# Game Theoretic Analysis of Multiparty Access Control in Online Social Networks

Hongxin Hu
Clemson University
Clemson, SC 29634
hhu@desu.edu

Gail-Joon Ahn
Arizona State University
Tempe, AZ 85287
gahn@asu.edu

Ziming Zhao
Arizona State University
Tempe, AZ 85287
ziming.zhao@asu.edu

Dejun Yang
Colorado School of Mines
Golden, CO 80401
djyang@mines.edu

## ABSTRACT

Existing online social networks (OSNs) only allow a single user to restrict access to her/his data but cannot provide any mechanism to enforce privacy concerns over data associated with multiple users. This situation leaves privacy conflicts largely unresolved and leads to the potential disclosure of users' sensitive information. To address such an issue, a MultiParty Access Control (MPAC) model was recently proposed, including a systematic approach to identify and resolve privacy conflicts for collaborative data sharing in OSNs. In this paper, we take another step to further study the problem of analyzing the strategic behavior of rational controllers in multiparty access control, where each controller aims to maximize her/his own benefit by adjusting her/his privacy setting in collaborative data sharing in OSNs. We first formulate this problem as a multiparty control game and show the existence of unique Nash Equilibrium (NE) which is critical because at an NE, no controller has any incentive to change her/his privacy setting. We then present algorithms to compute the NE and prove that the system can converge to the NE in only a few iterations. A numerical analysis is also provided for different scenarios that illustrate the interplay of controllers in the multiparty control game. In addition, we conduct user studies of the multiparty control game to explore the *gap* between game theoretic approaches and real human behaviors.

## Categories and Subject Descriptors

D.4.6 [**Security and Protection**]: Access controls; H.2.7 [**Information Systems**]: Security, integrity, and protection

## Keywords

Multiparty Access Control, Social Networks, Game Theory

## 1. INTRODUCTION

Online social networks (OSNs) have experienced explosive growth in recent years and become a *de facto* portal for hundreds of millions of Internet users. Facebook, for example, claims that it has more than 1.2 billion monthly active users [2]. As the popularity of OSNs continues to grow, a huge amount of possibly sensitive and private information has been uploaded to OSNs. To protect such a large volume of sensitive information, access control has received considerable attention as a central feature of OSNs [1, 3].

Today, nearly 4 out of 5 active Internet users visit OSNs [4], leading to a fundamental shift in the patterns of information exchange over the Internet. Users in OSNs are now required to be content *creators* and *managers*, rather than just being content *consumers*. Even though OSNs currently provide privacy control mechanisms allowing users to regulate access to information contained in their *own* spaces, users, unfortunately, have no control over data residing *outside* their spaces [8, 28, 34, 36]. For instance, if a user posts a comment in a friend's space, s/he cannot specify which users can view the comment. In another case, when a user uploads a photo and tags friends who appear in the photo, the tagged friends cannot restrict who can see this photo. Since multiple associated users may have different privacy concerns over the shared data, *privacy conflicts* occur and the lack of collaborative privacy control increases the potential risk in leaking sensitive information by friends to the public. In addition, federal and state government sectors have been leveraging social networks to exchange information and establish specialized groups/communities/task forces [27]. Even IT professionals started adopting social networks to look for solutions and best practices for their daily tasks while willingly sharing their tasks over OSNs [37]. Also, social networks have been widely accepted by a wide variety of patients who need to search for medical advices and exchange their experiences and other relevant information [15]. Such environments desperately need to protect and control the shared data due to its potential sensitivity and criticality. Therefore, it is essential to accommodate the special privacy control requirements coming from multiple associated users for collaboratively managing the shared data in OSNs.

To address such an issue, we recently proposed a multiparty access control (MPAC) model [22] to capture the core features of multiparty authorization requirements, which have not been accommodated by other access control systems for OSNs (e.g., [10, 11, 16, 17]). In particular, we introduced a systematic conflict detection and resolution approach [21] to cope with privacy conflicts occurring in collaborative management of data sharing in OSNs, balancing the need for privacy protection and the users' desire for information sharing by quantitative analysis of privacy risk and sharing loss. However, the proposed privacy conflict resolution mechanism assumes that all controllers are *well-behaved* to provide their pri-


*SACMAT'14,* June 25–27, 2014, London, Ontario, Canada.

http://dx.doi.org/10.1145/2613087.2613097.

vacy settings for collaborative sharing. In practice, users may attempt to *selfishly* maximize their own profits without respecting the benefit of the entire system.

In this paper, we take a further step toward analyzing the strategic behaviors of rational users who aim to maximize their own benefits in collaborative data sharing in OSNs. To this end, we formulate a multiparty control game, which models the interaction of controllers in multiparty access control. In addition, we derive the conditions and expressions of Nash Equilibrium (NE) for such a game. At an NE, no controller has an incentive to adjust her/his privacy setting when others fix their strategies. Moreover, we introduce two interactive adjustment algorithms to calculate the NE with respect to two different conditions, synchronous adjustment and non-synchronous adjustment, respectively. Our experimental analysis illustrates the system can converge to an NE in only a few iterations. We also provide a numerical analysis of the multiparty control game in terms of several different situations that reflect different incentives for controllers to change their privacy settings. Furthermore, we carry out user studies of the multiparty control game and articulate the gap between our game model and real human behaviors. We believe our game theoretic analysis provides important implications for the design of future collaborative sharing systems in OSNs.

The rest of the paper is organized as follows. In Section 2, we overview the multiparty access control mechanism, focusing on privacy conflict detection and resolution. In Section 3, we discuss our game model, along with the Equilibrium analysis and the convergence of our game. The details about evaluation results are described in Section 4. We overview the related work in Section 5. Section 6 discusses several important issues and our future work. We conclude this paper in Section 7.

## 2. OVERVIEW OF MULTIPARTY ACCESS CONTROL

Users in OSNs can post statuses and notes, upload photos and videos in their own spaces, tag others to their content, and share the content with their friends. On the other hand, users can also post content in their friends' spaces. The shared content may be connected with multiple users. For example, consider a photograph contains three users, Alice, Bob and Carol. If Alice uploads it to her own space and tags both Bob and Carol in the photo, Alice is called the *owner* of the photo, and Bob and Carol *stakeholders* of the photo. In another case, if this photo is posted by Alice to Bob's space, Alice is called the *contributor* of the photo. In addition, if Alice views a photo in Bob's space and decides to share this photo with her friends, the photo will be in turn posted to her space and she can authorize her friends to see this photo. In such a case, Alice is a *disseminator* of the photo. In all these cases, all associated users may be desired to specify privacy policies to control over who can see this photo. However, current online social networks, such as Facebook and Google+, only allow the data *owner* to fully control the shared data, but lack a mechanism to specify and enforce the privacy concerns from other associated users, leading to privacy conflicts being largely unresolved and sensitive information being potentially disclosed to the public. In order to enable a collaborative management of data sharing in OSNs, the multiparty access control (MPAC) model [22] was recently proposed.

When two users disagree on whom the shared data item should be exposed to, it causes a *privacy conflict*. The essential reason leading to the privacy conflicts is that multiple associated users of the shared data item often have different privacy concerns over the data item. For example, assume that Alice and Bob are two controllers of a photo. Each of them defines a privacy policy stating only her/his friends can view this photo. Since it is almost impossible that Alice and Bob have the same set of friends, privacy conflicts may *always* exist considering collaborative control over the shared data item. A systematic conflict detection and resolution mechanism has been presented in [21] to cope with privacy conflicts occurring in collaborative management of data sharing in OSNs, balancing the need for privacy protection and the users' desire for information sharing by quantitative analysis of privacy risk and sharing loss.

