A Game Theoretic Analysis of Blacklisting in Online Data Storage Systems

Bader Ali
School of Computer Science
McGill University
Montreal, QC H3A 2A7, Canada
Email: bali2@cs.mcgill.ca

Muthucumaru Maheswaran
School of Computer Science
McGill University
Montreal, QC H3A 2A7, Canada
Email: maheswar@cs.mcgill.ca

***Abstract*—In this paper, we investigate the problem of online data sharing on social networks from a game theoretic framework. We introduce blacklisting as trigger strategy to elicit cooperation among the players of a noncooperative sharing game. Using game theoretic analysis, we show the existence of an equilibrium in which the sharing conditions are honored when the involved players employ blacklisting strategies.**

I. Introduction

The rapid increase in participation in social networking sites and other content sharing sites along with the high volume of user generated data hosted on these sites has created many new challenges in different areas such as archiving, indexing, searching, and sharing [**?**]. In this paper, we focus on the sharing problem.

While online social networking is already enormously popular, sharing of personal content online is proving to be a hard problem. In many occasions users are often faced with sharing situations in which they want to limit the access to certain personal content to a specific set of friends. Depending on the content being shared, a personal data collection can have variety of different data with diverse sharing requirements.

Another important concern in the problem of sharing is the unauthorized sharing (redistribution) of content owned by people. When valuable objects are involved, users are willing to share if they expect the other party to honor the usage conditions bound to the objects. However, those who posses the shared objects can decide to dishonor the sharing conditions and perform unauthorized propagation of the objects. This problem is very similar to the digital content rights management problem [**?**] on the Internet which is turning out to be a very hard problem.

Most solutions to the sharing problem and by extension to the digital rights management problem take the mechanism-centric approach. The central idea of the mechanism-centric approach is to develop secure mechanisms based on advanced cryptographic techniques to prevent unauthorized operations on the shared data. Although these techniques are essential for securing the content on sharing systems, it is also illuminating to investigate the costs and benefits associated with honoring and dishonoring sharing conditions.

Inspired by previous work in the area of microfinance [**?**], [**?**] and trusted collaborations on social networks [**?**], we investigate the incentives the different parties to the sharing processes have for honoring or dishonoring the conditions attached to the sharing processes. We propose to model the sharing problem as a noncooperative game.

A social network is a network created by linking friends where each edge denotes a friendship. This provides a unique property to social networks where people are known to each other locally and are able to exert "social pressure" on friends to elicit favorable actions. The social pressure can be applied in many different ways and blacklisting is one of them. The amount of pressure a user can exert on others depends on the way the user is embedded in the social network. For example, if the user has many friends, then she can expect significant sanctioning capacity. Therefore, she can share data objects of high value with a requestor and still expect him to honor the conditions.

Our main objective is to identify, using game theoretic analysis, the necessary conditions for an equilibrium where sharing takes place and its conditions are honored when blacklisting is utilized as punishing tool for dishonoring requestors.

The rest of the paper is organized as follows: Section **??** presents the sharing game model. Section **??** defines a repeated sharing game model for online social networks. In Section **??** we introduce the blacklisting strategies and identify through equilibrium analysis the conditions where the sharing conditions are honored. The effects of network and non-network parameters on the model are discussed in Section **??**. Related work is discussed in Section **??**.

II. Sharing Game

We present a noncooperative game model to represent a sharing transaction in online social networks. In the sharing game model only two players are involved, the *requestor* who wishes to access an object of another user the *owner*. The owner can either decide to reject or fulfil the request made by the requestor. In a sharing transaction, the owner shares a copy of the object with the requestor who is free to utilize the object under certain conditions set by the owner (i.e., video sharing).

A sharing game is initiated when a user makes a sharing request for an object. In the game, the owner makes the first move where she can either reject the request and the game ends

