A Game Theoretical Approach in Securing P2P Storage against Whitewashers

Nouha Oualha and Yves Roudier

EURECOM, Sophia Antipolis France
{oualha, roudier}@eurecom.fr

***Abstract*—An inherent problem to a cooperation incentive mechanism implemented into a dynamic system where peers may join or leave at any time is the whitewashing problem. Whitewashers are peers that repeatedly misbehave, leave the storage system and rejoin with new identities thus escaping punishment imposed by the incentive mechanism. In order to deal with such whitewashers, the paper presents a penalty mechanism against strangers and it describes as well a theoretical game that models such mechanism and attempts to capture the point of tradeoff between restricting whitewashers and encouraging newcomers to participate into the system.**

***Index Terms*—Cooperation, P2P storage, game theory, whitewashing**

I. Introduction

P2P storage systems and algorithms have recently received a lot of interest, due particularly to the popularity of file sharing applications. In such systems, peers make use of untapped storage resources: they provide local storage space for other peers' data; in counterpart they acquire remote storage space for their personal data. Cooperation incentive mechanisms stimulate resource contributions which constitute the main premise for the well operation of P2P systems. Cooperation incentive mechanisms fall into two branches: remuneration approaches that provide virtual or real payment-based incentives for cooperative peers and reputation approaches that establish and maintain a reputation index for every peer in the network. In spite of these mechanisms, the fairness of peer contributions is not always guaranteed, for instance peers may whitewash i.e., they may not cooperate and then reconnect to the system with a fresh new identity to get rid of a negative reputation rating or to take profit from initial credit offered to newcomers in order to bootstrap the system. The whitewashing problem is essentially due to the presence of free or cheap pseudonyms for peers. Therefore, countering the whitewashing attacks demands either the use of irreplaceable pseudonyms e.g., through the assignment of strong identities by a central trusted authority, or requires imposing a penalty on all newcomers. The first solution reduces the decentralized nature of P2P systems and introduces a single point of failure. The second left option requires defining the just penalty parameter for the system. In this paper, we propose an evolutionary game theoretical model of the P2P storage system that relies on the penalty mechanism. The model allows capturing the features of the penalty mechanism with respect to its impact on discouraging whitewashing and the measure of its associated social welfare within the P2P storage system.

II. Problem Statement

In a P2P storage system, peers are able to store their data at several peers, called *holders*, within the P2P network; in counterpart they should contribute to the storage community by providing spare disk space for other peers. The availability and integrity of the stored data is periodically checked by some peers, named *verifiers*, appointed by the data *owner*.

A. P2P storage overview

Interactions that occur between participating peers to one data storage consist of several phases:

- *Storage phase:* the owner stores data at r holders.
- *Delegation phase:* the owner sends verification information to m verifiers in order to be able to periodically check data at holders.
- *Verification phase:* each verifier performs periodic checking of storage integrity and availability at its assigned holder using a remote data possession verification protocol (like [11]). Based on the result of such checking, the verifier decides whether the holder is cooperative or not. If the verifier detects storage default or corruption, the verifier has the requirement to notify the owner about it.
- *Retrieval phase:* the owner retrieves its data from the r holders.

B. Whitewashing problem

The proposed P2P storage system relies first and foremost on holder and verifier cooperation to properly function. Therefore, it may be exposed to several attacks due to peer misbehavior such as data destruction or corruption or even collusion between peers. Peer collusion can be mitigated through proper selection of data holders and verifiers. For instance, the random selection of peers within a structured P2P system limits pre-set collusions among these peers (for details refer to [1]). On the other hand, peer participation and data preservation can be stimulated thanks to the use of cooperation incentive mechanisms.

Still, such mechanisms are vulnerable to whitewashers that repeatedly leave the storage system and rejoin with new identities thus escaping any punishment caused by their previous misbehavior. With new identities, peers have a clean record: good reputation rating or a default initial amount of credits without debts to pay.