***Privacy Conflict Identification***: Through specifying the privacy policies to reflect the privacy concern, each controller of the shared data item defines a set of trusted users who can access the data item. The set of trusted users represents an *accessor space* for the controller. In [21], a space segmentation approach was provided to partition accessor spaces of all controllers of a shared data item into disjoint segments. Then, conflicting accessor space segments called *conflicting segments*, which contain accessors that some controllers of the shared data item do not trust, are identified. Each conflicting segment contains at least one privacy conflict.

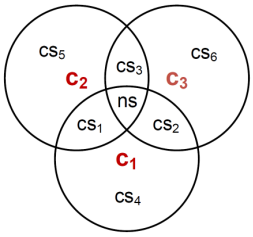



**Figure 1: Privacy Conflict Identification**

Figure 1 gives an example of identifying privacy conflicts based on accessor space segmentation. Circles are used to represent accessor spaces of three controllers, $c_1$, $c_2$ and $c_3$, of a shared data item. This example illustrates that three of accessor spaces overlap with each other, indicating that some accessors within the overlapping spaces are trusted by multiple controllers. After performing the space segmentation, seven disjoint accessor space segments are generated as shown in Figure 1. The accessor space segments are classified into two categories: *non-conflicting* segments and *conflicting* segments. A *non-conflicting* segment covers all controllers' access spaces, which means that any accessor within the segment is trusted by all controllers of the shared data item, indicating no privacy conflict occurs. A *conflicting* segment does not contain all controllers' access spaces, which means that accessors in the segment are untrusted by some controllers. Each *untrusting* controller points out a privacy conflict. In Figure 1, the segment $ns$ is a *non-conflicting* segment, and $cs_1$ through $cs_6$ are *conflicting* segments, where $cs_1$, $cs_2$ and $cs_3$ indicate *one* privacy conflict, respectively, and $cs_4$, $cs_5$ and $cs_6$ are associated with *two* privacy conflicts, respectively.

Once multiparty privacy conflicts are identified, a systematic approach for resolving privacy conflicts is needed. The process of privacy conflict resolution makes a decision to allow or deny the accessors within the conflicting segments to access the shared data item. In general, allowing the assessors contained in conflicting segments to access the data item may cause *privacy risk*, but denying a set of accessors in conflicting segments to access the data item may result in *sharing loss*.

***Measuring Privacy Risk***: The privacy risk of a conflicting segment is an indicator of potential threat to the privacy of controllers in

terms of the shared data item: the higher the privacy risk of a conflicting segment, the higher the threat to controllers' privacy. The basic premises for the measurement of privacy risk for a conflicting segment are: (a) the lower the number of controllers who trust the accessors within the conflicting segment, the higher the privacy risk; (b) the stronger the general privacy concerns of controllers, the higher the privacy risk; (c) the more sensitive the shared data item, the higher the privacy risk; and (d) the wider the data item spreads, the higher the privacy risk. In order to measure the overall privacy risk of a conflicting segment $\alpha$ denoted by $PR(\alpha)$, the following equation is used to aggregate the privacy risks of $\alpha$ due to different untrusting controllers.

$$PR(\alpha) = \sum_{\beta \in controllers_{ut}(\alpha)} (pc_\beta \times sl_\beta) \times n_\alpha \quad (1)$$

where function $controllers_{ut}(\alpha)$ returns all untrusting controllers of a conflict segment $\alpha$, $pc_\beta$ denotes the general privacy concern of an untrusting controller $\beta$ ($0 \leq pc_\beta \leq 1$), $sl_\beta$ denotes the sensitivity level of the shared data item explicitly chosen by an untrusting controller $\beta$ ($0 \leq sl_\beta \leq 1$), and $n_\alpha$ denotes visibility of the data item with respect to a conflicting segment captures how many accessors are contained in the segment $\alpha$.

***Measuring Sharing Loss***: When the decision of privacy conflict resolution for a conflicting segment is "deny", it may cause losses in potential data sharing since there are controllers expecting to allow the accessors in the conflicting segment to access the data item. The overall sharing loss $SL(\alpha)$ of a conflicting segment $\alpha$ is computed as follows:

$$SL(\alpha) = \sum_{\beta \in controllers_{t}(\alpha)} (1 - pc_\beta) \times (1 - sl_\beta) \times n_\alpha \quad (2)$$

where function $controllers_t(\alpha)$ returns all trusting controllers of a segment $\alpha$.

***Conflict Resolution Based on Privacy Protection and Data Sharing***: An optimal solution for privacy conflict resolution should cause lower privacy risk when allowing the accessors in some conflicting segments to access the data item, and get lesser loss in data sharing when denying the accessors to access the shared data item. Thus, for each conflict resolution solution $r$, a resolving score $RS(r)$ can be calculated using the following equation:

$$RS(r) = \frac{1}{\lambda \sum_{\alpha_1 \in CS_p^r} PR(\alpha_1) + (1-\lambda) \sum_{\alpha_2 \in CS_d^r} SL(\alpha_2)} \quad (3)$$

where $CS_p^r$ and $CS_d^r$ denote *permitted* conflicting segments and *denied* conflicting segments respectively in the conflict resolution solution $r$. And $\lambda$ and $1-\lambda$ are preference weights for the privacy risk and the sharing loss, $0 \leq \lambda \leq 1$, reflecting the privacy-sharing tradeoff. $\lambda$ can be calculated in terms of the average of sensitivity levels of all controllers. That is, $\lambda = \frac{\sum_{\beta \in controllers(d)} sl_\beta}{\ell \times n}$, where $controllers(d)$ returns all controllers of the shared data item $d$, and $n$ is the number of these controllers. Then, the optimal conflict resolution $CR_{opt}$ on the tradeoff between privacy risk and sharing loss can be the maximum resolving score, $CR_{opt} = \max_r RS(r)$.

To find the maximum resolving score, the privacy risk ($PR(\alpha)$) and the sharing loss ($SL(\alpha)$) are first calculated for each conflict segment ($\alpha$), individually. Finally, the following equation can be utilized to make the decisions for privacy conflict resolution.

$$Decision = \begin{cases} \text{Deny} & \text{if } \lambda PR(\alpha) \geq (1-\lambda) SL(\alpha) \\ \text{Permit} & \text{if } \lambda PR(\alpha) < (1-\lambda) SL(\alpha) \end{cases} \quad (4)$$

# 3. GAME MODEL

The privacy conflict resolution mechanism for multiparty access control presented in Section 2 assumes that all controllers are *well-behaved* to provide their privacy settings for collaborative sharing. However, in practice, controllers may attempt to *selfishly* maximize their own profits without respecting the benefit of entire system. For example, if a controller in the multiparty control system notices that the current privacy-sharing tradeoff (represented by $\lambda$ in Equation 3) for the conflict resolution is lower than her/his expectation, s/he may set a much stronger privacy preference to make the privacy-sharing tradeoff close to her/his expectation. In this section, we first introduce the basic game theory concepts and then articulate our multiparty control game model.