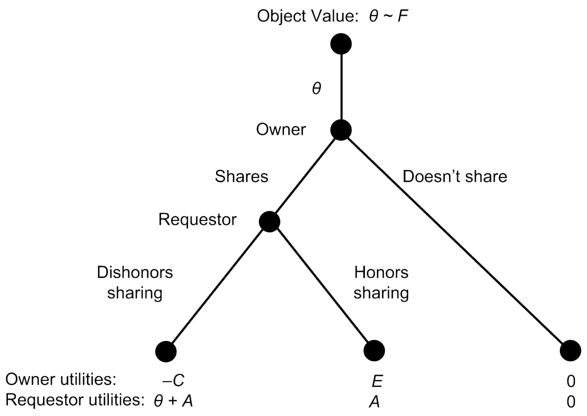

Fig. 1. Extensive form of the sharing game

or she can fulfil the request and grants the requestor access. If sharing takes place then the turn goes to the requestor where he can either honor or abuse sharing (the sharing conditions placed by the owner) and the game ends. The extensive (tree) form of the sharing game model is shown in Figure **??**. In the game, θ represents the value of the object being shared as observed by both the owner and the requestor when the game starts. We let the value of θ be randomly sampled from a continuous probability distribution F defined on the interval [0,∞). The payoffs gained by the owner and the requestor depend on the game. When the sharing request is rejected both the owner and requestor receive zero payoffs. If sharing takes place and the sharing conditions are honored then the owner's payoff is E which is derived from future requests the owner can make to the requestor, whereas the requestor's payoff A is obtained through the utilization of the object. When the sharing conditions are dishonored, then the owner's payoff is $-C$ because the owner incurs a loss because the sharing conditions are violated and the owner is not expected to derive any utility from future transactions with the requestor as a results of the lack of trust the between the two. The requestor's payoff however is $A + \theta$ resulting from the additional gain made from dishonoring the sharing conditions (e.g., pirating the object). Therefore, a highly valuable object results in a high incentive for the requestor to abuse the sharing conditions because the extra utility generated could be high.

III. Repeated Sharing Game Model

Rational players involved in a single sharing transaction are always expected to defect, the owner will not share and the requestor will dishonor the sharing conditions, because that combination of strategies form a Nash equilibrium. The reason is if the owner decides to share, then for the requestor, dishonoring yields the maximum payoff $A + \theta$ and in case the owner doesn't share, then the requestor won't improve his payoff by switching his strategy. Given the requestor's strategy, the best strategy for the owner is to abstain from sharing.

In social networks, users are expected to remain active and engage in many activities with other users in order to strengthen their social ties, create new relations, and derive social utility. Thus, we believe that a game modeling user interactions on a social network should reflect the persistence in user interactions. In addition, users who interact repeatedly take into account the outcome history of previous transactions when making decisions for future transactions. Considering the previous arguments, we present a repeated sharing game to model sharing transactions in social networks.

We define a repeated sharing game as being a repetition of the sharing game played at discrete moments in time (t = 0, 1, 2, ...). At each time step a pair of users engage in the sharing game. In order to simplify the equilibrium analysis of the repeated game, we will consider a single requestor playing with different owners on the social network. However, the analysis for the single requestor can be generalized to cover multiple requestors in the network. This is done by considering a separate independent repeated game for each requestor and the same analysis applies to each of those games separately. For the repeated game, we assume that there is an infinite supply of different objects with different values on the network. We also assume that the repeated game is infinite meaning that it consists of an indefinite number of sharing games played by the requestor and the owners.

In the repeated game model, we use an undirected graph to represent the social network. From the social network graph a single requestor is selected. Each sharing game is then played by the requestor and one of remaining network users. At the start of each sharing game the value of the object θ is set using the continuous distribution F and its value is known to both players. The owner for the sharing game is determined randomly through a simple random walk taken by the requestor on the social network graph. The random walk starts from a random starting user and then continues indefinitely. The sequence of nodes visited in the walk is a Markov chain where the initial node is selected uniformly at random. We denote by $\mathbf{P}$ =(p_{uv}) the matrix of transition probabilities of this Markov chain. So

$$p_{uv} = \begin{cases} 1/d(u), & \text{if } u, v \in E \\ 0, & \text{otherwise.} \end{cases} \qquad (1)$$

After each sharing game the requestor proceeds to play with one of the owner's friends. A conditional exchange of information between the current owner and her neighbors will take place at the end of each sharing game if the requestor dishonors sharing. In this case the owner will communicate the requestor's dishonoring behavior to all of her neighbors. If the requestor honors trust then no exchange of information takes place. In the game model, we assume that the users who know about the requestor's dishonoring behavior will blacklist him so they will not be willing to deal with the requestor in the future. If during the repeated game the requestor makes a sharing request to a blacklisting user then the request is always denied.

In the rest of the paper we will denote the repeated game with $\Gamma(S, \mathbf{P}, w, r)$, where S denotes a single sharing game, $\mathbf{P}$ is the transition matrix for the random walk, w is the requestor's discounting factor for future transactions, and r denotes the current requestor.