Particularly in a so open and dynamic P2P system where peers are able to freely join, disconnect, reconnect, and leave the system, whitewashing becomes an eminent attack. Such attack undermines the operation of the cooperation incentive mechanism since whitewashers are not motivated to cooperate because otherwise they are not punished and they are eventually cutting down the utilization of their storage resources: they consume but do not contribute. Without peer cooperation, the system may collapse in the tragedy of the commons [12].

C. *Penalty over strangers*

There are several solutions to the whitewashing problem. The first approach relies on a central trusted authority that assigns strong identities to peers (linked to real-world identities). Alternatively, the authority may impose the payment of membership fees. However, additionally to introducing a single point of failure, such approach reduces the decentralized nature of P2P systems.

Without a trusted third party, another option is to impose penalties on all newcomers: an insider peer may only probabilistically cooperate with newcomers (like in BitTorrent [2]), or peers may join the system only if an insider peer with limited invitation tickets invites them [3]. This option seems to be detrimental to the scalability of the system; it has even been shown that this degrades the total social welfare [4] because whitewashing behavior is not observable and thus the penalty affects all newcomers either cooperative ones or whitewashers.

Our paper studies the latter solution. The countering measure against whitewashing consists of a penalty mechanism. The imposed penalty is performed by each peer that does not cooperate with strangers with probability 1-p. The penalty may be also represented as service degradation by (1-p)-fraction imposed on each newcomer. The probabilistic strategy attempts to reach a point of tradeoff between restricting whitewashers and encouraging newcomers to join and participate into the system.

In the proposed P2P storage system, the penalty mechanism corresponds to making each peer accept to store or verify a newcomer's data only with some given probability p.

III. Evolutionary Game Model

In this section, some approaches inciting resource sharing and applying game theoretical models that we deem to be interesting are reviewed. Then, the game theoretical model of the P2P storage system with the penalty mechanism is described.

A. *Related work*

To achieve a socially optimal equilibrium for a self-organizing system with autonomous peers, different incentive mechanisms have been proposed in the literature.

[6] proposed a general and generic game theoretical framework to model and analyze cooperation incentive policies. The model studies the game dynamics where strategies change according to two learning models: the current-best (CBLM) and the opportunistic (OLM) learning models. In CBLM, each peer chooses the strategy that has the highest payoff. In the second learning model OLM, each peer randomly chooses another peer as its *teacher*. If the teacher has a better payoff than the peer, the latter adapts to the teacher's strategy. OLM is similar to evolutionary game concepts where the so-called teacher is the co-player of the peer. The main parameter of comparison between these learning models is robustness: a system is robust if it stays at a high contribution level even with perturbation such as peer arrivals or departures from the network. The mathematical analysis demonstrates that a system with CBLM is less robust than with OLM; this latter being alike a typical evolutionary game model. Moreover, the analysis allows comparing two incentive policies: the mirror incentive policy under which a peer provides service with the same probability as the requester serves other peers in the system, and the proportional incentive policy whereby the peer serves the requester with a probability equal to the requester's contribution to consumption ratio. The study shows that the mirror incentive policy may lead to a complete system collapse, while the proportional incentive policy can lead to a robust system. This result is quiet interesting because it demonstrates that a policy motivating fairness in terms of contributions and consumptions of resources achieves better stability than participatory incentives.

[7] opted also for an evolutionary study of applications in P2P systems. The authors proposed a model that they called a generalized form of the Evolutionary Prisoner's Dilemma (EPD). Though the model is very similar to the traditional EPD, they argued that the new model permits asymmetric transactions between a client peer and a server peer. Peers decide to cooperate or not based on a reciprocative decision function that sets the probability to cooperate with a given peer X to the ratio , rounded to a value in [0, 1], (cooperation X gave)/(cooperation X received), such function is comparable to the proportional incentive policy in [6]. The authors simulated EPD under various situations and obtained several results. They showed that techniques relying only on private history, where solely peer experiences are taken into account, fail in inciting cooperation among peers as the population size increases. However, techniques based on shared history better scales to large populations. Additionally, results demonstrate that cooperation with strangers fails to encourage cooperation in the presence of whitewashers. Therefore, the authors proposed an adaptive policy in which the probability of cooperation with strangers becomes equal at time t+1 to $p_C^{t+1} = (1-\mu)\times p_C^{t} + \mu\times C_t$, where C_t=1 if the last stranger cooperated and =0 otherwise. Simulations validate the adaptive policy by demonstrating that incentives based on such policy make the system converge to higher levels of cooperation.

