ICST Transactions on Collaborative Computing Research Article ICST.ORG

A Game Theoretic Approach for Modeling Privacy Settings of an Online Social Network

Jundong Chen*, Ankunda R. Kiremire, Matthias R. Brust, and Vir V. Phoha

Center for Secure Cyberspace, Louisiana Tech University, Ruston, LA 71270, USA

Abstract

Users of online social networks often adjust their privacy settings to control how much information on their profiles is accessible to other users of the networks. While a variety of factors have been shown to affect the privacy strategies of these users, very little work has been done in analyzing how these factors influence each other and collectively contribute towards the users' privacy strategies.

In this paper, we analyze the influence of attribute importance, benefit, risk and network topology on the users' attribute disclosure behavior by introducing a weighted evolutionary game model.

Results show that: irrespective of risk, users are more likely to reveal their most important attributes than their least important attributes; when the users' range of influence is increased, the risk factor plays a smaller role in attribute disclosure; the network topology exhibits a considerable effect on the privacy in an environment with risk.

Received on 14 February 2013; accepted on 23 March 2014; published on 27 May 2014

Keywords: game theory, social network, privacy settings, network topology

doi:10.4108/cc.1.1.e4

1. Introduction

Online social networks provide platforms for people to share information about themselves, which facilitates the establishment and enhancement of friendships between users [20]. However, the shared information can also be exploited by identity thieves, sexual predators, stalkers, etc., and this has triggered worldwide concern about privacy issues in online social networks.

Thus, users of online social networks face a dilemma: reveal more personal information to increase their chances of finding potential new friends and identifying old friends, or reveal less information to decrease the chance of their identities being inferred by unscrupulous characters. Therefore, each user weighs both the risk and benefit to determine how many profile attributes to reveal. Additionally, the privacy settings of other users potentially affect the choice of privacy settings for a user.

Little work has been done on investigating how these factors collectively influence users' privacy settings. Therefore, it is important to develop a model based on interaction of users that captures the influence of privacy risk and relationship-building on the level of self-disclosure.

In this paper, we propose an evolutionary game-theoretic model to study the behavior of users with regard to their privacy settings in a possible online social network. Our study conducts simulations of user behavior in a variety of network topologies, which include random, small-world, scale-free and Facebook friend networks.

The main contribution of this paper is threefold. First, our model investigates the importance of the revealed and/or hidden attributes to the users' behavior. By weighting the attributes, we consider that some attributes may have a higher impact than others in self-disclosure. As an illustration, given Alice is a user in a social network, our model investigates whether her decision to reveal important attributes (such as religion and sexual preferences) would affect other users' revelation decisions more or less than revealing her less important attributes (such as her favorite movies). Second, our model helps us to explore the users'

*Corresponding author. Email: jdc074@latech.edu

attribute disclosure behavior from different ranges of influence. For instance, how do risk and benefit affect Alice if she only discloses her attributes to her friends, as opposed to disclosing them to her friends as well as the friends of her friends? Third, our model allows us to investigate what influence the network topology has on the privacy strategy of the user. For example, if Alice decided to reveal all her attributes in a social network exhibiting small-world characteristics, would she make the same decision if the network exhibited random graph characteristics instead?

The results show that users tend to reveal their most important attributes more than their least important attributes regardless of the risk level. Important attributes are defined as the attributes which have a larger impact on the *social capital* of a user [6]. We also find that the range of influence plays a bigger role than the risk factor in users' disclosure of profile attributes. Additionally, we discover that network topologies have a higher impact on the users' attribute disclosure in the risk-included cases than they do in the risk-free cases.

The provided models and the gained results can be used to understand the influence of different factors on users' privacy choices and help users in determining how to optimize their disclosure strategies in a network while keeping the privacy risk at a low level.

The remainder of this paper is as follows. We discuss related work in the next section and specify the system model, definitions and strategies in Section 3. Our game-theoretic approach is described in Section 4, the results are presented in Section 6, and we conclude this paper with a discussion in Section 7.

2. Related work

Researchers have been studying the motivation of users to disclose their personal information in online social networks for sometime. Spiekermann et al. find that *Relationship-building* and *platform enjoyment* are the factors that motivate users' *self-disclosure* [12]. Aiello et al. show that people with higher similarity are more likely to be friends [13]. They identify similarity between users' profile attributes as an important factor in predicting the existence of a friendship between those users. It follows that if users reveal more attributes, there is an increased chance of sharing common attributes with other users and consequently becoming friends with them.

Game theory is the analysis of situations involving conflicts of interest using mathematical models [18]. Each participant is referred to as a player, and each player has a set of possible strategies they can employ to achieve their goals. Each player's utility is jointly determined by the strategies chosen by all the players in the game. Game theory is a growing field that has been applied to many areas including various aspects of online social networks. These aspects range from modeling network formation [10], to community detection [5], and discovering influential nodes [16].

Game theory has been applied to optimizing users' data sharing in online social networks. Kamhoua et al. propose a Markov game theoretic approach to help online social network users determine their optimum data sharing policy [9]. Squicciarini et al. design a model to facilitate users' management of shared data based on Clarke-Tax mechanism [22].

Game theory has also been employed to model personal information revelation in online social networks. Squicciarini et al. [23] conduct a survey to investigate the factors that affect the behavior of personal information revelation, and then use a game theoretic model to find out the dynamics of the revelation behavior. Their results show that close friends strongly influence users' revelation decisions.

The profile attribute privacy problem is similar to the classic *stag-hunt* game [21]. The stag-hunt game models a conflict between safety and cooperation. In the game, two hunters can either jointly hunt a stag or individually hunt a hare. The highest benefit can only be achieved through cooperatively hunting a stag. In contrast, a hunter is exposed to the highest risk if he decides to hunt a stag while the other hunter decides otherwise. This game is very similar to the situation that online social network users encounter while disclosing their profile attributes. The highest benefit accrues when both users reveal all their attributes. The highest risk occurs to a user when the other user reveals less attributes because the user with more revealed attributes is vulnerable to identify inference.

The approach presented in our paper is built upon evolutionary game theory on graphs. Szabó et al. review different types of evolutionary games on different structure of graphs [24]. Antonioni et al. employ the model of evolutionary game on graphs to investigate the cooperation in social networks [1].

In previous work, we apply weighted evolutionary game theoretic model to analyze users' behavior in profile attribute disclosure in an online social network [4]. The model is employed on three different network topologies, where we show that the disclosure of profile attributes is not only influenced by attribute importance but network connectivity as well.

In this work, we extend our previous work in a variety of ways. We investigate how an increase in the influential range affects the users' privacy strategies, by considering friends-of-friends in the utility function. Furthermore, we apply our model to actual Facebook friend networks and report more comprehensive results.

3. Preliminaries

This section contains fundamental assumptions, concepts, definitions and methods used throughout the paper.

3.1. Assumptions

We assume that users with more attributes in common are more likely to be friends. This assumption is based on the *homophily principle* exhibited in social networks [15]. Additionally, we assume that all users of the network attach the same importance to the same type of attribute, e.g. all users will attach higher importance to their address attribute than to their religion attribute.

These assumptions make it possible for us to investigate the influence of local properties such as profile attributes and their importance to users on a common ground while simultaneously exploring how global network properties affect users' privacy.

3.2. Risk and identity inference

To capture the risk of identity inference, we introduce the concept of *hiding*. A User x is *hidden* by another User y if y is more distinguishable than x. This happens when User x's attributes are a subset of User y's attributes. For example, if a user John Doe reveals a set of attributes $\{Doe, 25\}$ while another user Jane Doe reveals $\{Doe, Female, 25, Chicago\}$, then Jane is more distinguishable than John. Therefore, John is hidden by Jane. This is because a third party can more easily infer the identity of Jane than John given a set of revealed profile attributes. As a result, the risk to John Doe's identity is reduced by Jane Doe.

3.3. Privacy settings

The *privacy setting* is a configuration of the user's profile information, which allows the user to enable or disable the visibility of specific profile attributes to other network users. The privacy settings of a typical social network consist of different levels of visibility for different aspects of the users' profile. The aspects include profile attributes, activity logs, and friend lists while the levels of visibility include friends, friends of friends, and public. In our model, we only consider profile attributes and two levels of visibility, i.e. friends and friends of friends.

3.4. Network topologies

We examine the behavior of our model on five network topologies, which include a random network, a small-world network, a scale-free network, and two Facebook friend networks. In these topologies, a node represents a social network user while an edge between two nodes indicates that the two users are "friends". Friends of a user represent other network users who have direct access to that user's revealed attributes.

A *random network* is a graph where an edge occurring between two nodes follows a probability distribution [28]. As in [17], random graphs have been used for modeling social networks when the node degrees follow an appropriate probability distribution. The Erdös-Rényi (ER) [7] model is one of the models that can generate such random networks. Given n nodes, and that each edge occurs between two nodes with independent probability p, the average node degree k is approximately $n \cdot p$.