IV. Equilibrium Analysis of the Repeated Game

In this section, we find the necessary conditions for an equilibrium in which sharing conditions are honored in the repeated sharing game.

For the repeated game Γ, an equilibrium where sharing takes place and is honored can't be reached if sharing transactions take place unconditionally. The reason is if there are no threats of punishment for defection, then the requestor will always dishonor the sharing conditions since it represents the best choice for him. Thus, an equilibrium in which sharing takes place and is honored must be based on "conditionally cooperative" strategies in which the owner will switch from cooperative (sharing) to uncooperative behavior (not sharing) if the requestor dishonors sharing.

Trigger strategies [**?**] are a class of conditionally cooperative strategies that are employed in repeated non-cooperate games in order to develop cooperation among the players. In trigger strategies, a player will continue to cooperate as long the other player (opponent) cooperates. Once a defection is observed, the player will stop cooperating in future encounters. Trigger strategies vary depending on the trigger level and severity of the punishment.

For the repeated game $\Gamma(S, \mathbf{P}, w, r)$ we will consider a blacklisting based trigger strategy for the owners. The blacklisting trigger strategy is defined as follows:

1) The owner will act cooperatively, owner will share with the requestor, as long as the requestor acts cooperatively.
2) If the requestor deviates from cooperative behavior (dishonors the sharing conditions), then the owner and all of his/her friends will black-list the requestor forever.

Next we analyze equilibrium for the repeated game under the blacklisting trigger strategy. We find the necessary and sufficient conditions for an equilibrium where sharing can take place and is honored.

We identify each sharing game played at any time during the repeated game with the pair (θ, i), where i is the owner involved and θ is the value of the object requested. The social pressure that an owner can exert on the requestor depend on how she is embedded within the social network. To measure this potential, we introduce a threshold value ϑ_i for each owner in the social network. We denote these values as *sharing thresholds* since they indicate the extend to which an owner can safely share with the requestor in any sharing game. In the repeated game an owner who is involved in a sharing game will share the object with the requestor only if $\theta \leq \vartheta_i$ and the requestor is not blacklisted. Otherwise, the owner will reject the request. Thus, for a given sharing game if the object's value is too high, the owner will withhold because the requestor's incentive to dishonor sharing will be high.

The next theorem is adapted from [**?**] for our sharing game, it provides a subgame perfect equilibrium solution for the repeated sharing game $\Gamma(S, \mathbf{P}, w, r)$ in terms of the sharing thresholds.

Theorem 1: Consider the repeated game $\Gamma(S, \mathbf{P}, w, r)$ and let $\mathbf{P}$ be the transition matrix for the requestor r on the social network graph. Then, the vector $\boldsymbol{\vartheta} = (\vartheta_1, ..., \vartheta_n)$ of blacklisting trigger strategies is a subgame-perfect equilibrium if and only if

$$\vartheta_i = A\boldsymbol{e_i}[(\mathbf{I} - w\mathbf{P})^{-1} - \mathbf{I}]\boldsymbol{\mu^{(i)}}$$

where,
$\boldsymbol{e_i}$ is the ith unit vector of length n,
$\mathbf{I}$ is an identity matrix of size n, and
$\boldsymbol{\mu^{(i)}}$ is a vector of size n where the jth entry is $F(\vartheta_j)$ if j is a friend of i and zero otherwise.

Proof: The proof of the theorem is similar to [**?**] with some modifications. In the proof, we show that if condition stated above holds, then the desired equilibrium, sharing is always honored, is reached. The idea behind the proof is to show that the players will not improve their payoffs if they deviate from the equilibrium strategies at any point during the repeated game. To achieve this, we apply Bellman's optimality principle [**?**] to show that if a single deviation from the equilibrium strategies doesn't increase the payoff of the deviating player, then it will not be considered in the first place and the equilibrium stands. Assume, without loss of generality, that at time $t = 0$ the requestor is playing with owner (i). We need to consider two cases when $\theta > \vartheta_i$ and when $\theta \leq \vartheta_i$. In the first case when $\theta > \vartheta_i$, the owner would not share because the value of the object is too high and the requestor has high incentive to dishonor sharing if it takes place. In this case, both actors don't have any motivation to deviate from their choices because it yields the best possible payoff for both. In the second case where $\theta \leq \vartheta_i$, the owner will share. In this case, the owner will not defect because this choice yields the maximum possible payoff E for her. For the requestor, the rational choice is to dishonor and get $A + \theta$ if the short-term gain due to dishonoring is greater than the long-term loss from the punishment due to the blacklisting applied by the owner and her friends. Therefore, for the desired equilibrium we need to find the conditions for which the long-term loss for the requestor is greater than or equal to the short-term gain due to dishonoring. In other words, the requestor will not have the incentive to deviate from the equilibrium strategy because he is always better off honoring the conditions.