## 3.1 Basic Concepts in Game Theory

Game theory [31] is a discipline aiming at modeling situations where decision makers have to choose specific actions that have mutual or possibly conflicting consequences. A game consists of a set $\mathcal{P} = \{1, 2, ..., n\}$ of players. Each player $i \in \mathcal{P}$ has a non-empty strategy set $\Pi_i$. Let $s_i \in \Pi_i$ denote the selected strategy by $i$. A strategy profile $s$ consists of all the players' strategies, i.e., $s = (s_1, ..., s_n)$. Obviously, we have $s \in \Pi = \times_{i \in \mathcal{P}} \Pi_i$. Let $s_{-i}$ denote the strategy profile excluding $s_i$. Hence, we then have $s = (s_i, s_{-i})$. The utility function $u_i(s)$ of $i$ measures $i$'s valuation on strategy profile $s$. We say that $i$ prefers $s_i$ to $s_i^{'}$ if $u_i(s_i, s_{-i}) > u_i(s_i^{'}, s_{-i})$.

Given other players' strategies $s_{-i}$, $i$ can select a strategy, denoted by $\rho_i(s_{-i})$, which maximizes its utility function. Such a strategy is known as *best response* [31] in game theory, which can be formally defined as follows:

DEFINITION 1. *(Best Response). Given other player's strategies $s_{-i}$, a best response strategy of $i$ is a strategy $s_i \in \Pi_i$ such that $\rho_i(s_{-i}) = arg\max_{s_i \in \Pi_i} u_i(s_i, s_{-i})$, where $\Pi_i$ is the strategy space of $i$.*

To study the interactions of players, we adopt the concept of *Nash Equilibrium* (NE) [31], which is formally defined as follows:

DEFINITION 2. *(Nash Equilibrium). A strategy profile $s^{ne} = (s_1^{ne}, ..., s_n^{ne})$ is called a Nash Equilibrium, if for every play $i$, we have $u_i(s_i^{ne}, s_{-i}^{ne}) \geq u_i(s_i, s_{-i}^{ne})$ for every $s_i \in \Pi_i$.*

In an NE, none of the players can improve its utility by unilaterally deviating from its current strategy. Mathematically, it means $\rho_i(s_{-i}^{ne}) = s_i^{ne}$ for all $i \in \mathcal{P}$.

## 3.2 Multiparty Control Game

We model and study the interaction of controllers as a *multiparty control game* where each controller tries to maximize her/his own utility function. We derive conditions and expressions for the NE. This consists of the privacy setting strategy of each controller, such that no controller can benefit in terms of improving the utility by unilaterally deviating from the NE.

Consider a set of controllers, $\mathcal{P} = \{1, 2, ..., n\}$, who collaboratively control the sharing of a data item in a social network. The *multiparty control game* is played among $n$ controllers in the set $\mathcal{P}$. Each controller $i \in \mathcal{P}$ can specify her/his privacy policy. Then,

conflict detection and resolution mechanisms in the system are performed to discover and resolve privacy conflicts. Feedbacks of the conflict resolution are in turn provided to associated controllers. Based on the feedbacks, controllers can adjust their privacy settings to maximize their own utilities. For simplicity, we assume that the feedback returned to each controller indicates the privacy-sharing tradeoff, and the controller adjusts her/his privacy setting through changing the sensitivity level, $sl_i$, for the shared data item. The goal for each controller to adjust her/his privacy setting is to make the privacy-sharing tradeoff close to her/his expectation, $ep_i$. However, changing privacy setting may also result in the utility loss of the controller. For example, if a controller increases the sensitivity level for the shared data item, sharing loss values (calculated by Equation (2)) of the conflicting segments contained in this controller's access space are reduced. That means these conflicting segments have a higher chance to be denied due to such a privacy setting change, implying potential sharing loss for the controller. Therefore, we present the utility function of controller $i$ as follows:

$$u_i(sl_i, sl_{-i}) = -\mu_i(ep_i - \frac{\sum_{j\in\mathcal{P}} sl_j}{n})^2 - \tau_i(sl_i - ep_i)^2 \ . \quad (5)$$

In this utility function, if $sl_i$ is greater than $ep_i$, which means the controller $i$ strengthens her/his privacy setting, $\mu_i$ denotes the number of accessors in the conflicting segments *untrusted* by the controller $i$, and $\tau_i$ is the number of accessors in the conflicting segments *trusted* by the controller $i$. Otherwise, in case the controller $i$ weakens her/his privacy setting, $\mu_i$ and $\tau_i$ in this utility function indicate the numbers of *trusted* and *untrusted* accessors in conflicting segments, respectively. The *first term* in the utility function quantifies the utility gained by the controller $i$ and the *second term* in the utility function represents the utility loss of the controller $i$ when s/he changes her/his privacy setting. For instance, if the privacy-sharing tradeoff is lower than the controller's expectation in current system state, this means the controller's privacy risk is higher than her/his expectation after resolving privacy conflicts. The controller may increase the sensitivity level $sl_i$ of the shared data item to make the privacy-sharing tradeoff close to her/his expectation for reducing her/his privacy risk. At the same time, such a privacy setting change may also cause the sharing loss of the controller.

The set of controllers $\mathcal{P}$, the strategy space $\Pi$, and the utility function $\mathcal{U}$ define together the multiparty control game, $\mathcal{G}(\mathcal{P}, \Pi, \mathcal{U})$. In this game, each controller $i$ maximizes her/his own utility $u_i$ by choosing a *best response* strategy (privacy setting) $sl_i \in \Pi_i$, given the strategies (privacy settings) of others $sl_{-i}$, i.e.,

$$\rho_i(sl_{-i}) = arg \max_{sl_i\in\Pi_i} u_i(sl_i, sl_{-i}) \ . \quad (6)$$

## 3.3 Equilibrium Analysis

Based on the definition of NE (Definition 2), each controller plays her/his best response strategy in an NE. In other words, no controller has any incentive for changing her/his own strategy while the other controllers fix their strategies. To study the best response strategy of controller $i$, we calculate the derivatives of $u_i$ with respect to $sl_i$:

$$\frac{\partial u_i(sl_i, sl_{-i})}{\partial sl_i} = \frac{2\mu_i}{n}(ep_i - \frac{\sum_{j\in\mathcal{P}} sl_j}{n}) - 2\tau_i(sl_i - ep_i) \ . \quad (7)$$

$$\frac{\partial^2 u_i(sl_i, sl_{-i})}{\partial sl_i^2} = -\frac{\mu_i}{n^2} - \tau_i < 0 \ . \quad (8)$$

Since the second-order derivative of $u_i$ is negative, the utility $u_i$ is a *strictly concave function* in $sl_i$. Therefore, given any strategy profile $sl_{-i}$ of the other controllers, the best response strategy $\rho_i(sl_{-i})$ of controller $i$ is unique, if it exists. Setting the first derivative of $u_i$ to 0, we obtain

$$\frac{\mu_i}{n}(ep_i - \frac{\sum_{j\in\mathcal{P}} sl_j}{n}) - \tau_i(sl_i - ep_i) = 0 \ . \quad (9)$$

Solving for $sl_i$ in (9), we get

$$sl_i^* = \frac{(\mu_i n + \tau_i n^2)ep_i - \sum_{j\in\mathcal{P}\setminus\{i\}} sl_j^*}{\mu_i + \tau_i n^2} \ . \quad (10)$$

If all controllers have the same numbers of trusted/untrusted accessors in conflicting segments, i.e. $\mu_i = \mu$ and $\tau_i = \tau$ where $\forall i \in \mathcal{P}$, an explicit expression can be calculated for the unique NE. Through simple algebraic manipulations, we get

$$(1 + \frac{1}{\mu + \tau n^2})sl_i^* = \frac{(\mu n + \tau n^2)ep_i - \sum_{j\in\mathcal{P}} sl_j^*}{\mu + \tau n^2} \ . \quad (11)$$

and

$$\sum_{j\in\mathcal{P}} sl_j^* = \frac{\mu n + \tau n^2}{\mu + \tau n^2 + n - 1} \sum_{j\in\mathcal{P}} ep_j \ . \quad (12)$$