In a *small-world network*, each node is connected to every other node by a relatively small number of intermediate nodes, even though most of the nodes are not directly connected to each other. Online social networks have been shown to exhibit small-world properties and can be created by using a Watts-Strogatz model [25].

A *scale-free network* is a network where node degree distribution follows a power-law, i.e. the number of nodes decreases exponentially as the node degree increases [2]. To generate the scale-free network, seed nodes are placed within the network, then new nodes are added to the existing network incrementally following the principal of preferential attachment [2].

The Facebook friend networks considered in this work are networks constructed from actual Facebook profiles. The nodes of a Facebook friend network represent all the friends of that Facebook user. An edge between two nodes indicates that the two users are friends with each other on top of being friends with the principal user. *Mathematica* provides a *SocialMediaData* function to build such a Facebook friend network for any Facebook user [14, 26, 27].

4. Our approach

We present a weighted evolutionary game to investigate the influence of attribute importance (weight) and network topology on the social network users' behavior in profile attribute disclosure.

Nowadays, there are many online social networks with a variety of designs for their privacy settings [8]. In this paper, we model a possible social network with characteristics exhibited by some of the online social networks in existence. For example, our social network and game model consists of users, each of whom owns a profile comprised of profile attributes and is allowed to select how many and which attributes to reveal to friends or *friends-of-friends* in the network. However, we do not consider a user revealing a different set of attributes to different friends, which is a feature of some social networks.

4.1. Our approach: definitions

The definition of our basic social network is as follows.

Definition 1 (Social network). We define a social network as an undirected graph $G = (N, E)$ with node set N and edge set E, where the node set $N = \{1, 2, ..., n\}$ corresponds to n users in the network.

Additionally, we consider that the connectivity pattern of the network can follow the different network types described in the previous section. These networks include random, small-world, scale-free and Facebook friend networks.

Our weighted evolutionary game is implemented on top of this possible social network. The utility of a user is a combination of both *positive utility* and *negative utility*. The positive utility is represented by the summation of the weights of the attribute pairs with each neighbor on the network. On the other hand, the negative utility is represented by the probability of the identity of a user being inferred.

A *strategy* is a set of actions that players can execute. In our approach, the strategy involves selecting which and how many attributes to disclose.

Definition 2 (Privacy settings). The vector $A_x = (a_{x,1}, a_{x,2}, ..., a_{x,m})$ denotes the profile attributes for User x in the social network, where $a_{x,i}$ is his/her i^{th} attribute. The attribute vector A_x has a corresponding weight vector $W = (w_1, w_2, ..., w_m)$. For each User x, a sign flag vector $S_x = (s_{x,1}, s_{x,2}, ..., s_{x,m})$ denotes whether specific attributes are disclosed or revealed. If attribute $a_{x,i}$ is disclosed, then $s_{x,i} = 1$, otherwise $s_{x,i} = 0$.

For example, an attribute vector for a given user Alice, is represented by $A_{Alice} = (Name, Gender, Age, ..., Hometown)$. For simplicity, we assume that all the users have the same set of profile attributes. The sign flag vector $S_{Alice} = (0, 0, 0, ..., 1)$ means that Alice decides to reveal her hometown but withholds her name, gender, and age. We use $Attr\#i$ to represent a specific attribute i.

We use the concept of *pairs* to evaluate the similarities between two users. Two users Alice and Bob are said to have a *pair* if they both reveal the same attribute, e.g. hometown. Formally, a 2-tuple $(a_{x,i}, a_{y,i})$ is called a pair if and only if $s_{x,i} = 1$ and $s_{y,i} = 1$.

Fig. 1 shows a possible profile configuration for two users x and y which exhibits r pairs. Among the m attributes, User x reveals k_x attributes while User y reveals k_y attributes. Attributes $Attr\#1, Attr\#2, ..., Attr\#r$ are revealed by both users, which constitute the r pairs. The pairs are denoted by $(a_{x,1}, a_{y,1})$, $(a_{x,2}, a_{y,2})$, ..., $(a_{x,r}, a_{y,r})$. A higher number of pairs allows for the increased possibility of common ground between users. An increase in common ground leads to an increase in the strength of their friendship

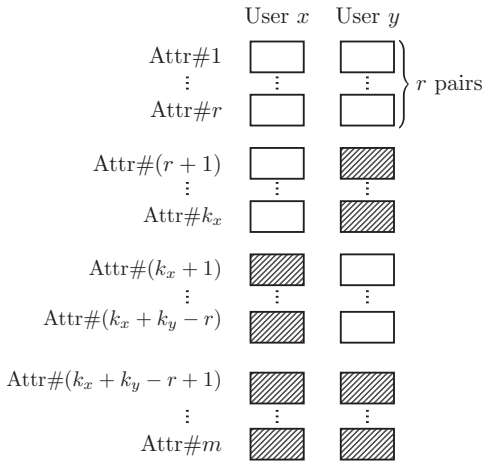


Figure 1. The figure shows a possible profile configuration for two users x and y, who disclose k_x and k_y attributes respectively out of the m possible attributes. The clear rectangles represent the disclosed attributes while the shaded rectangles represent withheld attributes.

[11]. In our case, a friendship is considered stronger if two friends reveal and share more common attributes.

We consider that the benefit and risk are affected by the users at two different levels of social closeness. The first level only includes User x's friends, and the second level also includes User x's *friends-of-friends*. We adopt *influential range* (IR) to represent which level of users contribute to User x's benefit and/or risk.

$$B_x(IR) = \begin{cases} \{F\}, & IR = 1, \\ \{F\} \cup \{FoF\}, & IR = 2, \end{cases} \quad (1)$$

where IR denotes influential range, F represents friend, and FoF stands for friend-of-friend. Therefore, $B_x(1)$ is the set of all the friends. $B_x(2)$ includes not just friends, but also friends-of-friends.

In our game, the utility is a combination of benefits (positive utility) and risks (negative utility). A user's positive utility is related to the amount and type of attributes that that user shares with other users in their influential range. The set of users who contribute to User x's positive utility is denoted by $B_x(IR)$.

Conversely, the risk is the probability of a user's identity being inferred. This probability is measured by the reciprocal of the number of the users who disclose the same or additional attributes, i.e. how many users in the influential range can hide that user. The set $B_x^h(IR)$ consists of users in the influential range who disclose the same attributes as x or extra attributes in addition to those disclosed by User x, and can possibly hide User x. The set $B_x^h(IR)$ determines how much risk a user is exposed to.

The combined utility (payoff) function is obtained by using Equation 2, where w_P and w_N are the weight coefficients for the positive utility $\sum_{y \in B_x(IR)} (S_x \wedge S_y) \times W^T$ and negative utility $\frac{1}{|B_x^h|}$ respectively[1].

$$u_x = w_P \cdot \sum_{y \in B_x(IR)} (S_x \wedge S_y) \times W^T - w_N \cdot \frac{1}{|B_x^h(IR)|} \quad (2)$$

We define the benefit-to-risk ratio (BRR) as $w_P : w_N$, which is the ratio of the coefficient for positive utility to the coefficient for negative utility.

4.2. Our approach: model

Our model is iterative and synchronous. First, each user in the network is assigned a random initial attribute sign flag vector. In every iteration, each user compiles a set of candidate neighbors whose privacy settings they may mimic. This set consists of the neighbors who derive a higher utility from their privacy settings than the user derives from his/her own settings. Based on the neighbors' utilities, each user decides whether to change or maintain their strategy. A user is likely to change his/her strategy if his/her neighbors derive a higher utility from their own strategies than the user derives from his/her own. If a user decides to change his/her strategy, one of the candidate neighbors is then selected as the object to mimic. The mimicking process involves a user changing one digit of their sign flag to the corresponding digit of the candidate neighbor's sign flag. This is analogous to a user Alice deciding to reveal her location attribute after seeing that her friend Bob, who has a higher utility, has a revealed location attribute. At the end of each iteration, all the users update their strategies synchronously. The procedure keeps running iteratively until there are no users who change their sign flags between two consecutive iterations. When this condition has been met, the model is said to achieve convergence.

Formally, users follow the *replicator rule* to update their strategies between two successive time steps [19]. Each node makes a decision to maintain or change its current strategy based on the utilities exhibited by its neighbors. Given u_x^t and u_y^t are the utilities of User x and User y respectively at time t, the probability of User x (at time $t+1$) adopting the strategy of User y (at time t) is given by

$$P_{x,y}^{t+1} = \begin{cases} \frac{u_y^t - u_x^t}{d_{max}}, & u_y^t > u_x^t, \\ 0, & u_y^t \leq u_x^t. \end{cases} \quad (3)$$

[1]Unless otherwise stated, we use notation $\wedge$ to represent logic AND. Notation W^T refers to the transpose of vector W.