Let EU_H be the expected utility of the requestor when he always honors, and let EU_D be the expected utility when the requestor dishonors sharing once. Given that the object values are sampled from the continuous distribution $F(X) = Pr\{\theta \leq X\}$, then the requestor's payoff when playing with any owner i in the future equals zero with probability $Pr(\theta > \vartheta_i) = 1 - F(\vartheta_i)$ and is equal to A with probability $F(\vartheta_i)$ provided that the requestor is not black-listed. Given that the requestor starts the repeated game with owner i and using the transition matrix $\mathbf{P}$ to dictate the next owner the requestor will play with, we can find the expected utility of the requestor when there is no deviation as.

$$EU_H = A+\sum_{t=1}^{\infty} Aw^t\boldsymbol{e_i}\mathbf{P}^t\boldsymbol{\mu} = A+A\boldsymbol{e_i}[(\mathbf{I}-w\mathbf{P})^{-1}-\mathbf{I}]\boldsymbol{\mu} \tag{2}$$

where $\boldsymbol{\mu} = (\mu_1, ..., \mu_n)$ with $\mu_j = F(\vartheta_j)$.

Now, consider the other case when the requestor deviates from the equilibrium strategy and dishonors the conditions. Once the sharing is dishonored the requestor will be blacklisted. Thus, according to the repeated game model the requestor will get zero payoff if he happens to play with the same owner or any of her friends. The payoff for the requestor from the first game in which he abused sharing is $A+\theta$. Assuming the requestor starts with owner i, we find the expected payoff in this case as,

$$\begin{aligned} EU_D = (A+\theta) + \sum_{t=1}^{\infty} Aw^t\boldsymbol{e_i}\mathbf{P}^t[\boldsymbol{\mu}-\boldsymbol{\mu^{(i)}}] = \\ (A+\theta) + A\boldsymbol{e_i}[(\mathbf{I}-w\mathbf{P})^{-1}-\mathbf{I}][\boldsymbol{\mu}-\boldsymbol{\mu^{(i)}}] \end{aligned} \tag{3}$$

In the above equation, $\boldsymbol{\mu^{(i)}}$ is a n-vector where for all $j \neq i$, $\mu_j^{(i)} = \mu_j$ if j is a friend of i and $\mu_j^{(i)} = 0$ otherwise. In this step we basically set the expected payoff from the owner and her friends to zero by subtracting the $\boldsymbol{\mu^{(i)}}$ vector from $\boldsymbol{\mu}$ in Equation (**??**).

To have the desired equilibrium, then $EU_H \geq EU_D$ must hold for all $\theta \leq \vartheta_i$. Hence, this is equivalent to

$$\theta \leq A\boldsymbol{e_i}[(\mathbf{I}-w\mathbf{P})^{-1}-\mathbf{I}]\boldsymbol{\mu^{(i)}} \tag{4}$$

In equilibrium, because Equation (**??**) must hold for all $\theta \leq \vartheta_i$, then, the maximum possible trust threshold of owner i is attained by setting the threshold value to the right hand side of Equation (**??**). So we get

$$\vartheta_i = A\boldsymbol{e_i}[(\mathbf{I}-w\mathbf{P})^{-1}-\mathbf{I}]\boldsymbol{\mu^{(i)}} \tag{5}$$

Now since the same proof also holds true for all the other owners in the network, the blacklisting trigger strategies are in equilibrium. ■

The sharing thresholds $\boldsymbol{\vartheta}$ presented in Theorem **??** indicate the extend to which the owners can safely share with the requestor and the $(F(\vartheta_1), ..., F(\vartheta_n))$ values represent the proportion of times each owners will share with the requestor. The values of the ϑ_i's and $F(\vartheta_i)$'s depend on the social pressure that each owner has on a requestor via blacklisting. In other words, owners with high punishing capability have higher sharing thresholds because the long term losses for the requestor due to blacklisting by those owners is high. Next we discuss the effects of the model (non-network) and network parameters on the on the sharing thresholds.