Then, the unique NE of the game is gotten as

$$sl_i^{ne} = \frac{(\mu n + \tau n^2)(ep_i - \frac{1}{\mu+\tau n^2+n-1}\sum_{j\in\mathcal{P}} ep_j)}{\mu + \tau n^2 - 1} \ . \quad (13)$$

Even though the controllers have different numbers of trusted/untrusted accessors in conflicting segments, we can still get the unique NE. The best response functions of the controllers can be expressed at the $sl^*$ in matrix form

$$sl^* = Asl^* + B, \quad (14)$$

where $B = (b_1, b_2, ..., b_n)$ and $b_i = \frac{(\mu_i n + \tau_i n^2)ep_i}{\mu_i + \tau_i n^2}$, and

$$A = \begin{pmatrix} 0 & -\frac{1}{\mu_1+\tau_1 n^2} & \cdots & -\frac{1}{\mu_1+\tau_1 n^2} \\ -\frac{1}{\mu_2+\tau_2 n^2} & 0 & \cdots & -\frac{1}{\mu_2+\tau_2 n^2} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{1}{\mu_n+\tau_n n^2} & -\frac{1}{\mu_n+\tau_n n^2} & \cdots & 0 \end{pmatrix}$$

Thus, the NE is

$$sl^* = (I - A)^{-1}B, \quad (15)$$

where $I$ is the identity matrix and $(.)^{-1}$ indicates the matrix inverse.

## 3.4 Converging to Nash Equilibrium

In the multiparty control game, the controllers interact with each other and adjust their privacy settings, unless the system is at the Nash equilibrium. They usually cannot reach a stable status in a single round. We model controller dynamics with interactive adjustment algorithms.

***Synchronous Adjustment***: In synchronous adjustment (SA), controllers adjust their privacy settings simultaneously at a time step $t = 1, 2, ..., n$ in terms of their own best response functions derived from (10):

$$sl_i(t+1) = \begin{cases} \frac{(\tau_i n + \mu_i n^2)ep_i - (\overline{sl} - sl_i(t))}{\tau_i + \mu_i n^2}, & \text{if } ep_i > \frac{\overline{sl}}{n}; \\ sl_i(t), & \text{if } ep_i = \frac{\overline{sl}}{n}; \\ \frac{(\mu_i n + \tau_i n^2)ep_i - (\overline{sl} - sl_i(t))}{\mu_i + \tau_i n^2}, & \text{if } ep_i < \frac{\overline{sl}}{n}. \end{cases} \quad (16)$$

where $\overline{sl} = \sum_{j \in \mathcal{P}} sl_j$.

From (16), we can notice that if a controller's privacy expectation ($ep_i$) is higher than the current privacy-sharing tradeoff ($\frac{\overline{sl}}{n}$), the controller strengthens her/his privacy setting ($sl_i$). If a controller's privacy expectation is lower than the current privacy-sharing tradeoff, the controller weakens her/his privacy setting. Otherwise, the controller keeps her/his privacy setting. Algorithm 1 shows the pseudocode of SA algorithm.

**Algorithm 1**: Synchronous Adjustment (SA)

**Input**: Initial sensitivity level $sl(0)$, convergence threshold $\psi$.
**Output**: NE of the game.

```
/* Initialize time step, t, and privacy expectation, ep */
t ← 0;
foreach i ∈ P do
    ep_i ← sl_i(0);
/* Find the stable state */
repeat
    sl̄(t) ← Σ_{i∈P} sl_i
    foreach i ∈ P do
        if controller i adjusts then
            if ep_i ≥ sl̄(t)/n then
                sl_i(t+1) = ((τ_i n + μ_i n^2) ep_i − (sl̄(t) − sl_i(t))) / (τ_i + μ_i n^2).
            else
                sl_i(t+1) = ((μ_i n + τ_i n^2) ep_i − (sl̄(t) − sl_i(t))) / (μ_i + τ_i n^2).
        else
            sl_i(t+1) = sl_i(t).
    t ← t + 1;
until There is no controller satisfying the condition: |sl(t) − sl(t−1)| > ψ ;
```

***non-synchronous Adjustment***: In practice, it is hard to require all controllers to update their privacy settings simultaneously. Therefore, a more realistic solution is to design a non-synchronous adjustment (NA) algorithm for practical collaborative sharing scenarios. In non-synchronous adjustment, we consider that controllers adjust their privacy settings one by one at one time step. The NA algorithm for the controller $i$ is formally defined with the same function as (16), but $\overline{sl}$ is defined as

$$\overline{sl} = \sum_{j<i} sl_j(t+1) + \sum_{j \geq i} sl_j(t). \tag{17}$$

The pseudocode of NA algorithm is shown in Algorithm 2.

**Algorithm 2**: non-synchronous Adjustment (NA)

**Input**: Initial sensitivity level $sl(0)$, convergence threshold $\psi$.
**Output**: NE of the game.

```
/* Initialize time step, t, and privacy expectation, ep */
t ← 0;
foreach i ∈ P do
    ep_i ← sl_i(0);
/* Find the stable state */
repeat
    foreach i = 1 to n do
        sl̄ = Σ_{j≤i} sl_j(t+1) + Σ_{j≥i} sl_j(t)
        if ep_i ≠ sl̄(t)/n then
            if ep_i ≥ sl̄(t)/n then
                sl_i(t+1) = ((τ_i n + μ_i n^2) ep_i − (sl̄(t) − sl_i(t))) / (τ_i + μ_i n^2).
            else
                sl_i(t+1) = ((μ_i n + τ_i n^2) ep_i − (sl̄(t) − sl_i(t))) / (μ_i + τ_i n^2).
        else
            sl_i(t+1) = sl_i(t).
    t ← t + 1;
until There is no controller satisfying the condition: |sl(t) − sl(t−1)| > ψ ;
```

# 4. EVALUATION

In this section, we present our evaluation results for our multiparty control game including both experimental analysis and user studies.

## 4.1 Experimental Analysis

To explore the convergence to the Nash equilibrium of our multiparty control game, we implemented and analyzed two interactive adjustment algorithms discussed above in a simulation system. We also presented a numerical analysis of the multiparty control game based on three different situations with respect to the number of untrusted accessors ($\mu$) and the number of trusted accessors ($\tau$) in the conflicting segments.

### *4.1.1 Convergence Analysis*

To view the process of system convergence, we ran the simulation on a 10-controller environment with initial sensitivity levels ranging from 0.1 to 1 in increments of 0.1, and considered all controllers have 20 untrusted accessors ($\mu = 20$) and 20 trusted accessors ($\tau = 20$).

For a synchronous scenario (each controller adjusts the sensitively level simultaneously), the interactive adjustment of sensitivity levels is depicted in Figure 2(a). We can observe that the speed of convergence to Nash equilibrium values is very fast (within 5 steps) in this scenario.

Regarding a non-synchronous scenario, a similar result occurs as shown in Figure 2(b). However, the convergence takes more steps (approximately 20 steps), since only one controller can update the sensitively level per step in such a scenario.