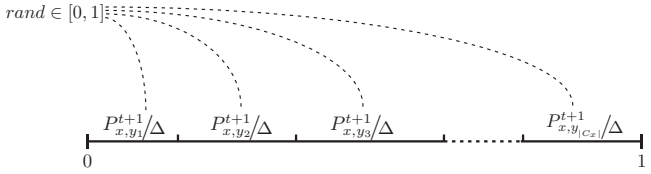


Figure 2. The figure shows the implementation of selecting one of the candidate neighbors as y^* based on the model of *balls into non-uniform bins*, where $C_x = y_1, y_2, ..., y_{|C_x|}$. The probability of selecting neighbor y_i is directly proportional to P_{x,y_i}^{t+1}

We use the largest difference d_{max} in payoff between any two users in the network to guarantee that $P_{x,y}^{t+1} \in [0, 1]$. Equation 3 implies that the probability of User x following the strategy of a neighbor (User y) is proportional to the payoff difference between users x and y, when User y's utility is higher than User x's. This probability value is evaluated for all members of the candidate neighbor set C_x.

Each user's decision to maintain or change his/her strategy depends on $P_{x,y}^{t+1}$ values for the entire candidate neighbor set C_x. The probability of User x maintaining its original strategy, as derived from [19], is given by

$$\overline{Q}_x^{t+1} = \prod_{y \in C_x} (1 - P_{x,y}^{t+1}) \quad (4)$$

Conversely, the probability of User x changing its strategy between t and $t+1$ is given by

$$Q_x^{t+1} = 1 - \prod_{y \in C_x} (1 - P_{x,y}^{t+1}). \quad (5)$$

After evaluating all probabilities and deciding to change his/her strategy, each user selects the neighbor to mimic in the update process. A higher $P_{x,y}^{t+1}$ value for candidate y translates to a higher probability of being selected as the mimic object y^*. The implementation of selecting y^* is based on a mathematical model called *balls into non-uniform bins* [3], in which the probability[2] $P(y_i)$ of a ball falling into a certain bin is proportional to the size of the bin. In Fig. 2, the size of the each bin is exactly equal to $P_{x,y}^{t+1}/\Delta$, where $\Delta = \sum_{y \in C_x} P_{x,y}^{t+1}$. In total, there are $|C_x|$ bins. Therefore, the probability of the ball falling into ith bin is given by

$$P(y_i) = P_{x,y_i}^{t+1}/\Delta \quad (6)$$

After the mimic object is determined, the specific attribute to mimic is randomly selected from the attributes with different sign values.

The algorithm for updating the attribute sign flag is shown in Algorithm 1.

[2]In this paper, we use y to refer to a general user, and we use y_i to refer to a specific user.

Algorithm 1: Algorithm for updating profile attribute sign flag

Input: Initial sign flag iSF
Output: Final sign flag fSF

Assign iSF for each node;
do
  for *each node* **do**
    Find the set of candidate neighbors C_x;
    Evaluate $P_{x,y}^{t+1}$ for all members of candidate set;
    Evaluate probability of changing strategy Q_x^{t+1};
    Generate a random number $rand \in [0, 1]$;
    if $rand < Q_x^{t+1}$ **then**
      /* *Decision is made to change strategy* */
      Select neighbor y^* from C_x;
      /* *Neighbor is selected using balls into non-uniform bins* */
      Change single bit from SF_x to mimic SF_{y^*};
    end
  end
  All nodes update sign flags synchronously;
while *any node changes sign flag*;
return fSF

4.3. Working case for risk-free scenario

In this subsection, we describe a working case of a risk-free scenario of our model, in which the influential range is restricted to a user's friends (neighbors). Fig. 3a shows the topology structure of the network in this example, which consists of 8 users, whose profile attributes and associated weights are shown in Fig. 3b. The profile attributes include (Name, Gender, Age,..., Hometown) with weight vector $(w_1, w_2, w_3, ..., w_7) = (0.02, 0.06, 0.10, 0.14, 0.18, 0.22, 0.28)$. Fig. 3c shows the initial sign flags for all 8 users. For example, User 5 has a sign flag $S_5 = (1100110)$ which means that only his/her name, gender, education and occupation are revealed. In the next few paragraphs, we show how User 5 may change their strategy in our model.

In the first step, every user calculates their utilities from Equation 2. This involves a comparison of the users' revealed attributes with each neighbor. User 5 has two neighbors: User 1 and User 2 with initial sign flags $S_1 = (1000110)$ and $S_2 = (0110011)$ respectively. The attributes pairs between any two users are obtained by using bit-wise AND operation between the users' sign flag vectors. The bit-wise AND operation between S_1 and S_5 is (1000110), which means that both User 1 and User 5 disclosed attributes 1, 5 and 6. The summation of the weights of attribute pairs (Equation 2) is therefore given by $w1 + w5 + w6$, which evaluates to 0.42. Similarly, the summation of the weights of attribute pairs between S_2 and S_5 is 0.28. The positive utility for any user is obtained by summing the weighted pair sums for all his/her neighbors. In this case, the positive utility for User 5 is the sum of the weighted attribute pairs between User 5 and both User 1 and User 2. This evaluates to $0.42 + 0.28 = 0.70$. In a similar fashion, the utilities are evaluated for all the network users. Table 1 shows the positive utilities for Users 5, 1, and 2.

In the second step, each user evaluates the probability $P_{x,y}^{t+1}$ of mimicking his/her neighbors according to Equation 3. The maximum range between the utility values for the network nodes $d_{\max}$ is found to be 1.38. User 5 only has to consider User 1 and User 2 when evaluating these probability values. $P_{5,1}^1$ evaluates to 0.41 while $P_{5,2}^1$ evaluates to 0.49.

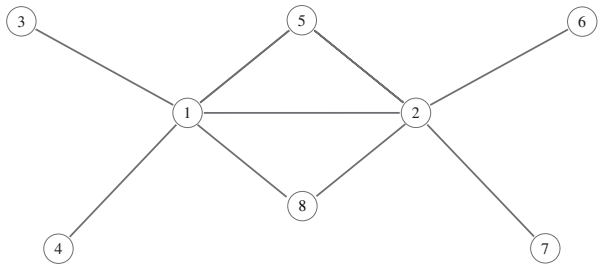
In the third step, each user decides whether to change or maintain his/her strategy by using Equation 5 which utilizes the probabilities evaluated in the step above. For User 5, Q_5^1 evaluates to 0.6991. If a randomly selected number in the range $[0, 1]$ is less than Q_5^1, then User 5 decides to change his/her strategy. Otherwise, User 5 maintains his/her strategy. In our case, User 5 decides to change his/her strategy.

In the fourth step, users who decided to change their strategies select a candidate neighbor to mimic. Candidate neighbors should exhibit higher utility values than the user itself. The probability of User x selecting a specific neighbor y is directly proportional to $P_{x,y}^{t+1}$ for that neighbor. Since Users 1 and 2 both have higher utilities than User 5, they are both viable candidates for User 5 to mimic. After normalizing $P_{5,1}^1$ and $P_{5,2}^1$, the bin sizes for User 1 and User 2 are 0.46 and 0.54 respectively (cf. Equation 6 and Fig. 2). In our case, User 5 selects User 2 as the mimic object.

In the fifth step, each user who decided to change their strategy selects which attribute to reveal or withhold to resemble their mimic object. Comparing User 5 and User 2's sign flags reveals that they differ in four positions, i.e. 1, 3, 5, and 7. User 5 can mimic User 2 in one of the following ways: revealing attribute 3, revealing attribute 7, withholding attribute 1, or withholding attribute 5. In our case, User 5 decides to reveal attribute 7.

All five steps are repeated in each iteration until no single user changes his/her strategy between two successive iterations. The system is then said to have converged.

Fig. 3d shows the sign flags for all 8 users after a single iteration. Fig. 3e shows the sign flags for the whole network after convergence. In this simulation, convergence is achieved after 11 iterations.



(a)

w_1 (0.02)	w_2 (0.06)	w_3 (0.10)	w_4 (0.14)	w_5 (0.18)	w_6 (0.22)	w_7 (0.28)
Name	Gender	Age	Religion	Education	Occupation	Hometown

(b)

Node	w_1	w_2	w_3	w_4	w_5	w_6	w_7
User 1	1	0	0	0	1	1	0
User 2	0	1	1	0	0	1	1
User 3	1	1	0	0	1	0	0
User 4	0	1	0	1	0	0	1
User 5	1	1	0	0	1	1	0
User 6	0	1	0	1	0	1	1
User 7	1	0	1	0	1	0	0
User 8	1	0	0	1	1	1	0

(c)

Node	w_1	w_2	w_3	w_4	w_5	w_6	w_7
User 1	1	0	0	0	1	1	0
User 2	0	1	1	0	0	1	1
User 3	1	0	0	0	1	0	0
User 4	0	1	0	1	0	0	0
User 5	1	1	0	0	1	1	1
User 6	0	1	1	1	0	1	1
User 7	1	1	1	0	1	0	0
User 8	1	0	0	1	0	1	0

(d)

Node	w_1	w_2	w_3	w_4	w_5	w_6	w_7
User 1	0	1	1	0	0	1	1
User 2	0	1	1	0	0	1	1
User 3	1	1	1	0	1	1	1
User 4	0	0	0	1	0	0	1
User 5	0	1	1	0	0	1	1
User 6	0	1	1	0	0	1	1
User 7	0	1	1	0	0	1	1
User 8	0	1	1	0	0	1	1

(e)

Figure 3. (a) A sample network consisting of 8 users connected to each other, (b) each user has a profile with 7 attributes with a weight vector $(w_1, w_2, ..., w_7) = (0.02, 0.06, 0.10, 0.14, 0.18, 0.22, 0.28)$, (c) initial sign flags for all 8 users that indicate which attributes are revealed and which attributes are withheld (a "1" indicates an attribute revealed while a "0" indicates an attribute withheld), (d) after every user compares his strategy with that of his neighbors, every user updates their strategy, (e) the illustrated system converges after 11 iterations and gives the resultant sign flags for all users.