From the threshold equation in Theorem **??** we consider the effects of the following parameters on the thresholds, the sanction cost A, the requestor's discounting factor w, and the requestor's request patterns captured through the simple random walk $\mathbf{P}$. A black-listed requestor will incur a loss of A for each game played with a blacklisting owner and so if the sanction cost increase so will the loss that the requestor will suffer for each rejected request. Thus, the requestor will be less willing to dishonor if the sanction cost is high and so the owner can have a higher sharing threshold with the requestor. For the requestor a higher discounting factor w indicates that he cares more about future transactions therefore, the punishment will be more severe allowing for a higher sharing thresholds. For the random walk, we postpone the discussion of its effect to the next section when we present the simulation results.

Since the effect of the network parameters on the sharing thresholds is not immediately obvious from the threshold equations, we will consider the effect of two network parameters, the owner's degree and the size of the maximum clique in which the owner is a member. On social networks, the degree represents the number of friends that an owner has and so owners with many friends are expected to have high threshold because they have a high blacklisting capacity and effectively a stronger punishing capability. Cliques on the other hand represent strongly connected groups where all of its members are considered equal in terms of the sharing thresholds due to the network structural properties of such groups. Owners who are members of large cliques are expected to have high thresholds because they have high degree in addition, to being connected to friends that have high thresholds.

In the next section, we use simulations applied on traces extracted from actual online social networks to further analyze the effects of the different parameters on the sharing thresholds.

V. Simulation Setup and Results

In this section, we use extensive simulations to study the effects of the network and model parameters on the sharing thresholds of the owners.

To setup the simulations we used topologies extracted from `flickr.com` [**?**]. Using the traces we constructed a synthetic social network with approximately 1.7 million users as the main social graph. From the main social graph we extracted a set of 1000 different subgraphs each subgraph containing 1000 nodes. To extract each subgraph, we select a random seed node from the main social graph and then use a breadth first expansion from the seed node to form the subgraph. For each subgraph we selected ten different requestors and formulated a repeated sharing game based on them. Thus, the results reported in this section are for $1000 \times 10 = 10,000$ different repeated games.

For each repeated game we form its transition matrix **P** after removing the involved requestor from the subgraph associated with the sampled game. The remaining model parameters were fixed for the sampled games. In the simulations, we set the value of the discounting factor w to 0.9 and the payoff cost A to 1. For the object values, we use the probability distribution $F_a(\vartheta) = Pr\{\theta \leq \vartheta\} = \vartheta/(a+\vartheta)$. Here, a is the average of the object values in the network and is set to 1.0 in the simulations. Using MATLAB, we find the solution for each sampled repeated game and get the sharing thresholds for all the users in the subgraph. Thus, the solution set consists of $10,000 \times 999 = 9,990,000$ different threshold values for the different sampled games. For our analysis we randomly

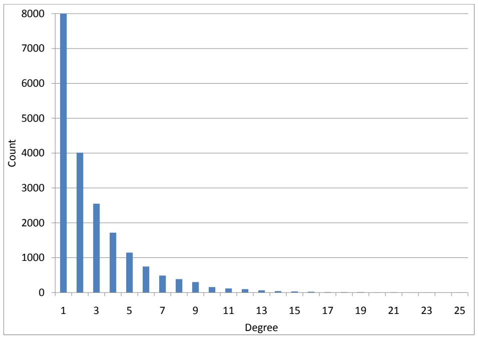

Fig. 2. Distribution of node degree for the bottom 10% threshold values

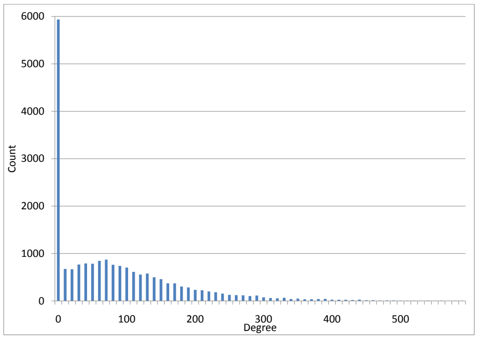

Fig. 3. Distribution of node degree for the top 10% threshold values

extracted 200,0000 threshold values from the solution set. In addition, for each user in our final sampled set we find the information related to the node's network properties i.e. degree and size of the maximum clique in which the nodes is member of.