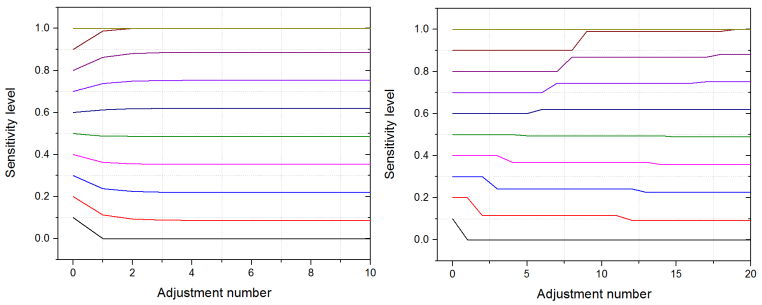
### *4.1.2 Numerical Analysis*

For the numerical analysis of our multiparty control game, we only focused on the initial and final (Nash equilibrium) sensitivity levels of the controllers under three different conditions.

In the first scenario, we studied a condition in which controllers have untrusted accessors more than trusted accessors ($\mu > \tau$). In this case, a controller with an expected (initial) sensitivity level higher than the privacy-sharing tradeoff (the average sensitivity level) has a strong incentive to enlarge her/his sensitivity level for reducing her/his privacy risk. However, a controller with an expected sensitivity level lower than the privacy-sharing tradeoff is reluctant to deviate too much from her/his initial sensitivity level due to the small number of trusted accessors in conflicting segments. Setting all controllers with 30 untrusted accessors ($\mu = 30$) and 10 trusted accessors ($\tau = 10$), Figure 3(a) illustrates the initial and final sensitivity levels of all controllers.

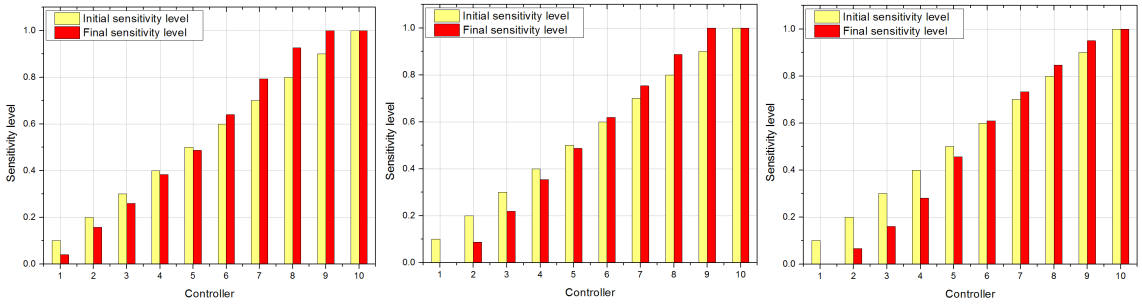
The second scenario studies the case when all controllers have the same number of untrusted accessors and trusted accessors ($\mu = \tau$). In such a case, the controllers with higher and lower initial sensitivity levels have similar intentions to change their sensitivity levels. Figure 3(b) shows the results of numerical analysis regarding 20 untrusted accessors and 20 trusted accessors for each controller.

In case that all controllers have untrusted accessors fewer than trusted accessors in conflicting segments ($\mu < \tau$), a controller with an initial sensitivity level lower than the privacy-sharing tradeoff has a much stronger incentive to deviate from her/his initial sensitivity level for mitigating her/his sharing loss. Considering 10 un-




(a) Convergence under SA (b) Convergence under NA

**Figure 2: Convergence to NE**




(a) $\mu > \tau$ (b) $\mu = \tau$ (c) $\mu < \tau$

**Figure 3: Initial and Final Sensitivity Levels of Controllers in Numerical Analysis**

trusted accessors and 30 trusted accessors for each controller, the results of numerical analysis are depicted in Figure 3(c).

## 4.2 User Study

We conducted user studies of the multiparty control game with respect to real human behaviors. The purpose of user studies is to verify if users behave as our game theoretical model expected. If there are some deviations of their behaviors from the model's predictions, we attempt to capture the factors that may cause such deviations.

### *4.2.1 User Study Design and Setup*

We designed two different kinds of user studies, which are approved by our institute's IRB. One is a multiple-round game (MRG) where participants set their sensitivity levels of photos at each round and they are told the average sensitivity levels after all participants finished inputting values. Another is a single-round game (SRG) where participants are told how many friends (trusted accessors) and non-friends (untrusted accessors) can view their photos after they initiate their sensitivity level settings, and they are only provided one chance to change their sensitivity levels.

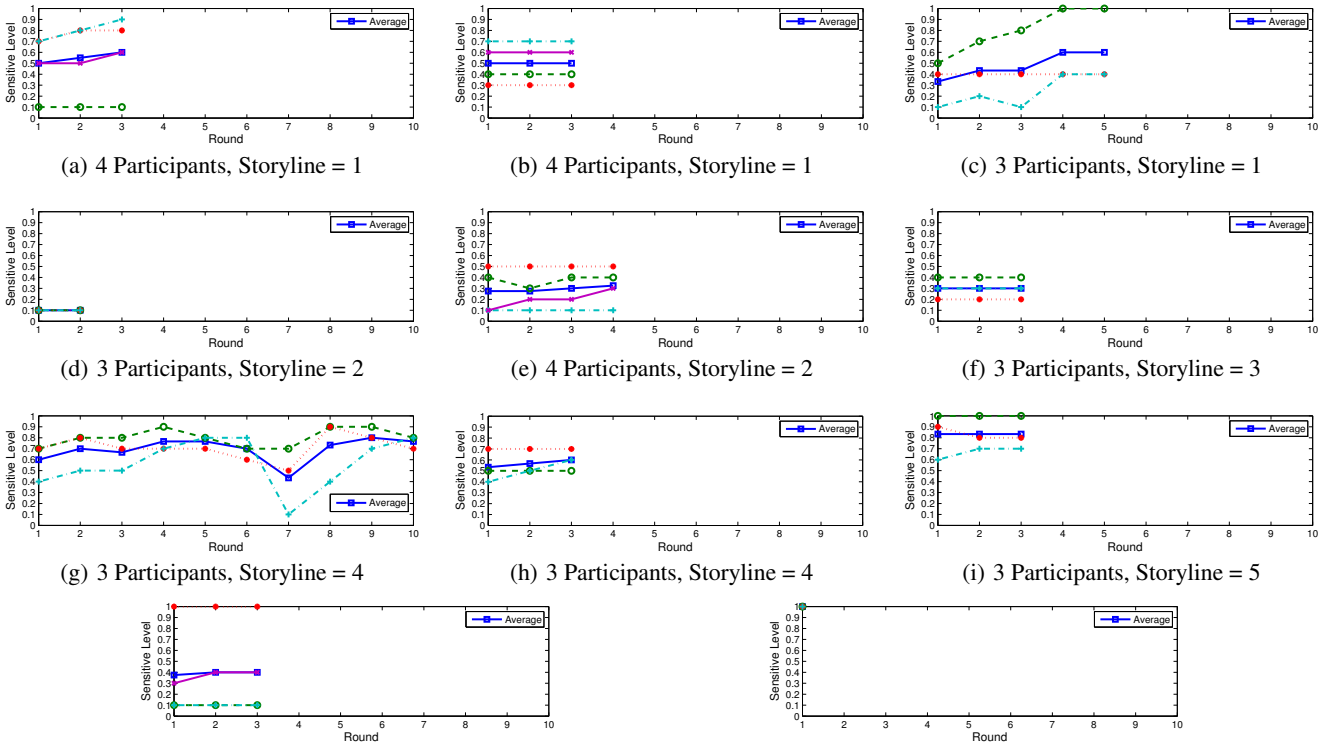
As part of the user studies, we first explained the motivation of our user studies to the participants, which is 'On Facebook or similar online social networks, a person who uploads a photo can tag other people and get control over who can see this photo. However, people tagged in the photo have no control over it. We are proposing a system that allows everyone tagged in a photo to collaboratively control the shared photo '. Therefore, they can better understand what is the purpose of our proposed system and behave more rationally. No matter which type of games they are in, the participants were asked to finish surveys before and after the games. The survey before a game asks some general questions about themselves and their experiences and feelings towards photo sharing and tagging in OSNs. The survey after a game asks why a participant makes certain choices in the game.