5. Simulations settings

In this section, we describe the underlying simulation settings. The simulations deal with risk-included and risk-free cases of the weighted evolutionary game.

Table 1. The Process of Calculating Payoff Value and Choosing Mimic Object from the Candidate Neighbors.

User	Neighbor	AND result	Weighted result	Positive utility	$P_{x,y}^{t+1}$
User 5	User 1	1000110	$w_1 + w_5 + w_6 = 0.42$	0.70	N/A
	User 2	0100010	$w_2 + w_6 = 0.28$		
User 1	User 2	0000010	$w_6 = 0.22$	1.26	0.41
	User 3	1000100	$w_1 + w_5 = 0.2$		
	User 4	0000000	0		
	User 5	1000110	$w_1 + w_5 + w_6 = 0.42$		
	User 8	1000110	$w_1 + w_5 + w_6 = 0.42$		
User 2	User 1	0000010	$w_6 = 0.22$	1.38	0.49
	User 5	0100010	$w_2 + w_6 = 0.28$		
	User 6	0100011	$w_2 + w_6 + w_7 = 0.56$		
	User 7	0010000	$w_3 = 0.10$		
	User 8	0000010	$w_6 = 0.22$		

Note: Maximum utility max = 1.38
Minimum utility min = 0
Maximum range between any two nodes' utilities $d_{\max} = 1.38$
$(w_1, w_2, ..., w_7) = (0.02, 0.06, 0.10, 0.14, 0.18, 0.22, 0.28)$

The simulation is designed to consider user profiles with 7 attributes ($m = 7$). Each user can choose to reveal or to withhold each of these attributes. A 7-bit flag is assigned to each user, which corresponds to the attributes. For example, the flag 1000110 for User 1 means that Attributes 1, 5 and 6 are revealed while Attributes 2, 3, 4, and 7 are withheld.

We begin by randomly assigning the attribute flag to all users of the network. During each iteration, each user has two options: maintain his/her attribute flag, or change it (by revealing or withholding a single attribute).

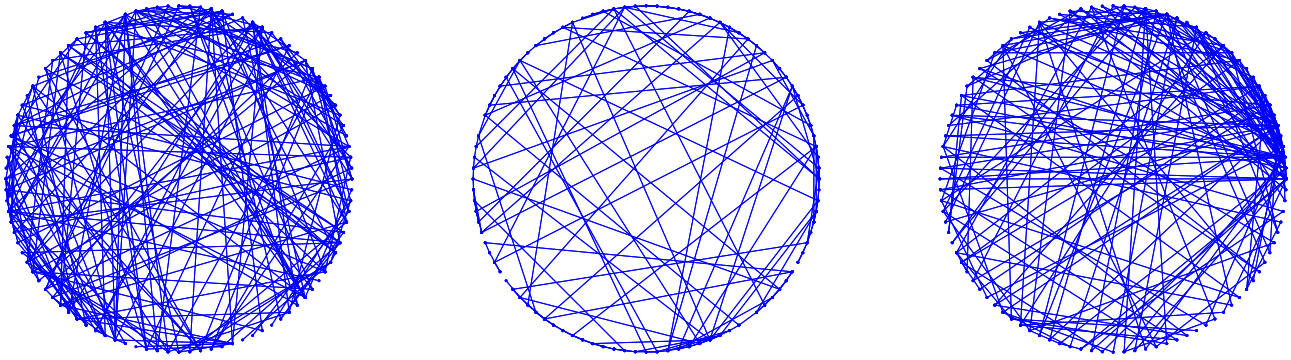
To consider different levels of the risk, we choose 3 different benefit-to-risk ratios (*BRR*s), which are 1 : 0, 1 : 15, and 1 : 30 (cf. Table 2). While all the attributes are assigned to different weights, the weight vector for the attributes is assumed to be the same for each user of the network. Additional simulation settings are shown in Table 2. We run the simulation for each configuration 500 times. After averaging 500 simulation results, we obtain the dynamic curves in each of the considered networks, which include random, small-world, scale-free, and Facebook friend networks.

The size and average node degree for each network are all listed in Table 3.

In Fig. 4, the visualized graphs for the random, small-world, and scale-free networks are shown. The visualized graphs for the Facebook friend networks are depicted in Fig. 5. The Facebook graphs (FB1 and FB2) are obtained using the *SocialMediaData* function in *Mathematica*. Fig. 5a and Fig. 5b are from two different Facebook accounts.

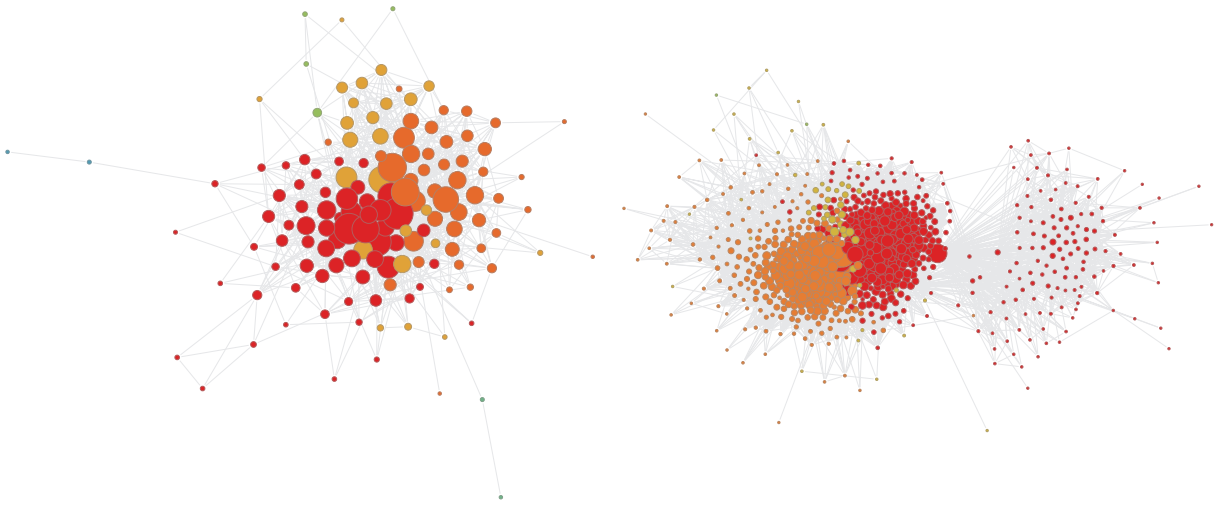
6. Results

In this section, we describe the results derived from simulations of the weighted evolutionary game on a



(a) Random network **(b)** Small-world network **(c)** Scale-free network

Figure 4. The network topologies used in the simulations. The average node degree for each network is 4, and each network includes 100 nodes.



(a) FB1 **(b)** FB2

Figure 5. The Facebook friend networks used in the simulations. Network FB1 and FB2 are comprised of 151 and 502 nodes respectively.

Table 2. Values Assigned to Specific Parameters in order to Obtain the Presented Results

Parameter	Value
m	7
$w_P : w_N$	$1:0, 1:15, 1:30$
W	$(0.02, 0.06, 0.10, 0.14, 0.18, 0.22, 0.28)$

Table 3. The Properties of Networks in the Simulation

Network	Size	Average Node Degree
Random network	100	4
Small-world network	100	4
Scale-free network	100	4
FB1	151	15.0
FB2	502	49.0

random network, a small-world network, a scale-free network and two Facebook friend networks.

The attribute dynamic curves for random network, small-world network, scale-free network, FB1, and FB2 are shown in Fig. 6, Fig. 7, Fig. 8, Fig. 9, and Fig. 10 respectively. Each dynamic curve shows how the proportion of the entire population that discloses any specific attribute changes with time. Each dynamic plot consists of 7 curves corresponding to 7 attributes, *Attr*#1, *Attr*#2, ..., *Attr*#7, which are numbered according to their importance (weight), i.e. *Attr*#7 is the most important attribute, while *Attr*#1 is the least important attribute.