[4] have studied in more depth the whitewashing problem in P2P systems using a game theoretical model that particularly takes into account heterogeneity of users' behavior. In order to sustain the system when the societal generosity is low, punishment mechanisms against free-riding users are required. The proposed punishment mechanism consists on imposing a penalty on free-riding behavior with probability (1-p). The optimal value for the probability p is defined by the maximum

obtained performance of the system. Still, such mechanism can be undermined by the availability of cheap pseudonyms through which a free-rider may choose to whitewash. To measure the effect of whitewashing behavior, the authors computed system performance considering the cases of permanent identities and free identities, in addition to different turnover rates that represent user arrival and departure rates (arrivals and departures are assumed *type-neutral* i.e., they do not alter the type distribution). Their study demonstrates that the penalty mechanism is effective when both the societal generosity and the turnover rate are low; otherwise a notable societal cost due to whitewashing is experienced (we will also come to such result in our study of an evolutionary game model of the audit-based incentives).

In the remainder of this paper we will present a game theoretical model describing the features of a P2P storage system and capturing the whitewashing problem in such system. We endeavor with such model to discuss the ability of the strategy based on the probabilistic cooperation with strangers in coping with whitewashers.

B. Model

We model the storage system as an evolutionary game. Evolutionary game theory provides a dynamic framework for analyzing repeated interactions. In such games, randomly chosen players interact with each other, and then the player with the lower payoff switches to the strategy of the player with the higher payoff i.e., players reproduce proportionally to their payoffs. Hence, strategies with poor payoffs eventually die off, while well-performing strategies thrive.

In the proposed system, an owner stores data replicas at r holders. It appoints m verifiers for its data replica that will periodically check storage at holders.

Our proposed evolutionary game is similar to the game in [8] where players have either the role of the donor or the role of the recipient. The donor can confer a benefit b to the recipient, at a cost $-c$ to the donor.

We consider three roles in our game: owner, holder, and verifier; any peer may play several of these roles throughout the game (in uniform random selection).

- Role of the owner: store data at r holders and delegate their verification to m verifiers. The owner receives verification results from verifiers and may then appropriately react to data destruction (by re-replicating its data elsewhere for instance). Additionally, the owner may update its belief (i.e., reputation) about the behavior of the concerned holder (considering this later as cooperative or defector, discussed later on).
- Role of the holder: keep data stored or destroy them (depending on its strategy), and also respond to challenges conducted by the verifiers.
- Role of the verifier: periodically check storage at the holders assigned to it. Whenever the verifier detects the destruction or corruption of some data at a holder, it then notifies the owner. It further updates its own belief about this holder.

One-stage game

The one-stage game represents an interaction between one data owner, r data holders, and m verifiers randomly chosen. In a one-stage game, the owner is considered a recipient, the r holders and m verifiers are donors. The owner gains b if at least one holder donates at a cost $-c$; however if no holder donates then the owner gains βb if at least one verifier donates at a cost $-\alpha c$ ($\alpha \leq 1$) for each verifier. The latter case corresponds to the situation where the cooperative verifier informs the owner of the data destruction, and then the owner may replicate its data elsewhere in the network thus maintaining the security of its data storage.

Donors which are either holders or verifiers have the choice between cooperating, which we call interchangeably donate, or defecting:

- Cooperation whereby the peer is expected to keep others' data in its memory and to verify data held by other peers on behalf of the owner.
- Defection whereby the peer destroys the data it has accepted to hold, and also does not verify others' data as it promised to.

Storage of data and their verification are two dependant actions. Peers with some determined behavior take these two actions as falling under the same objective: either to cooperate or to shirk.

With the periodic verification, the owner can infer the behavior of the holder, but not that of the verifier. Verifiers are not more trusted than other peers and may lie about verification, for instance reporting an absence of response to a challenge for a cooperative holder. However, a non-cooperative verifier may mimic a cooperative strategy by sending a bogus result. The owner therefore cannot determine with certainty whether a verifier chose to adopt a cooperative strategy.