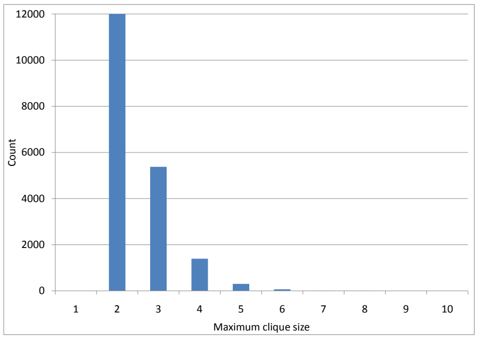

Fig. 4. Distribution of maximum clique size for the bottom 10% threshold values

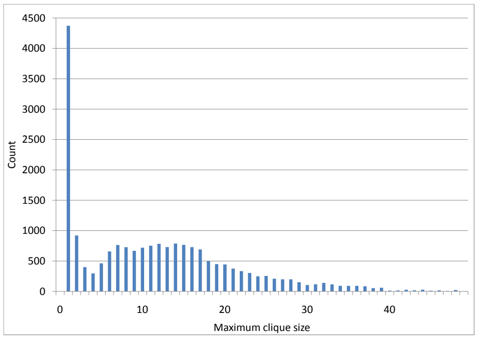

Fig. 5. Distribution of maximum clique size for the top 10% threshold values

For the network parameters, we first consider the effect of the node degree on the sharing threshold. In the previous section we reasoned that nodes with many friends (high degree) are expected to have high sharing thresholds because they have high blacklisting capacity. To check the validity of our assertion, we took the top 10 percent and bottom 10 percent threshold values from the sampled thresholds and compared their node degrees. Figures **??** and **??** shows the distribution of node degrees for the bottom and top 10 percent sampled threshold values respectively. For the bottom 10 percent, almost all of the nodes have degrees ranging between 1 and 13 with the median being 2. This means that 50% of the nodes have two friends or less and the other half have 3 or more friends with 19 being the maximum. The distribution of degrees in the top 10 percent had greater spread ranging from 2 up to 600 with a median of 65. From Figure **??**, we also note that a considerable number of nodes have degree of 10 or less. The reason for this is that having high degree is sufficient but not necessary for having a high threshold value because there are other network and model parameters that affect the threshold values. On the other hand having low degree is a necessary condition for having a low threshold value. In addition to the node degree, we examined the effect of another network parameter, the maximum clique size of a node on the thresholds. As for the model parameters we briefly describe how the object request pattern of the requestor resulting from the random walk affects the threshold values.

Next, we consider the influence of strongly connected social groups [**?**] on the sharing thresholds. In particular, we look at the relationship between the threshold value of a node and the size of the maximum clique size in which the node is a member. We again consider the top and bottom 10 percent threshold values and compare the distribution of the maximum cliques for both sets. Figures **??** and **??** show the distribution of clique sizes for both sets. For the bottom 10 percent thresholds, the maximum cliques range from 2 to 6 with a median of 2 and the majority over 70% of the nodes having cliques sizes of 3 or less. The distribution of the clique sizes of the top 10 percent have larger spread from 2 up to 50 with a median of 12. For the clique sizes of the top thresholds, we observe a similar pattern to the degrees of the top thresholds in terms of the spread of the clique sizes and the existence of considerable number of small cliques. This again is due to the same reason explained above for the large degrees. Therefore, the majority of the nodes with high trust thresholds are either members of sizable cliques or have large number of friends or the combination of both.

For non-network parameters, the simulations show an effect for the requestor's object request patterns, modeled as a simple random walk, on the trust thresholds. The results show that

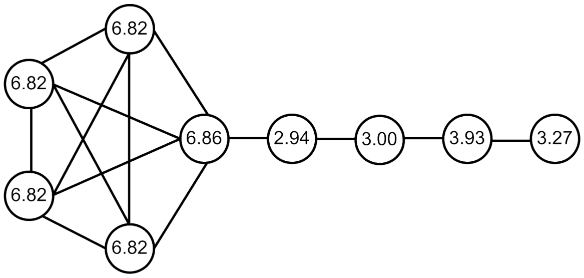

Fig. 6. Sharing threshold values for the nodes when the object request pattern is based on a simple random walk