There are 6 sub-figures (Figs. a-f) in each figure. The 3 sub-figures in the left column (Figs. a, c, e) correspond

to the simulation results when we consider the benefit and risk only within the users' friends. The 3 sub-figures on the right side (Figs. b, d, f) correspond to simulation results when we consider both the users' friends and friends-of-friends. The 2 sub-figures in each row have the same benefit-to-risk ratio (*BRR*). The top (Figs. a, b), middle(Figs. c, d) and bottom(Figs. e, f) rows correspond to *BRR* values of 1 : 0, 1 : 15, and 1 : 30 respectively, where (*BRR* = 1 : 0) represents risk-free scenario.

The first observation is a general reduction in attribute revelation with an increase in risk. Consider Fig. 6 which shows the attribute dynamics in a random network: comparing Figs. 6a, 6c, and 6e shows that increasing the risk causes less users to reveal attributes. Fig. 6a shows that over 85% of the population reveal all their attributes by 100 iterations when there is no risk. Introducing risk causes users to reveal less attributes. In fact, Fig. 6e shows that all users withhold all their attributes by 50 iterations when *BRR* = 1 : 30. The small-world, scale-free, and Facebook networks (cf. Figs. 7, 8, 9, and 10) all exhibit similar observations. While this observation might seem intuitive, it provides some form of vindication for our model.

The second observation is that the networks generally exhibit larger drops in attribute revelation when the range of influence is restricted to friends as opposed to when friends-of-friends are also considered. For example, Figs. 7a and 7b show almost identical levels of revelation without risk. However, increasing the risk leads to more attributes withholding in Fig. 7c and 7e than it does in Figs. 7d and 7f. This means that risk plays a more dominant role in attribute disclosure when only the friends of a user are considered.

The third observation is that increasing the users' range of influence generally results in increased levels of attribute revelation. Consider Fig. 8 which captures attribute dynamics in a scale-free network: comparing the left (Figs. 8a, 8c, 8e)and right columns (Figs. 8b, 8d, 8f) shows that maximum revelation is obtained by as early as 40 iterations for all attributes when friends-of-friends are considered (Figs. 8b, 8d, 8f). In contrast, the risk-free scenario with friends (Fig. 8a) only obtains maximum revelation for some of the attributes, while Figs. 8c and 8e do not obtain maximum revelation for any attributes at all. This observation can be attributed to the process of enlarging the influential range. Increasing the range results in an increase in the number of users who can hide any specific user which leads to a reduction in risk. Increasing the range also allows for more users who share the same attributes which leads to an increase in the user's benefit.

The next observation is related to the friends influential range (Figs. a, c, and e). Increasing the risk factor has a larger effect on attribute disclosure in the random and small-world networks than in the scale-free and Facebook networks. Comparing Figs. 6 and 7 to Figs. 8, 9 and 10 shows that *BRR* = 1 : 30 causes complete attribute withholding in the random and small-world networks in contrast to partial attribute withholding in the scale-free and Facebook networks.

The final observation is related to the effect of network topology on attribute disclosure with the range of influence restricted to friends. We find that network topology plays a more considerable effect on the privacy in risk-included scenarios than in a risk-free scenario for the random, small-world, and scale-free networks. Comparing Figs. 6a, 7a and 8a shows that the networks exhibit similar performance in the risk-free environment (*BRR* = 1 : 0). However, comparing Figs. 6c, 7c and 8c as well as Figs. 6e, 7e and 8e shows that the performance is different for different networks. For example, Figs. 6e and 7e show complete attribute withholding while Fig. 8e shows partial attribute disclosure.

7. Conclusions

In this paper, we analyze the behavior of users in a social network regarding how they choose their privacy settings. We model a basic social network and define a game-theoretical model on top of it, in which users are able to adjust their privacy settings according to certain strategy options. In order to make the model more realistic, we include weights corresponding to the importance that users attach to certain attributes.

With the resulting weighted evolutionary game model, we aim to investigate the influence of various factors, such as attribute importance, benefit, risk and network topology, on the privacy settings employed in social networks.

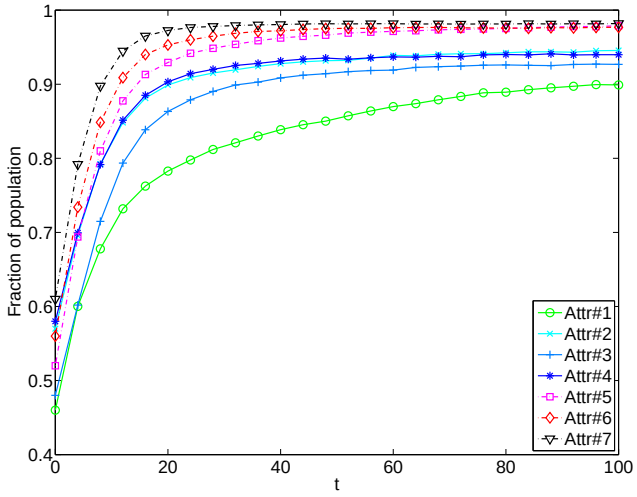
The results show that the most important attributes exhibit higher levels of revelation than the least important attributes. This finding is more evident in random and scale-free networks than in small-world networks.

We also find that increasing the risk exhibits limited effect on the privacy dynamics of the network if we consider the benefit and risk from friends-of-friends. In the Facebook friend networks, which include more users and feature higher average node degree, increasing risk coefficient only slightly affect the level of attribute disclosure.

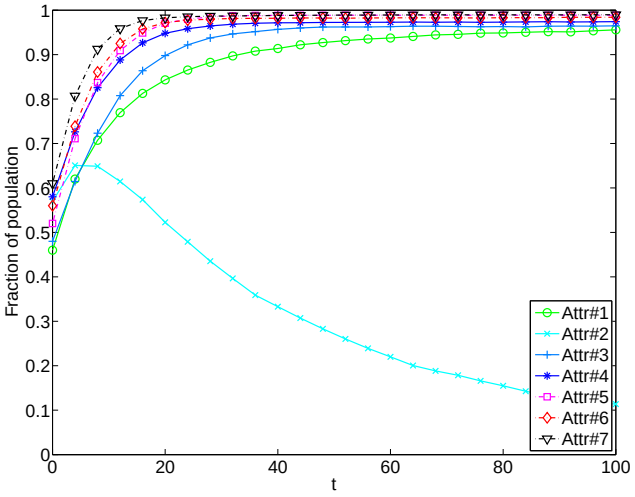
The approach presented in this paper provides an initial approach to study and understand the dynamics of privacy settings in social networks.

Acknowledgment

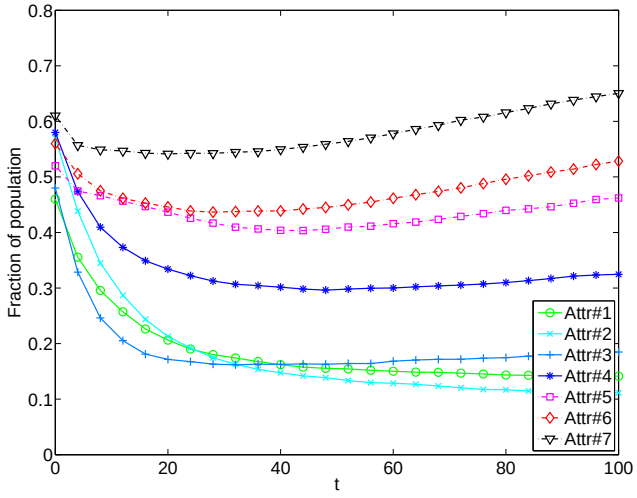
Jungdong Chen expresses his gratitude to Dr. Louis E. Roemer and Alberto Antonioni for their helpful discussions.