Some verifiers may also crash or leave the system, and be unable to communicate results of verifications. However, we will not deal with this problem in the following study; we rather rely on the distribution of the verification task to multiple verifiers to mitigate the non cooperation or failure of verifiers.

One negative result from a verifier is not enough for the owner to decide that the holder is non cooperative. Such a notification may however be used as a warning that the holder may have destroyed its data. Based on such a warning, the owner would replicate the endangered data, therefore maintaining or even increasing storage reliability to his advantage.

Strategies

Our study considers two types of strategies: the peers that follow the desired behavior in the P2P storage system and particularly use the penalty mechanism to deal with strangers, and the peers that defect and whitewash.

Discriminators are peers that adhere to the following strategy (corresponding to the audit-based strategy in [1]):

- Discriminate and probabilistically cooperate with strangers (D^p): the discriminator donates under conditions: it donates with probability p with a stranger and probability 1 with a peer that previously donated. A discriminator may know that a peer has donated in a previous game in the case where that peer was a holder and the discriminator was its verifier or the owner of the data that the peer was storing.

Defectors are peers that not only defect but also probabilistically whitewash to cover up their defection:

- Always defect and probabilistically whitewash ($AllD^w$): the peer never donates in the role of the donor and may be a whitewasher with probability w so that it is not identified by a discriminator. The value w may represent the average rate (per generation) at which defectors change identities.

Fitness

We respectively denote the frequency (fitness) of strategies $AllD^w$ by y and D^p by z. The expected values for the total payoff obtained by the two strategies are denoted by U_{AllD^w} and U_{D^p}, and the average payoff in the population by:

$$\overline{U} = y \times U_{ALLD^w} + z \times U_{D^p}$$

To simplify the formulation of the fitness for each strategy, we will use the following functions:

$$f(u) = -c(r + m\alpha) \times u$$
$$g(u) = b(1 - u^r + \beta u^r(1 - u^m))$$

The function $f(u)$ gives the cost paid by a peer for storing and verifying data for a fraction u of peers. On the other hand, the function $g(u)$ gives the benefit obtained if a fraction u of peers defect as holders and as verifiers of the peer's data.

Let q be the probability that the discriminator knows what a randomly chosen co-player chose as a holder strategy in a previous one-stage game (the discriminator being an owner or verifier in that game). The probability q is computed in [9]. This probability particularly depends on the system churn that is the peer join rate λ and interaction rate between peers σ. The probability q at time t is derived as (see [9] for formulation details):

$$q(t) = \frac{\sigma}{\sigma + \lambda}(1 - e^{-(\sigma+\lambda)t})$$

A peer playing the strategy $AllD^w$ will never cooperate, so it will never donate. It will gain a benefit b if it is chosen as an owner and at least one of its data holders is not any of these types: a defector or a discriminator that knows the peer or that probabilistically defects because either it does not know the peer or the peer itself is a whitewasher. Otherwise, the peer may gain a benefit βb if at least one of its verifiers is not of any of the former two types.

$$\begin{aligned} U_{ALLD^w} &= g\big(y + q(1 - w)z \\ &\quad + \big(w + (1 - q)(1 - w)\big)(1 - p)z\big) \\ &= g(1 - p(1 - q(1 - w))z) \end{aligned}$$

A peer playing the strategy D^p will cooperate if the recipient was cooperative in a previous interaction or will probabilistically cooperate if it does not know the latter. It will donate at a cost $-c$ if it is chosen as a holder or at a cost $-\alpha c$ if it is chosen as a verifier. It will gain a benefit b if it is chosen as an owner and at least one of its data holders is not a defector or a discriminator that the peer previously defects with it (the peer defects with a fraction p of discriminators that it does not know), otherwise, it may gain a benefit βb if at least one of its verifiers is not a defector or again a discriminator that the peer previously defects with it.