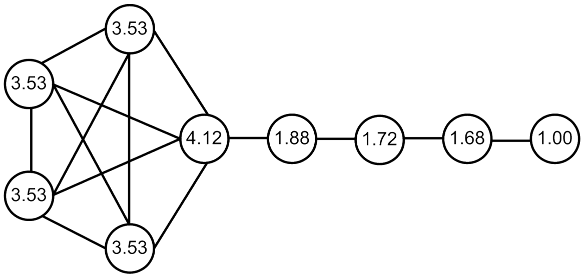

Fig. 7. Sharing threshold values for the nodes when the object request pattern is based on uniform distribution

nodes or cluster of nodes that have few connections to other social network components (i.e., isolated nodes) tend to have higher trust thresholds. The reason is a random walk that reaches an isolated clusters will spend longer time at those clusters before escaping to other parts of the network this allows the nodes in such clusters to punish the requestor for longer periods in case of a defection. We illustrate the effect, using a small graph. For the graph, we formulate its repeated game, and find the thresholds using our simple random walk for the object request pattern. Then, using a uniformly random based request pattern we again find the threshold values for the same repeated sharing game. Figures **??** and **??** show the example graph with the threshold values, shown inside each node, for the random walk based request pattern and the uniformly request pattern respectively. Comparing the threshold values for the chain of nodes in the two figures, we immediately notice that under the random walk based request pattern, the threshold values of the nodes increase as the nodes become more distant from the clique component. When the uniformly random request pattern is used, the thresholds values of the same set of nodes decrease as they become more distant from the clique.

VI. Related Work

In Chapter 3 of [**?**], Buskens presents a game theoretic model for the control effects in social networks. The model consists of a repeated trust game played by a trustee and a network of trustors. In the model, the trustors use trigger strategies to penalize the trustee for defections. Under trigger strategies, the author proofs the existence of an equilibrium in which trust can be placed and is honored and presents a solution to the model. In addition, the effects of various network and model parameters on the equilibrium solution are analyzed using approximation methods and simulations on different small synthetic networks.

Although our game model has several similarities to the one in the above work, our model is different in certain aspects as well. We introduce a blacklisting trigger strategy in which only the owner and her friends will stop sharing with the requestor in case the requestor defects with the owner. Whereas, in Buskens's model every trustor could sanction the trustee if she discovers a defection in the history of the trustee's transactions with other trustors. We believe that in large social networking communities a defection would trigger a blacklisting reaction similar to the one in our model simply because the friends of the cheated owner are expected to react more strongly than other socially distant users on the network.

Mobius and Szeidl [**?**] address the problem of informal contract enforcement on social networks by considering borrowing situations between agents. They present a game theoretic model in which relationships between individuals generate social collateral that can be used to control the moral hazard in borrowing situations. Trust between two agents is defined as the maximum amount that one agent can borrow from another. The authors proof the existence of an equilibrium by showing that a borrowing transaction can take place if the value of the requested item is bounded above by the maximum network flow (or trust flow) between the borrower and lender on the social network. Furthermore, they derive closed form expressions that relate trust to the social network structure. In our work, we consider sharing situations on the social network and present a game model for it and then find the necessary conditions for an equilibrium where sharing is honored which is similar to problem consider by the authors. However, our game model is different from the author's model. Moreover, we employ a blacklisting strategy as a punishing tool to reach the equilibrium whereas the authors utilize the social relationships as a collateral in their model.

In addition, there is a large body of work treating the problem of sharing in peer-to-peer systems using game theory (a representative set is given by [**?**], [**?**], [**?**], [**?**]). Utilizing different game theoretic models, they address the problem of promoting cooperation in peer-to-peer systems when non-cooperative users can benefit from free-riding on others' resources. Since these papers address the same problem, we briefly discuss one work. In [**?**], Zhang et al. introduce an unstructured file sharing game and an overlay formation game to model interactions among self-interested users. Users are modeled as players, where each user adjusts her number of connections on its available paths to maximize her utility. They show using examples the existence of multiple stable network states, Nash equilibria, for the file sharing game on general networks. In addition, they study the Tit-for-Tat strategy through the overlay formation game and prove the existence of equilibrium overlays. Our work is similar to the above in the sense that we use game theory in order to achieve cooperative behavior between users in sharing transactions in social networks. However, we differ in certain aspects for example, we deal with transactions on social networks where relationships can have an effect on these transactions, while this not the case in peer-to-peer systems. Also, our game model achieves cooperation through the application of sanctioning for noncooperative behavior while for the work above it is mostly based on incentive design to avoid the problem.

Game theoretic models have also been proposed to address different problems related to wireless communications systems and networks, we briefly mention a few. In [**?**], the authors discuss the problem of cooperative sensing in cognitive radio where they propose an evolutionary game framework to study the interactions between selfish users in cooperative sensing. The work in [**?**], presents a distributed optimization framework for wireless multihop sensor networks based on a game theoretic approach. The authors in [**?**], study Aloha, a random access scheme for random-access based wireless networks, using cooperative and noncooperative Aloha games.