For both types of games, we did not use actual photos, because they may introduce privacy violations. Also, we did not leverage the real-world social network platforms, since it is hard to force all people in specific photos to take part in our games simultaneously. Instead, our current games use imaginary scenes by describing a photo to the participants and explaining them that this photo is shared through a social networking site and s/he is tagged in it. Since each participant's sensitivity levels, which are associated with their personalities and other factors, for different photos may be different, we designed several storylines of photos, for which we believe may enable participants to make different choices. The storyline of each photo describes: 1) who are in the photo; 2) where they are; and 3) what they are doing. The storylines are carefully designed so that each involved individual is to be equal in position. The complete storylines used in our games are listed in Table 1.

For the multiple-round games, in each round, each participant is asked to specify a sensitivity level of an imaginary photo based on our description of the photo content. In order to make the participants a more intuitive understanding of the concept of sensitivity level, they are allowed to choose a value between 0.1 and 1, where 0.1 denotes 'the photo is not sensitive to me at all and I want to share it with the public', 0.4 denotes 'the photo is kind of sensitive and I want to share it with my friends', 0.7 denotes 'the photo is very sensitive and I only share it with my close friends', 1 denotes 'the photo is extremely sensitive and I hope only tagged people can see it', and the other numbers denote more fine-grained levels accordingly. The participants are also told that, after everyone specifies her/his sensitivity level, the average of the imputed sensitivity levels is leveraged for making the final decision of photo sharing. Then, we compute the average of sensitivity levels, which is also a number between 0.1 and 1. The number is additionally rounded to the nearest tenth and its corresponding meaning is presented to the participants, where 0.1 denotes 'the photo will be public' and 1 denotes 'only tagged people can see this photo'. Each game con-

**Table 1: Storylines of the Imaginary Photos**

| Number | Storyline |
|---|---|
| 1 | This is a photo about you and your colleagues working in the office |
| 2 | This is a photo about you and your classmates in the commencement |
| 3 | This is a photo about you and your family members in the commencement |
| 4 | This is a photo about you having drinks with your friends in a party |
| 5 | This is a photo about you having drinks with strangers in a bar |




(a) 4 Participants, Storyline = 1 (b) 4 Participants, Storyline = 1 (c) 3 Participants, Storyline = 1

(d) 3 Participants, Storyline = 2 (e) 4 Participants, Storyline = 2 (f) 3 Participants, Storyline = 3

(g) 3 Participants, Storyline = 4 (h) 3 Participants, Storyline = 4 (i) 3 Participants, Storyline = 5

(j) 4 Participants, Storyline = 5 (k) 3 Participants, Storyline = 5

**Figure 4: Multiple Round Game Results. Each game continues for at most 10 rounds or stops when an equilibrium has been reached.**

tinues for at most 10 rounds or terminates when an equilibrium has been reached.

For the single-round games, we first describe a photo to all the participants as same as the multiple-round game and ask all the participants to set their sensitivity levels. After that, instead of giving them an average of sensitivity levels, they are told how many of their friends and non-friends can view the photo at that moment. We provide one of the three different scenarios, which are 1) 30 friends and 10 non-friends, 2) 20 friends and 20 non-friends, and 3) 10 friends and 30 non-friends, to the participants in each game. Then, each of them has one chance to change her/his sensitivity level of the photo. No further feedback is shown to the participants.

We invited 20 participants who are all students in our institution to take part in our user studies. We divided participants into several groups where all group members know each other in a social network. All games were played by participants in person and they were not allowed to interact with other participants directly. We played MRG 11 times and SRG 5 times, and obtained survey results from all participants. Even though we have conducted limited number of experiments and the participants in the games may share similar background, their tendencies could still provide us significant insights into users' decision making in our games.

### 4.2.2 *User Study Results and Findings*

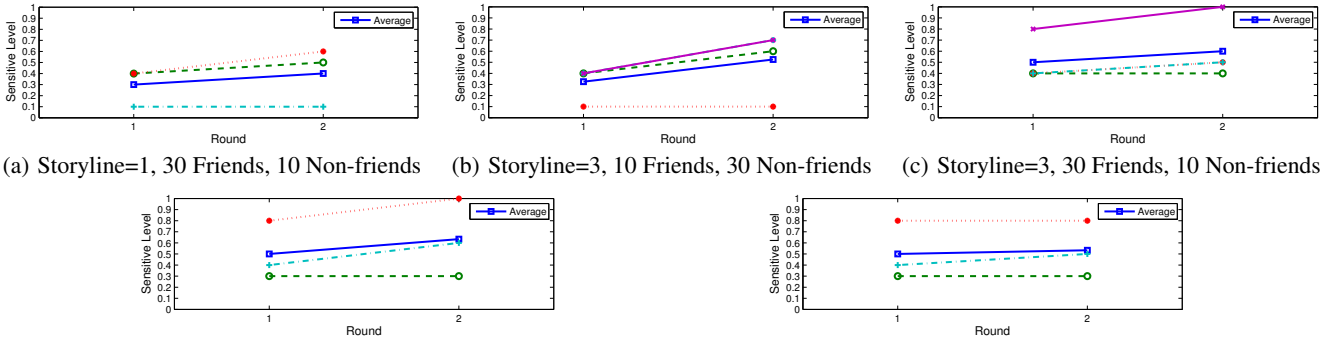
We now present the user study results and our findings based on participants' choices and survey answers. The results of MRG and SRG are depicted in Figures 4 and 5, respectively.

***Finding 1:*** **Users agree that everyone in a photo should have the right to decide who can view it.**

According to the participants' answers on 'Do you believe all the people in a photo that is posted in an online social network should give a say about who can view it?', 100% participants in our studies believe so and they are not satisfied with the current options for photo sharing and tagging in Facebook and Google+. A more detailed question revealed that 27% participants allow their friends to tag them without their approvals, another 55% participants allow friends to tag them but sometimes remove those tags, 9% participants only allow tagging with their approvals, and another 9% participants never allow friends to tag them.

***Finding 2:*** **Games reach an equilibrium in a timely manner.**

As shown in Figure 4, 8 out of 11 multiple-round games reached an equilibrium in only three rounds in our experiments, which indicates that a game-based multiparty control approach as proposed in this paper could produce acceptable results for all participants in a timely manner. Even though users' choices may not always follow




(a) Storyline=1, 30 Friends, 10 Non-friends (b) Storyline=3, 10 Friends, 30 Non-friends (c) Storyline=3, 30 Friends, 10 Non-friends

(d) Storyline=5, 10 Friends, 30 Non-friends (e) Storyline=5, 20 Friends, 20 Non-friends

**Figure 5: Single Round Game Results. Participants have only one chance to change their sensitivity levels after the initial settings.**

the best strategy in terms of our game theoretic analysis, we found that our game-based approach could help all the people in a photo to collaboratively control who can view the picture.