$$\begin{aligned} U_{D^p} &= f\left(p\left((1 - q)\big((1 - w)y + z\big) + wy\right) + qpz\right) \\ &\quad + g(y + (1 - p)z) \\ &= f\big(p(1 - q(1 - w)(1 - z))\big) + g(1 - pz) \end{aligned}$$

The dynamics of strategies' fitness follow the differential replicator equations defined below:

$$\frac{dy}{dt} = y(U_{AllD^w} - \overline{U})$$
$$\frac{dz}{dt} = z(U_{D^p} - \overline{U})$$

The basic concept of replicator dynamics is that the growth rate of peers taking a strategy is proportional to the fitness acquired by the strategy. Thus, the strategy that yields more fitness than average fitness of the whole system increases, and vice versa.

IV. Simulation Experiments

This section analyses the results of the study of the evolutionary game model. Using the above differential equations, the model is simulated within several scenarios to capture the impact of various parameters on the convergence of the system to equilibrium.

We consider files with an average size of 500MB that are stored at a rate of 3 files per day and per peer. The verification metadata corresponding to each file has an average size of 10KB. Newcomers to the storage system arrive at a rate of 10 peers per month. These newcomers are assumed detaining the same strategy as their hosts.

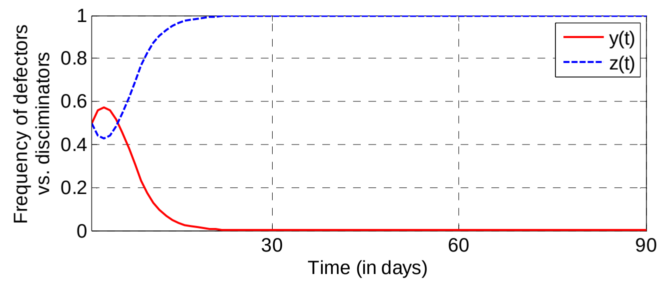


Fig. 1. Frequency of defectors and discriminators. m=5, r=3, β=0.1, α=20.10^{-6}, λ=10/month, N=1000, γ=3 files/day, b=1, c=0.01, p=w=0.5, $y(0)$=0.5, and $z(0)$=0.5.

Fig. 1 shows the convergence of the storage of the system to an equilibrium where only discriminators are active. Defectors are totally eliminated by discriminators.

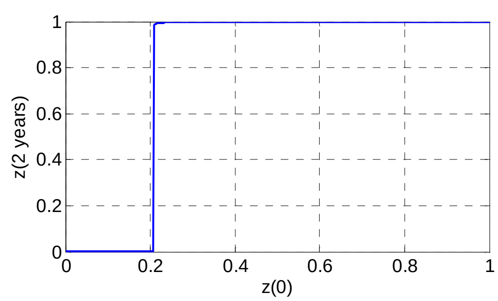


Fig. 2. Frequency of discriminators at equilibrium varying their initial frequency. m=5, r=3, β=0.1, α=20.10^{-6}, λ=10/month, N=1000, γ=3 files/day, b=1, c=0.01, p=w=0.5.

There is a little increase in the population of defectors in the beginning of the evolutionary game due to the fact that discriminators are still not able to distinguish between a discriminator and a defector. However, with time they have a good knowledge of discriminators (fraction p of them) and defectors (fraction (1-w) of them).

Fig. 2 depicts the frequency of discriminators at equilibrium varying their initial frequency. The figure demonstrates that the equilibrium where only discriminators are present in the system is only achieved if there is enough population of discriminators in the system. Otherwise, the defectors win the game by eliminating discriminators.

The equilibrium where only discriminators are active depends also on the probability of cooperation of discriminators with strangers. Fig. 3 demonstrates that if this probability is sufficiently high, the frequency of discriminators decreases and may attain zero.

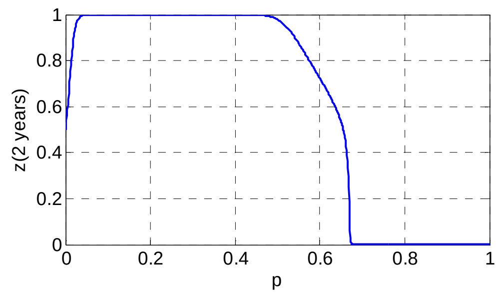


Fig. 3. Frequency of discriminators at equilibrium varying their probability of cooperation with strangers *p*. *m*=5, *r*=3, β=0.1, α=20.10^{-6}, λ=10/month, *N*=1000, γ=3 files/day, *b*=1, *c*=0.01, *w*=0.5, *y*(0)=0.5, and *z*(0)=0.5.