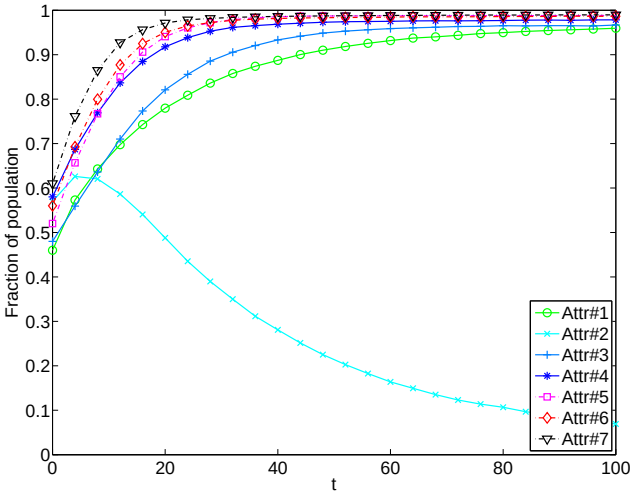
(a) Random network (BRR=1:0, IR={F})



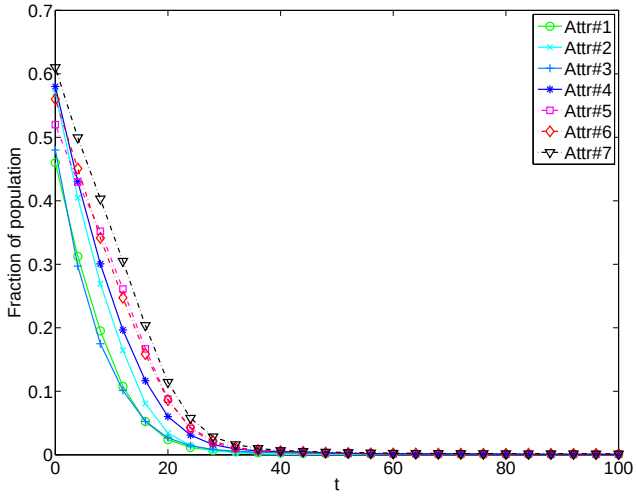
(b) Random network (BRR=1:0, IR={F}∪{FoF})



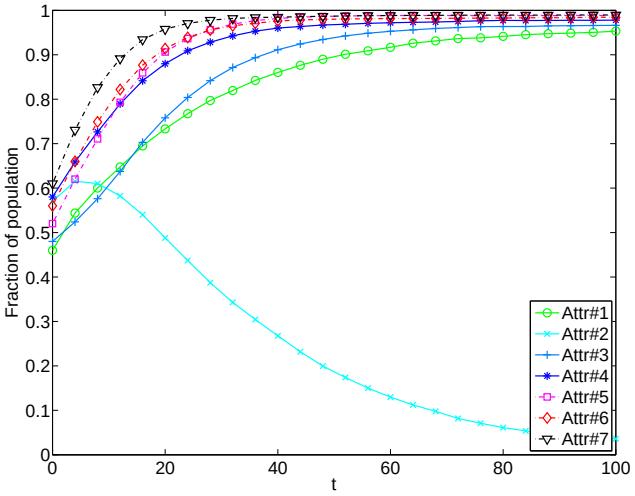
(c) Random network (BRR=1:15, IR={F})



(d) Random network (BRR=1:15, IR={F}∪{FoF})

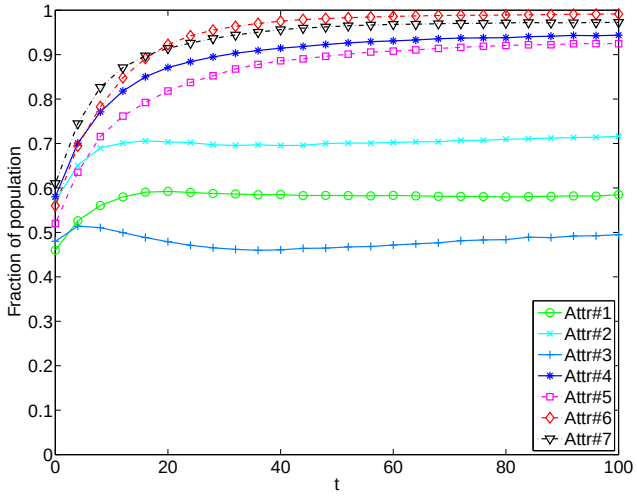


(e) Random network (BRR=1:30, IR={F})

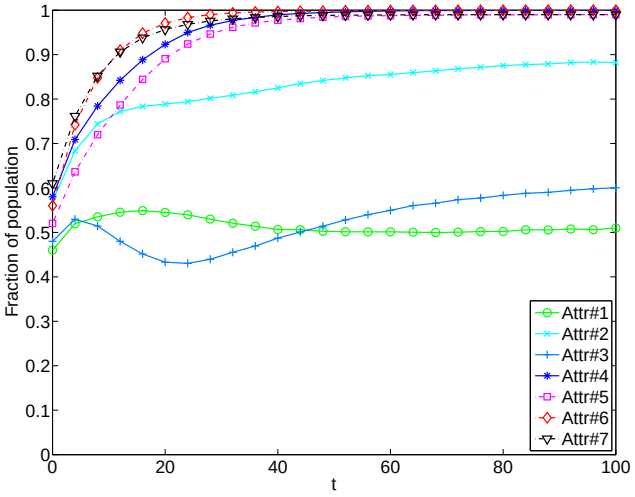


(f) Random network (BRR=1:30, IR={F}∪{FoF})

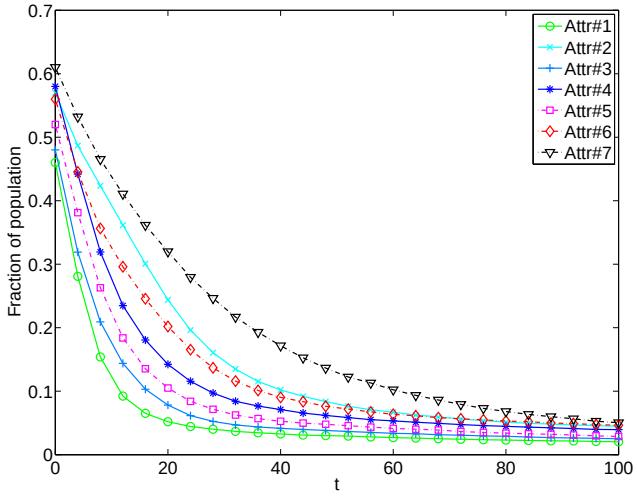
Figure 6. Attribute dynamics for the weighted evolutionary game in random network. The figures in left column correspond to applying Friends as the influential range of the utility function.



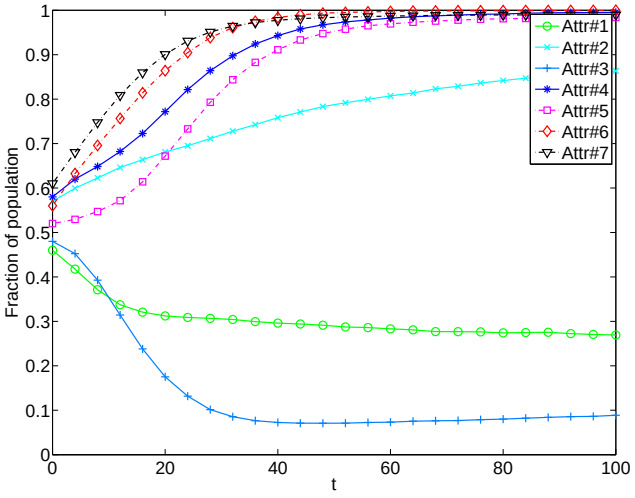
(a) Small-world network (BRR=1:0, IR={F})



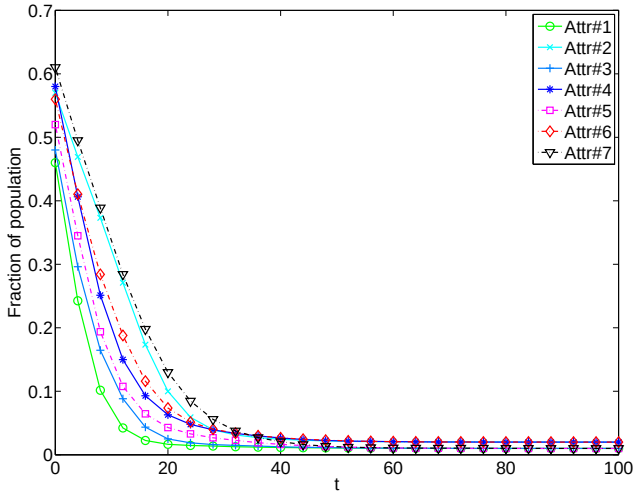
(b) Small-world network (BRR=1:0, IR={F}∪{FoF})



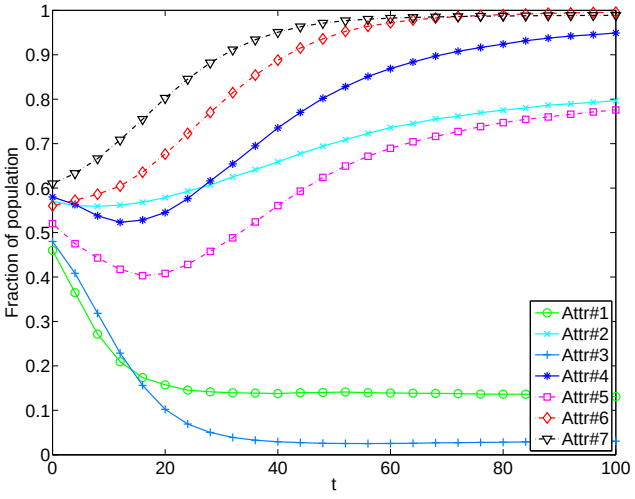
(c) Small-world network (BRR=1:15, IR={F})