***Finding 3:*** **A user' sensitivity level settings are highly related to the content of photos.**

When we asked if a user cares more about sharing with friends or forbidding non-friends to view a photo, 55% participants replied that it depends on the photo. Another 27% participants answered they care more about their privacy. We computed the average sensitivity levels for all users' inputs on each photo storyline. Storyline 2 received the lowest average sensitivity level that is 0.24. Most participants believe such a photo is not so sensitive and they agree to share it with some strangers. Storyline 4 got the highest average sensitive level which is 0.66. Most participants only want to share such a photo with their close friends.

***Finding 4:*** **Users tend to change their sensitivity levels in order to make the averages closer to their expected sensitivity levels.**

According to the survey answers, 50% participants in our games claim that they have the experiences to change their sensitivity levels to make the averages closer to their own original sensitivity levels and attempt to maximize their own benefits. Such behaviors are consistent with what our game theoretic model predicts. We computed the number of such changing behaviors in our collected data. If the multiplication of a user's current sensitivity level setting minus her/his last round setting and the average of last round minus his/her current setting is negative, denoted as $(sl_{now} - sl_{last}) \times (average_{last} - sl_{now}) < 0$, we say this change is towards her/his own sensitivity level instead of the average. In our collected data, 18.6% sensitivity level changes belong to this category, which is an evidence that users' behaviors do follow our game theoretic patterns in some cases.

***Finding 5:*** **Sometimes users may not adopt the best strategies when making decisions.**

To measure whether a sensitive level change is towards the average of last round or other directions, we used the criteria that the multiplication of a user's current sensitivity level setting minus her/his last round setting and the average of last round minus her/his current setting is positive, denoted as $(sl_{now} - sl_{last}) \times (average_{last} - sl_{now}) > 0$, to indicate such cases. It turns out 28.3% sensitivity level changes fall into this category. Based on the survey answers and in-person discussions with the participants, we observed several reasons behind such human behaviors:

- *Reason 1: Users may not always maximize their own benefits without respecting others' benefits.* Some participants indicated that the average sensitivity levels received from the last round made them reconsider their own choices. And they were willing to change their sensitivity levels towards the last averages, because such behaviors show their respects to their peers.
- *Reason 2: Users seem to be honest and use our system more for the negotiation than the manipulation.* Our game theoretic model suspects that users may choose more extreme sensitivity values to make the averages closer to their expectations. In those cases, the sensitivity values chosen by users may not reflect their true sensitivity levels of the shared photos. Even though, as discussed in Find 3, such behaviors did exist and 50% participants did admit they had such experiences in the games, we found the participants were unwilling to manipulate the system by deviating from their expected sensitivity levels. Two evidences support such a conclusion based on our survey: 1) 60.0% participants said their sensitivity value settings always reflect their true sensitivity values; and 2) 53.2% sensitivity value settings are consistent with the previous setting values, which indicates participants would rather stick to what they have initially chosen.
- *Reason 3: Users care more about others' privacy protection than their own data sharing*. In most cases, users who chose low sensitivity values tended to increase their sensitivity levels to reach agreements with others. Participants showed strong tendencies with this pattern, because they believed respecting others' privacy concerns is more important than maintaining their own sharing intentions. In our collected data, 85% average sensitive levels are increased from the last rounds.

In summary, our user studies showed that our game theoretic model could capture many features of the human decision making process in multiparty access control systems. However, the proposed model still needs to be refined. Especially, we should consider more fine-grained quantification of utility gain and loss in our model with respect to some other aspects, such as peers' privacy concerns, for more accurate analysis of user behaviors in multiparty access control.

## 5. RELATED WORK

Several access control schemes for OSNs have been introduced (e.g., [10, 11, 16, 17, 24]). Carminati et al. [10] introduced a rust-based access control model, which allows the specification of access rules for online resources, where authorized users are denoted in terms of the relationship type, depth, and trust level between users in OSNs. They also introduced a semi-decentralized discretionary access control model and a related enforcement mechanism

for controlled sharing of information in OSNs [11], and proposed a semantic web based access control framework for social networks. Fong et al. [17] presented an access control model that formalizes and generalizes the access control mechanism implemented in Facebook, admitting arbitrary policy vocabularies that are based on theoretical graph properties. Carrie [12] claimed relationship-based access control as one of new security paradigms that addresses unique requirements of Web 2.0. Then, Fong [16] formulated this paradigm called a Relationship-Based Access Control (ReBAC) model that bases authorization decisions on the relationships between the resource owner and the resource accessor in an OSN. However, none of these work could accommodate privacy control requirements with respect to the *collaborative* data sharing in OSNs.

The need of collaborative management for data sharing, especially photo sharing, in OSNs has been addressed by some recent research [8, 20, 25, 34, 36]. Also, game theory as a rich set of mathematical tools has been used to model and analyze the interactions of agents in security and privacy problems [5, 6, 13, 18, 19, 29, 32, 33]. Alpcan *et al.* [6] introduced a game theoretic model to study the evolution of trust for digital identity in online communities. Chen *et al.* [13] presented a weighted evolutionary game-theoretic model to study the behavior of users in OSNs regarding how they choose their privacy settings. In particular, Squicciarini *et al.* [34] proposed a solution for collective privacy management for photo sharing in OSNs that adopted Clarke-Tax mechanism [14] to enable the collective enforcement of privacy preferences and game theory to evaluate the scheme. However, the auction process adopted in their approach indicates only the winning bids could finally determine who was able to access the data, instead of accommodating all stakeholders' privacy preferences. In contrast, we propose a simple but flexible mechanism for collaborative management of shared data in OSNs. And game theory is leveraged in this paper to model and analyze the strategic interaction of users in multiparty access control.

Measuring privacy risk in OSNs has been recently addressed by several work [7, 26, 35]. Becker *et al.* [7] presented *PrivAware*, a tool to detect and report unintended information loss through quantifying privacy risk associated with friend relationship in OSNs. Talukder *et al.* [35] discussed a privacy protection tool, called *Privometer*, which can measure the risk of potential privacy leakage caused by malicious applications installed in the user's friend profiles and suggest self-sanitization actions to lessen this leakage accordingly. Liu *et al.* [26] proposed a framework to compute the privacy score of a user, indicating the user's potential risk caused by her/his participation in OSNs. Their solution also focused on the privacy settings of users with respect to their profile items. Compared with those work, the multiparty access control can help measure the privacy risk caused by different privacy concerns from multiple users.

# 6. DISCUSSION AND FUTURE WORK

As we have discussed before, our game theoretic model should be enhanced to consider more fine-grained quantification of utility gain and loss for accurate analysis of user behaviors. In addition, the current utility function in our model only captures the privacy setting adjustment through changing the sensitivity level of shared data item, and the utility gain and loss with respect to trusted and untrusted accessors of each controller. Further development of our game theoretic model will be investigated to better reflect reality and capture more sophisticated factors, such as accessor space changes for adjusting privacy settings, controllers' general privacy concerns, and trust levels of accessors, which may also significantly influence user behaviors in multiparty access control. Besides, we will study other alternative game theoretic approaches [29] for formulating our game model.

We will also conduct more extensive user studies of the multiparty control game to analyze the strategic interactions of users in *real-world* social network platforms, considering a variety of factors, such as the numbers of trusted/untrusted accessors in conflicting segments, different trust levels of accessors and controllers, and different relationships among controllers. Those experimental studies can additionally articulate the *gap* between game theoretic approaches and real human behaviors [9], and potentially help us capture some missing aspects of our game-theoretic model.