Varying the probability of whitewashing *w* in the system affects also the frequency of discriminators at equilibrium (see Fig. 4). For sufficiently high *w*, defectors invade the population of discriminators and win the game. For instance, if all defectors are whitewashers, discriminators are eliminated from the game.

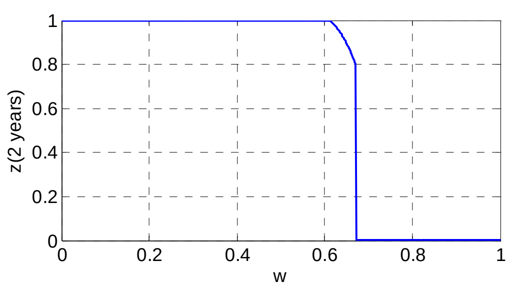
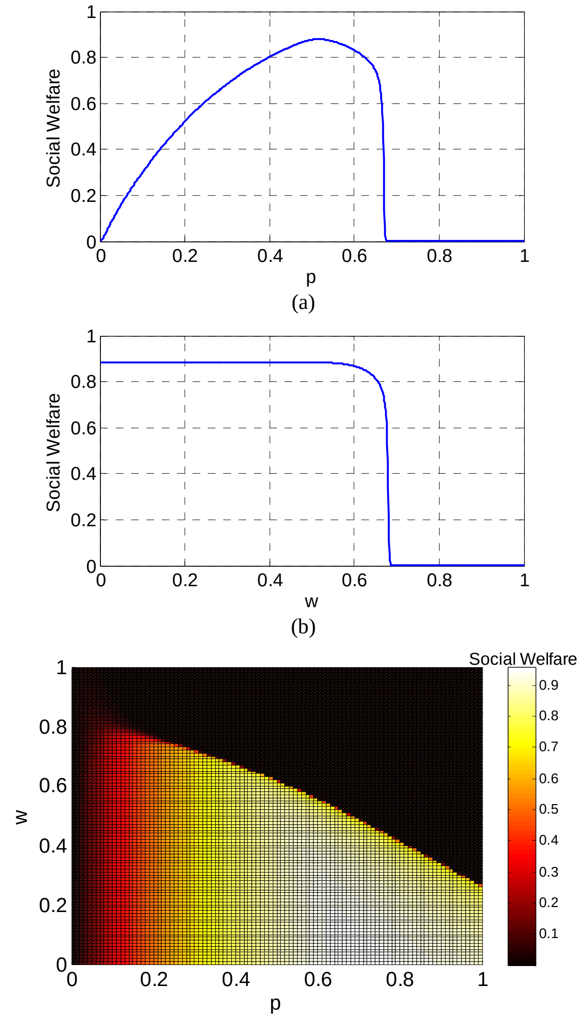


Fig. 4. Frequency of discriminators at equilibrium varying the probability of whitewashing *w*. *m*=5, *r*=3, β=0.1, α=20.10^{-6}, λ=10/month, *N*=1000, γ=3 files/day, *b*=1, *c*=0.01, *p*=0.5, *y*(0)=0.5, and *z*(0)=0.5.

The social welfare illustrates the well-being of the community of peers as a whole. It is derived as the total sum of player payoffs.

Fig. 5 shows that this welfare is maximized for a defined value of the probability of cooperation of discriminators with strangers *p* (0.5<*p*<0.9) and if the discriminators are not eliminated from the system (probability of whitewashing *w* <0.7).

Discriminators are the only contributors to the game therefore their presence increases the payoff of peers. Their cooperation may be undermined by the presence of defectors that use the system without contributing and particularly whitewashers that defect and go without being detected by the discriminators. Increasing *p*, it certainly increases the benefit for all peers but at the same time it increases the cost due to the presence of defectors. Fig. 5.c demonstrates that there is an optimal value for *p* that achieves the highest social welfare and this optimal depends on *w*.