(d) Small-world network (BRR=1:15, IR={F}∪{FoF})

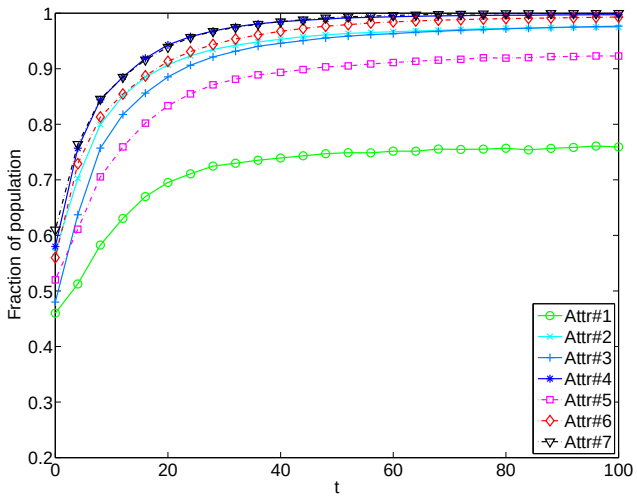


(e) Small-world network (BRR=1:30, IR={F})

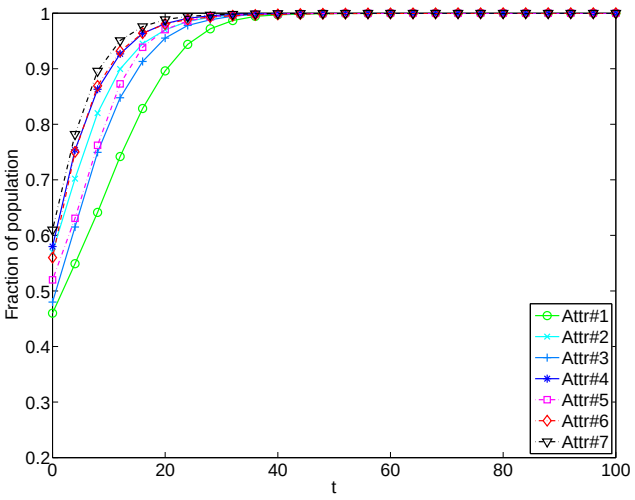


(f) Small-world network (BRR=1:30, IR={F}∪{FoF})

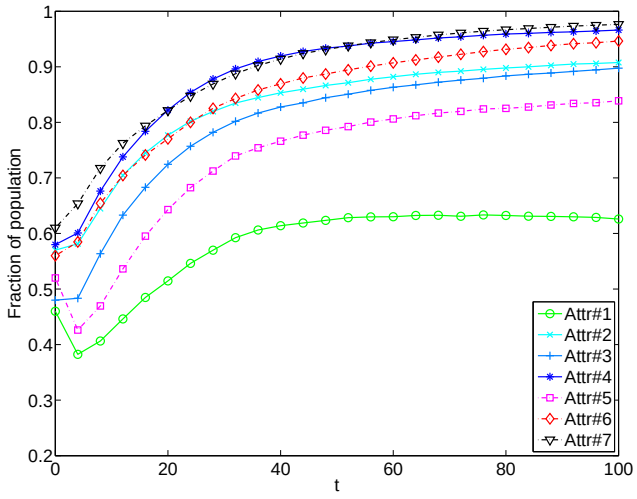
Figure 7. Attribute dynamics for the weighted evolutionary game in small-world network. The figures in left column correspond to applying Friends as the influential range of the utility function.



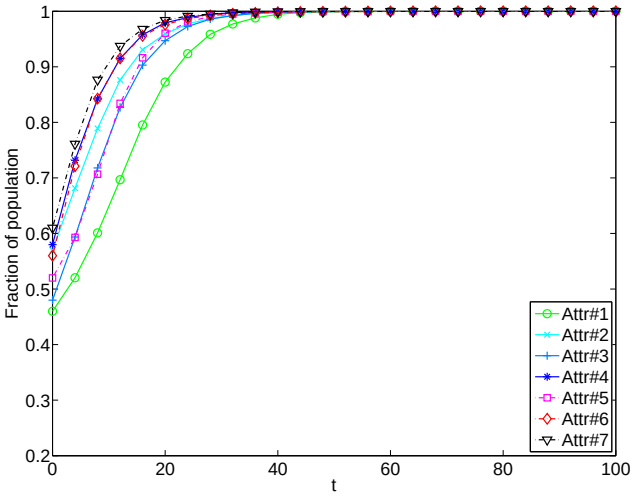
(a) Scale-free network (BRR=1:0, IR={F})



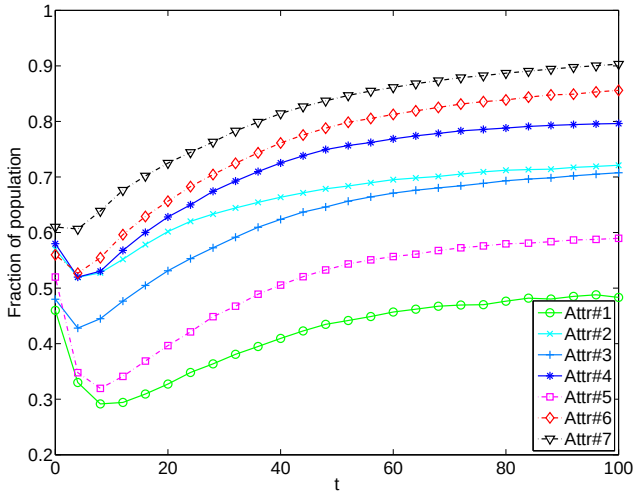
(b) Scale-free network (BRR=1:0, IR={F}∪{FoF})



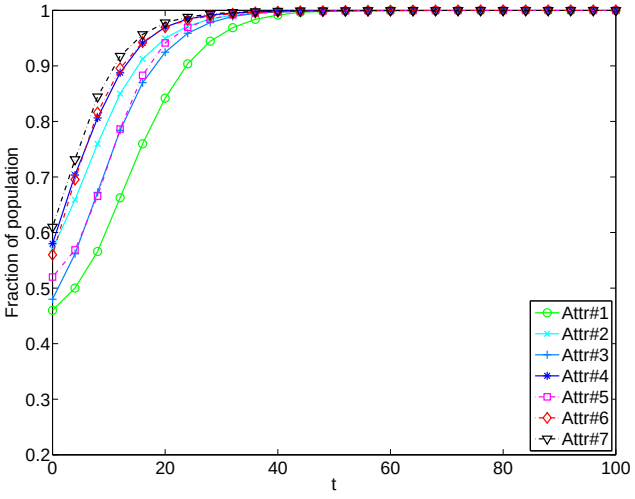
(c) Scale-free network (BRR=1:15, IR={F})



(d) Scale-free network (BRR=1:15, IR={F}∪{FoF})