Another issue for multiparty privacy control is that a group of users could *collude* with one another so as to manipulate the final decision. Consider an attack scenario, where a set of malicious users may want to make a shared photo available to a wider audience. They could collude with each other to assign a very low sensitivity level for the photo and specify policies to grant a wider audience to access the photo. We will also investigate a game theoretic mechanism to tackle collusion activities in multiparty privacy control in OSNs with the consideration of the proposed approaches in the recent work [23, 30, 38].

# 7. CONCLUSION

In this paper, we investigated the problem of analyzing the strategic behavior of rational controllers in multiparty access control, where each controller aims to maximize her/his own benefit by adjusting her/his privacy setting in collaborative data sharing in OSNs. We formulated such a problem as a multiparty control game and proved the existence of unique NE of this game. In addition, we introduced interactive update algorithms to compute the NE. Moreover, a numerical analysis was provided for several scenarios that illustrate the interplay of controllers in multiparty access control in OSNs. We further carried out user studies of the multiparty control game to examine the gap between game theoretic approaches and real human behaviors. We believe our game theoretic analysis and additional insights gained from this study would help identify important implications in designing the enhanced multiparty access control systems in OSNs.

# Acknowledgments

The work of H. Hu, G.-J. Ahn and Z. Zhao was partially supported by the grants from National Science Foundation (NSF-IIS-0900970 and NSF-CNS-0831360) and Department of Energy (DE-SC0004308).

# 8. REFERENCES

[1] Facebook Privacy Policy. `http://www.facebook.com/policy.php/`.

[2] Facebook Statistics. `http://www.statisticbrain.com/facebook-statistics/`.

[3] Google+ Privacy Policy. `http://http://www.google.com/intl/en/+/policy/`.

[4] The State of Social Media 2011: Social is the new normal, 2011. `http://www.briansolis.com/2011/10/state-of-social-media-2011/`.

[5] T. Alpcan and T. Başar. *Network security: A decision and game-theoretic approach*. Cambridge University Press, 2010.

[6] T. Alpcan, C. Örencik, A. Levi, and E. Savaş. A game theoretic model for digital identity and trust in online communities. In *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pages 341–344. ACM, 2010.

[7] J. Becker and H. Chen. Measuring privacy risk in online social networks. In *Proceedings of the 2009 Workshop on Web*, volume 2. Citeseer.

[8] A. Besmer and H. Richter Lipford. Moving beyond untagging: Photo privacy in a tagged world. In *Proceedings of the 28th international conference on Human factors in computing systems*, pages 1563–1572. ACM, 2010.

[9] C. Camerer. *Behavioral game theory: Experiments in strategic interaction*. Princeton University Press, 2003.

[10] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, pages 1734–1744. Springer, 2006.

[11] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security (TISSEC)*, 13(1):1–38, 2009.

[12] E. Carrie. Access Control Requirements for Web 2.0 Security and Privacy. In *Proc. of Workshop on Web 2.0 Security & Privacy (W2SP)*. Citeseer, 2007.

[13] J. Chen, M. R. Brust, A. R. Kiremire, and V. V. Phoha. Modeling privacy settings of an online social network from a game-theoretical perspective. In *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*, pages 213–220. IEEE, 2013.

[14] E. Clarke. Multipart pricing of public goods. *Public choice*, 11(1):17–33, 1971.

[15] C. B. et al. The power of social networking in medicine. *Nature biotechnology*, 27(10):888–890, 2009.

[16] P. Fong. Relationship-Based Access Control: Protection Model and Policy Language. In *Proceedings of the First ACM Conference on Data and Application Security and Privacy*. ACM, 2011.

[17] P. Fong, M. Anwar, and Z. Zhao. A privacy preservation model for facebook-style social network systems. In *Proceedings of the 14th European conference on Research in computer security*, pages 303–320. Springer-Verlag, 2009.

[18] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes. On non-cooperative location privacy: a game-theoretic analysis. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 324–337. ACM, 2009.

[19] J. Grossklags, N. Christin, and J. Chuang. Secure or insure?: a game-theoretic analysis of information security games. In *Proceedings of the 17th international conference on World Wide Web*, pages 209–218. ACM, 2008.

[20] H. Hu and G. Ahn. Multiparty authorization framework for data sharing in online social networks. In *Proceedings of the 25th annual IFIP WG 11.3 conference on Data and applications security and privacy*, DBSec'11, pages 29–43. Springer, 2011.

[21] H. Hu, G. Ahn, and J. Jorgensen. Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference*, ACSAC'11, pages 103–112. ACM, 2011.

[22] H. Hu, G. Ahn, and J. Jorgensen. Multiparty access control for online social networks: model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, 15(7):1614–1627, 2013.

[23] H. Kargupta, K. Das, and K. Liu. Multi-party, privacy-preserving distributed data mining using a game theoretic framework. *Knowledge Discovery in Databases: PKDD 2007*, pages 523–531, 2007.

[24] S. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, and H. Choi. D-FOAF: Distributed identity management with access rights delegation. *The Semantic Web–ASWC 2006*, pages 140–154, 2006.

[25] A. Lampinen, V. Lehtinen, A. Lehmuskallio, and S. Tamminen. We're in it together: interpersonal management of disclosure in social network services. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, pages 3217–3226. ACM, 2011.

[26] K. Liu and E. Terzi. A framework for computing the privacy scores of users in online social networks. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 5(1):6, 2010.

[27] T. Lohman. Federal government embracing gov 2.0. *Computerworld*, 2011.

[28] M. Madejski, M. Johnson, and S. Bellovin. The Failure of Online Social Network Privacy Settings. Technical Report CUCS-010-11, Columbia University, NY, USA. 2011.

[29] M. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. Hubaux. Game theory meets network security and privacy. *ACM Computing Survey*, 45(3), 2013.

[30] D. Niyato and E. Hossain. Competitive pricing for spectrum sharing in cognitive radio networks: Dynamic game, inefficiency of nash equilibrium, and collusion. *Selected Areas in Communications, IEEE Journal on*, 26(1):192–202, 2008.

[31] M. Osborne. *An introduction to game theory*, volume 3. Oxford University Press New York, NY, 2004.

[32] A. C. Squicciarini and C. Griffin. An informed model of personal information release in social networking sites. In *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, pages 636–645. IEEE, 2012.

[33] A. C. Squicciarini, C. Griffin, and S. Sundareswaran. Towards a game theoretical model for identity validation in social network sites. In *Privacy, security, risk and trust (PASSAT), 2011 ieee third international conference on and 2011 ieee third international conference on social computing (SocialCom)*, pages 1081–1088. IEEE, 2011.

[34] A. C. Squicciarini, M. Shehab, and F. Paci. Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*, pages 521–530. ACM, 2009.

[35] N. Talukder, M. Ouzzani, A. Elmagarmid, H. Elmeleegy, and M. Yakout. Privometer: Privacy protection in social networks. In *Proceedings of 26th International Conference on Data Engineering Workshops (ICDEW)*, pages 266–269. IEEE, 2010.

[36] K. Thomas, C. Grier, and D. Nicol. unFriendly: Multi-party Privacy Risks in Social Networks. In *Privacy Enhancing Technologies*, pages 236–252. Springer, 2010.

[37] S. Weglage. How it professionals are using social media. *IT World*, 2010.

[38] Y. Wu, B. Wang, K. Liu, and T. Clancy. A scalable collusion-resistant multi-winner cognitive spectrum auction game. *Communications, IEEE Transactions on*, 57(12):3805–3816, 2009.