(c)

Fig. 5. Social welfare at equilibrium varying (a) the probability of cooperation *p* (*w*=0.5), (b) probability of whitewashing *w* (*p*=0.5), and (c) both of them. *m*=5, *r*=3, β=0.1, α=20.10^{-6}, λ=10/month, *N*=1000, γ=3 files/day, *b*=1, *c*=0.01, *y*(0)=0.5, and *z*(0)=0.5.

Fig. 6 depicts the variation of the social welfare with the replication rate *r* and the verification distribution factor *m*. The figure shows that there is an optimal value for the replication rate *r* for which the social welfare is maximized (*r*~4). Exceeding this value, the social welfare decreases until reaching the value zero i.e., the system collapses. Increasing *r* makes the benefit obtained by the owner increase since the chances to select a cooperative holder are improved; however the replication rate *r* affects also the cost of cooperation that is solely paid by discriminators.

Varying *m* has less impact on the social welfare because the cost charged on discriminators is minimized by the significantly low unit cost value αc (α=20.10^{-6}). The social welfare increases by increasing *m* (small increase) since a high value of *m* means better chances to have a verifier that is discriminator and then gain a benefit βb if all holders are defectors.

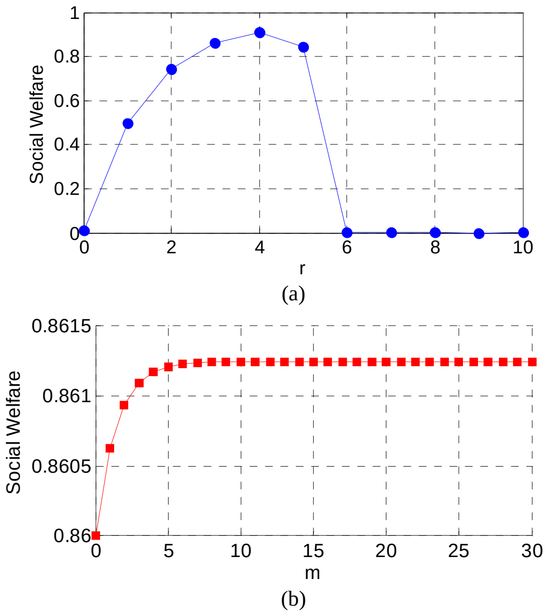


Fig. 6. Social welfare at equilibrium varying (a) replication rate r (m=5) and (b) verification distribution factor m (r=3). β=0.1, α=20.10^{-6}, λ=10/month, N=1000, γ=3 files/day, b=1, c=0.01, p=w=0.5, y(0)=0.5, and z(0)=0.5.

Fig. 7 demonstrates that there is a maximum value for tolerable churn. If peers arrive in the system at a high rate, discriminators may not be able to distinguish sufficiently quickly defectors and they may then be eliminated from the system. Churn can be tolerated until a given rate identified in the figure (λ~0.09) for the considered system parameters.

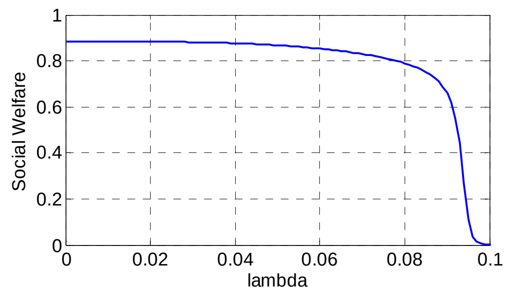


Fig. 7. Social welfare at equilibrium varying the churn λ. m=5, r=3, β=0.1, α=20.10^{-6}, N=1000, γ=3 files/day, b=1, c=0.01, p=w=0.5, y(0)=0.5, and z(0)=0.5.

Discussion

Simulation results demonstrate that discriminators are not hopeless in front of defectors and that even they may win over them for a judicious choice of system parameters, notably the fraction of discriminators in the system should be initially not null, the replication rate and the churn sensed in the system should not be considerably high.