VII. Conclusion and Future Work

In this paper, we investigated the problem of online data sharing on social networks. For the sharing problem two major issues stand out, controlling access to shared content and preventing unauthorized redistribution of the content.

Inspired by previous work in the area of microlending in finance [**?**] and trust collaboration on social networks [**?**], we studied the incentives for users to break or adhere to the strategies that underly the key mechanisms used in online data sharing. We developed a game theoretic model for the sharing problem and analyzed them as part of this study. The major contributions of our study are the following:

- We introduced a noncooperative game for modeling sharing data objects in social networks. To elicit cooperation, we introduced blacklisting as a trigger strategy that could offset the incentives that may be present in a noncooperative game.
- We proof the existence of an equilibrium for the repeated sharing game in which sharing can take place and is honored, and provide an analytical solution the captures the necessary conditions required to sustain such an equilibrium.
- Using extensive simulations on topologies extracted from online social networking traces, we studied and analyzed the effects of different network and non-network (model) parameters on the equilibrium solution.

Future work will investigate different request distributions and their effects on the equilibrium solution, also we intend to experiment with different game models that incorporate temporary blacklisting and concurrent transactions and understand how these elements can affect the analytical solution.

References

[1] R. Ramakrishnan and A. Tomkins, "Towards a peopleweb," *IEEE Computer*, vol. 40, no. 8, pp. 63–72, Aug. 2007.

[2] R. Dhamija and F. Wallenberg, "A framework for evaluating digital rights management proposals," in *In 1st International Mobile IPR Workshop*, Aug. 2003.

[3] J. Morduch, "The microfinance promise," *Journal of Economic Literature*, vol. 37, no. 4, pp. 1569–1614, 1999.

[4] D. Karlan, "Social connections and group banking," *Economic Journal*, vol. 117, pp. F52–F84, Feb. 2007.

[5] M. J. Burgera and V. Buskens, "Social context and network formation: An experimental study," *Social Networks Journal*, vol. 31, no. 1, pp. 63–75, 2009.

[6] J. W. Friedman, *Game theory with applications to economics*. New York, NY: Oxford University Press, 1986.

[7] V. Buskens, *Social Networks and Trust*. Norwell, MA: Kluwer academic Publishers, 2002.

[8] R. Bellman, *Dynamic Programming*. Princeton, NJ: Princeton University Press, 1957.

[9] http://socialnetworks.mpi-sws.org/.

[10] S. Wasserman and K. Faust, *Social Network Analysis*. New York, NY: Cambridge University Press, 1997.

[11] M. Mobius and A. Szeidl, "Trust and social collateral," National Bureau of Economic Research, Inc, NBER Working Papers 13126, May 2007. [Online]. Available: http://ideas.repec.org/p/nbr/nberwo/13126.html

[12] H. Zhang, G. Neglia, D. Towsley, and G. L. Presti, "On unstructured file sharing networks," *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pp. 2189–2197, May 2007.

[13] M. Rogers and S. Bhatti, "Cooperation under scarcity: The sharer's dilemma," in *AIMS '08: Proceedings of the 2nd international conference on Autonomous Infrastructure, Management and Security*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 28–39.

[14] K. Lai, M. Feldman, I. Stoica, and J. Chuang, "Incentives for cooperation in peer-to-peer networks," in *Proc. the Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, 2003.

[15] G. Philippe, K. Leyton-Brown, I. Mironov, and M. Lillibridge, "Incentives for sharing in peer-to-peer networks," in *EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce*. New York, NY, USA: ACM, 2001, pp. 264–267.

[16] B. Wang, K. Liu, and T. Clancy, "Evolutionary game framework for behavior dynamics in cooperative spectrum sensing," in *Global Telecommunications Conference. IEEE GLOBECOM '08. IEEE*, Dec 2008, pp. 1–5.

[17] J. Yuan and W. Yu, "Distributed cross-layer optimization of wireless sensor networks: A game theoretic approach," in *Global Telecommunications Conference. IEEE GLOBECOM '06. IEEE*, Dec. 2006, pp. 1–5.

[18] Y. Cho and F. Tobagi, "Cooperative and non-cooperative aloha games with channel capture," in *Global Telecommunications Conference. IEEE GLOBECOM '08. IEEE*, Dec. 2008, pp. 1–6.