha = 0.7$, $\beta = 2$, and $\gamma = 0.78$, but it decreases to four times if we slightly increase γ to 0.82.

An example of the time transition of the reputation score is illustrated in Figure 6. This figure assumes $\alpha = 0.7$, $\beta = 2$, and $\gamma = 0.85$. If we apply Rule (3) instead of Rule (1) forever, as is shown in Figure 6 (a), the score after whitewash eventually becomes larger than the penalized score. However, by switching the rule to Rule (1) after passing an appropriate number of repetitions (e.g., in this example, by switching the rule after three times of applications), we can guarantee that the resulting score is still greater than the score after whitewash, as in shown in Figure 6 (b).

6. Schemes

In this section, we propose several reputation management schemes based on the extended update rules.

6.1 Threshold Type

The first idea is to switch the rule from Rule (3) to Rule (1) by the value of the reputation score. More concretely, it switches the rule when: 1) it encounters the upper bound on n, or 2) the reputation score exceeds a predetermined threshold (e.g., 0.8). This scheme is intended to "allow" users when their reputation score exceeds the threshold, since the fact of exceeding the threshold indicates that it has repeated sufficient number of collaborative actions. In fact, since the score after applying Rule (2) is at most $1/\beta$, to reach threshold θ ($> 1/\beta$), it should repeat at least m collaborative actions satisfying the following inequality:

$$\theta < \gamma^m(1/\beta) + 1 - \gamma^m.$$

By solving it, we have the following lower bound on m,

$$m > \frac{\log(1 - \theta) - \log(1 - 1/\beta)}{\log \gamma}.$$

6.2 Counting Type

The second idea is to (gradually) increase the number of repetitions depending on the number of adversarial actions which have been conducted by the corresponding peer. More concretely, the scheme works as follows: 1) Prepare a variable w to count the number of adversarial actions conducted by the peer. Variable w is initialized to zero and is incremented when it conducted an adversarial action. 2) The number of penalizations (i.e., the number of applications of Rule (3)) is determined as

$$\min\{f(w), n^*\}$$

where f is an appropriate monotonically increasing function such as $f(w) = w$ and $f(w) = w^2$, and n^* is an upper bound on n determined by Equation (4).

6.3 Random Type

The third scheme uses the notion of randomization. In the last two schemes, each peer can predict the strength of penalization from the outcome of past trials. For example, in the first scheme, a malicious peer knows that the penalization finishes after reaching its score to the threshold, and in the second scheme, a malicious peer knows from its experience that the strength of penalization against its next adversarial action. To effectively hide such information from malicious peers, a randomization could be used in the following manner: 1) After detecting an adversarial action of a peer, the central manager selects a random number r from set $\{1, 2, \ldots, n^*\}$. 2) It then penalizes during r consecutive rounds after reducing the score of the corresponding peer by Rule (2).

7. Concluding Remarks

In this paper, we propose new schemes for the reputation management in P2P applications which discourages whitewash while encouraging good behaviors. Our proposed scheme can control the strength of penalty against adversarial actions.

Topics for our future work are listed as follows:

- The evaluation of the proposed schemes considering the incentive of users to participate in the system. In actual P2Ps, each user reserves a right to leave from the system if she feels that it is not attractive compared with the required cost. Our current analysis misses such an issue.
- Combination with other techniques to discourage whitewash. For example, by combining the proposed schemes with Adrian and Marco's scheme described in Section 2, we could reduce the number of whitewashes in actual P2P environments.
- Detailed analysis of the fairness in the proposed schemes. We need to give a formal definition of fairness, as well as the tuning of several parameters to meet the fairness criteria.

Acknowledgements

This work was supported in part by the Scientific Grant-in-Aid from Ministry of Education, Science, Sports and Culture of Japan and the Telecommunications Advancement Foundation.

References

[1] J. Chen, H. Lu, and S. D. Bruda. "A Solution for Whitewashing in P2P Systems Based on Observation Preorder." *Proc. of International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC '09)*, pp.547–550, 2009.

[2] C. Costa and J. Almeida. "Reputation Systems for Fighting Pollution in Peer-to-Peer File Sharing Systems." *Proc. of the 7th IEEE International Conference on Peer-to-Peer Computing (P2P 2007)*, pp.53–60, 2007.

[3] Y.-M. Liu, S.-B. Yang, L.-T. Guo, W.-M. Chen, and L.M. Guo. "A Distributed Trust-based Reputation Model in P2P System." *Proc. of the 8h ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, pp.294–299, 2007.

[4] Y. Liu, W. Xue; K. Li, Z. Chi, G. Min, and W. Qu. "DHTrust: A Robust and Distributed Reputation System for Trusted Peer-to-Peer Networks." *Proc. of GLOBECOM 2010*, pp.1–6, 2010.

[5] S. Marti and H. Garcia-Molina. "Limited reputation sharing in P2P systems." *Proc. of the 5th ACM Conference on Electronic Commerce (EC '04)*, pp.91–101, 2004.

[6] Z. Malik and A. Bouguettaya. "Reputation Bootstrapping for Trust Establishment among Web Services." *Internet Computing, IEEE* , IEEE, 13(1): 40–47, 2009.

[7] A. P. de Pinninck, W. M. Schorlemmer, C. Sierra, and S. Cranefield. "A social-network defence against whitewashing." *Proc. of the 9th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2010)*, pp.1563–1564, 2010.

[8] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker. "A scalable content-addressable network." *Proc. of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp.161–172, 2001.

[9] I. Reitzenstein and R. Peters. "Assessing Robustness of Reputation Systems Regarding Interdependent Manipulations." *E-Commerce and Web Technologies*, Lecture Notes in Computer Science, 2009, Vol. 5692, pp.288–299, 2009.

[10] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan. "Chord: A scalable peer-to-peer lookup service for internet applications." *ACM SIGCOMM Computer Communication Review*, 31(4): 149–160, 2001.

[11] Y.-M. Tseng and F.-G. Chen. "A free-rider aware reputation system for peer-to-peer file-sharing networks." *Expert Syst. Appl.*, 38(3): 2432–2440. 2011.

[12] Z. Xu, Y. He, and L. Deng. "A Multilevel Reputation System for Peer-to-Peer Networks." *Proc. of the 6th International Conference on Grid and Cooperative Computing (GCC 2007)*, pp.67–74, 2007.

[13] M. Yang, Y. Dai, and X. Li. "Bring Reputation System to Social Network in the Maze P2P File-Sharing System." *Proc. of the International Symposium on Collaborative Technologies and Systems (CTS 2006)*, pp.393–400, 2006.

[14] Y. Zhang and Y. Fang. "A Fine-Grained Reputation System for Reliable Service Selection in Peer-to-Peer Networks." *IEEE Transactions on Parallel and Distributed Systems*, 18(8): 1134–1145, 2007.

[15] B. Y. Zhao, J. D. Kubiatowicz, and A. D. Joseph. "Tapestry: An Infrastructure for Fault-tolerant Wide-area Location and Routing." *Technical Report*, CSD-01-1141. University of California at Berkeley, 2001.