The results show also that there is an optimal probability p for the penalty mechanism that achieves a high social welfare for the whole P2P storage system. However, a non-zero welfare is only obtained if the whitewashing phenomena is restricted to a given fraction of defectors. For instance, if all defectors are whitewashing discriminators are entirely eliminated and the system collapses.

This result motivates the requirement to supplement the proposed penalty mechanism with other means that prevent or at least limit the whitewashing behavior such as controlling the peers that join the system using a cryptographic puzzle [10] or even imposing the payment of a membership fee. Another solution is to force or motivate peers to stay online a minimum amount of time in the system like in [13] (1/w is then increased) because peer connection time must be taken into consideration. As a result, if the average imposed peer time connection (1/w) is fixed, the probability of cooperation p that maximizes the social welfare can be then deduced (given other preset parameters like r, m, and λ).

V. Conclusion

In this paper, we validated a penalty mechanism designed to prevent whitewashing behavior in a P2P storage system. We theoretically demonstrate that with such mechanism, cooperative peers win over free-riders that may whitewash in an open system, although under particular conditions revealed in the paper as the basis for the P2P storage system.

References

[1] Nouha Oualha and Yves Roudier. Reputation and Audits for Self-Organizing Storage. In the 1st Workshop on Security in Opportunistic and SOCial Networks (SOSOC 2008), Istanbul, Turkey, September 2008.

[2] Michael Piatek, Tomas Isdal, Thomas Anderson, and Arvind Krishnamurthy. Do incentives build robustness in BitTorrent?. In Proceedings of the ACM/USENIX Fourth Symposium on Networked Systems Design and Implementation (NSDI 2007), 2007.

[3] François Lesueur, Ludovic Mé, and Valérie Viet Triem Tong. A Sybilproof Distributed Identity Management for P2P Networks In Proceedings of the 13th IEEE Symposium on Computers and Communications (ISCC) 2008, IEEE Computer Society, Marrakech, Morocco.

[4] Michal Feldman, Christos H. Papadimitriou, John Chuang, and Ion Stoica. Free-riding and whitewashing in peer-to-peer systems. IEEE Journal on Selected Areas in Communications 24(5): 1010-1019 (2006).

[5] Gary E Bolton and Axel Ockenfels. ERC: a theory of equity, reciprocity, and competition. American Economic Review 90(1): 166-193, 2000.

[6] Bridge Q. Zhao, John C. S. Lui, Dah-Ming Chiu. Analysis of Adaptive Protocols for P2P Networks. In IEEE INFOCOM 2009.

[7] Kevin Lai, Michal Feldman, Ion Stoica, and John Chuang. Incentives for Cooperation in Peer-to-Peer Networks. In Proceedings of the 1st Workshop on Economics of Peer-to-Peer Systems, UC Berkeley, Berkeley, California, USA, June 2003.

[8] Hannelore Brandt and Karl Sigmund. The good, the bad and the discriminator--errors in direct and indirect reciprocity. Journal of Theoretical Biology, Volume 239, Issue 2, 21 March 2006, Pages 183-194.

[9] Nouha Oualha and Yves Roudier. Evolutionary game for peer-to-peer storage audits. In the 3rd International Workshop on Self-Organizing Systems (IWSOS'08), December 10-12, Vienna, Austria.

[10] Vivek Vishnumurthy, Sangeeth Chandrakumar and Emin Gun Sirer. KARMA: A Secure Economic Framework for P2P Resource Sharing. In Proceedings of the Workshop on the Economics of Peer-to-Peer Systems, Berkeley, California, June 2003.

[11] Nouha Oualha, Melek Önen, and Yves Roudier, "A Security Protocol for Self-Organizing Data Storage", in Proceedings of 23rd International Information Security Conference (SEC 2008) IFIP Sec 2008, September 2008, Milan, Italy.

[12] Garrett Hardin, "The Tragedy of the Commons". Science, Vol. 162, No. 3859 (December 13, 1968), pp. 1243-1248.

[13] Wuala, the social online storage: http://www.wuala.com/