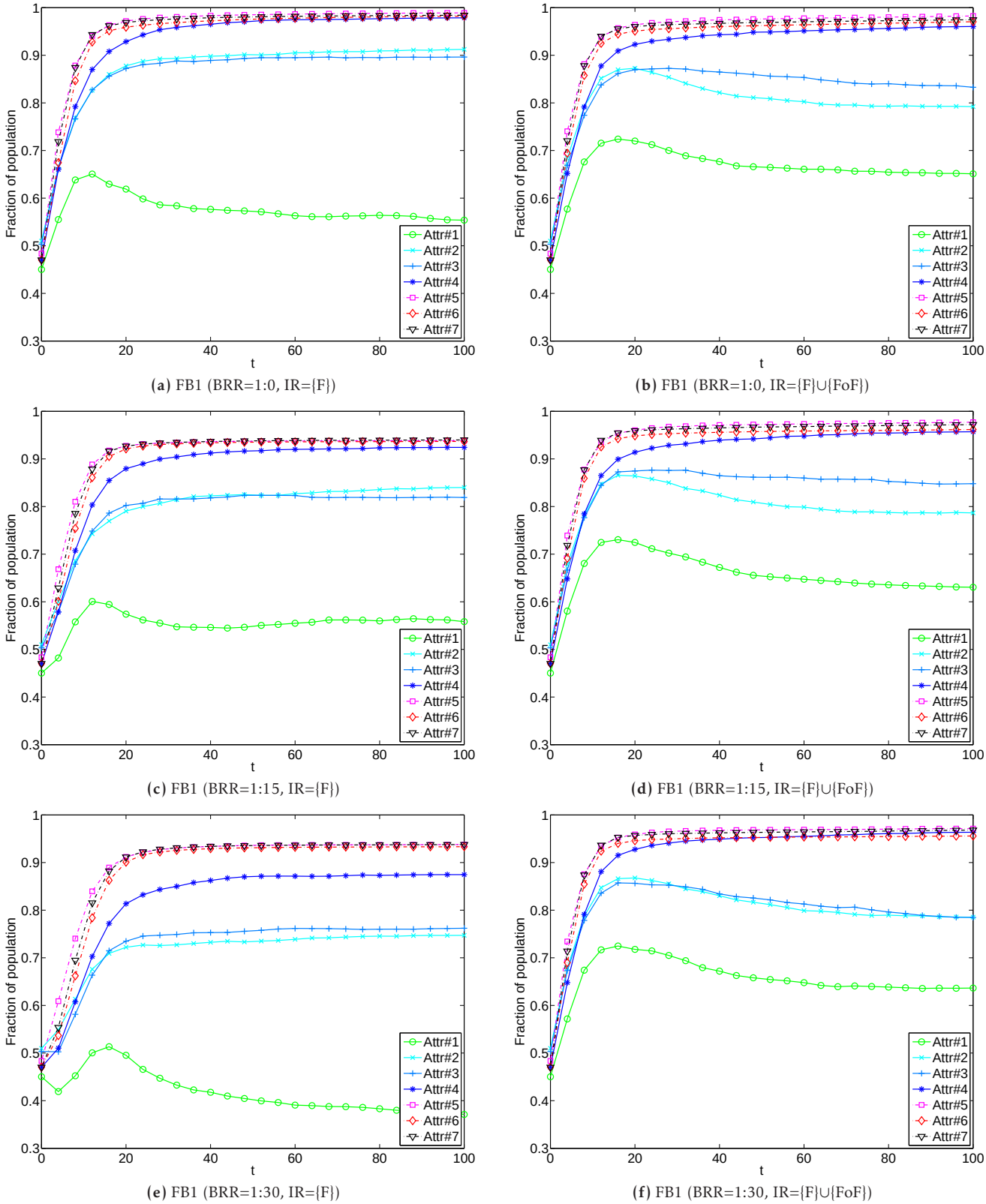


(e) Scale-free network (BRR=1:30, IR={F})



(f) Scale-free network (BRR=1:30, IR={F}∪{FoF})

Figure 8. Attribute dynamics for the weighted evolutionary game in scale-free network. The figures in left column correspond to applying Friends as the influential range of the utility function.



(a) FB1 (BRR=1:0, IR={F})

(b) FB1 (BRR=1:0, IR={F}∪{FoF})

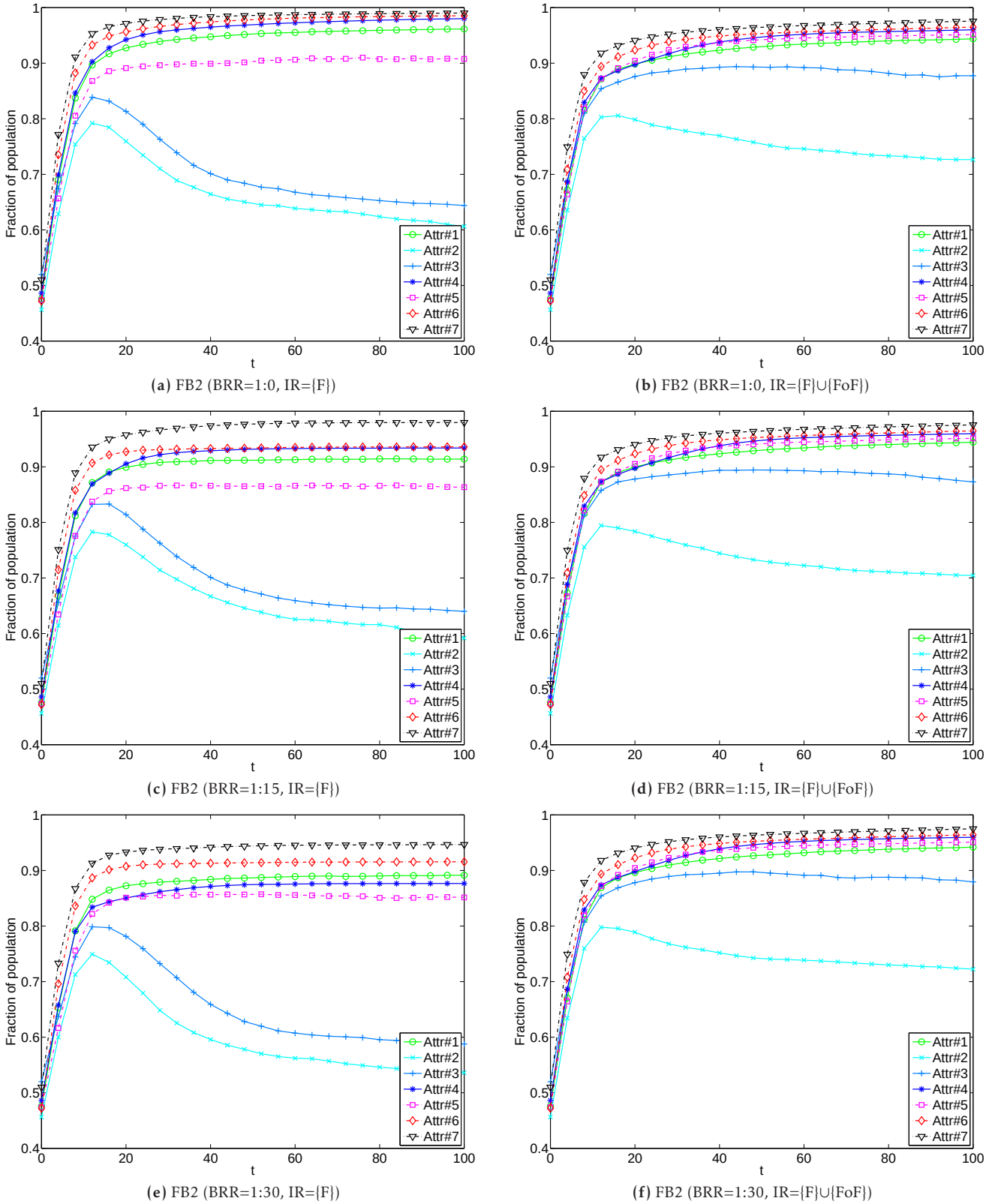
(c) FB1 (BRR=1:15, IR={F})

(d) FB1 (BRR=1:15, IR={F}∪{FoF})

(e) FB1 (BRR=1:30, IR={F})

(f) FB1 (BRR=1:30, IR={F}∪{FoF})

Figure 9. Attribute dynamics for the weighted evolutionary game in FB1. The figures in left column correspond to applying Friends as the influential range of the utility function.



(a) FB2 (BRR=1:0, IR={F})

(b) FB2 (BRR=1:0, IR={F}∪{FoF})

(c) FB2 (BRR=1:15, IR={F})

(d) FB2 (BRR=1:15, IR={F}∪{FoF})

(e) FB2 (BRR=1:30, IR={F})

(f) FB2 (BRR=1:30, IR={F}∪{FoF})

Figure 10. Attribute dynamics for the weighted evolutionary game in FB2. The figures in left column correspond to applying Friends as the influential range of the utility function.

References

[1] Antonioni, A. and Tomassini, M. (2012) Cooperation on social networks and its robustness. *Advances in Complex Systems* **15**(supp01): 1250046.

[2] Barabási, A.L. and Albert, R. (1999) Emergence of Scaling in Random Networks. *Science* **286**(5439): 509–512.

[3] Berenbrink, P., Brinkmann, A., Friedetzky, T. and Nagel, L. (2010) Balls into non-uniform bins. In *2010 IEEE International Symposium on Parallel Distributed Processing (IPDPS)*: 1–10.

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

[5] Chen, W., Liu, Z., Sun, X. and Wang, Y. (2011) Community detection in social networks through community formation games. In *22nd International Joint Conference on Artificial Intelligence (IJCAI)*: 2576–2581.

[6] Ellison, N.B., Steinfield, C. and Lampe, C. (2007) The benefits of facebook "friends:" social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication* **12**(4): 1143–1168.

[7] Erdös, P. and Renyi, A. (1960) On the evolution of random graphs. *Publ. Math. Inst. Hung. Acad. Sci* **5**: 17–61.

[8] Evans, S. (April 24, 2013) Top 18 social networks who have joined the 100 million (and more) users club, http://sarahsfav.es/2013/04/24/socialnetworks/.

[9] Kamhoua, C., Kwiat, K. and Park, J. (2012) A game theoretic approach for modeling optimal data sharing on online social networks. In *9th International Conference on Electrical Engineering, Computing Science and Automatic Control (CCE)*: 1–6.

[10] Kleinberg, J., Suri, S., Tardos, E. and Wexler, T. (2008) Strategic network formation with structural holes. *SIGecom Exch.* **7**(3): 11:1–11:4.

[11] Kossinets, G. and Watts, D.J. (2009) Origins of Homophily in an Evolving Social Network. *American Journal of Sociology* **115**(2): 405–450.

[12] Krasnova, H., Spiekermann, S., Koroleva, K. and Hildebrand, T. (2010) Online social networks: why we disclose. *Journal of Information Technology* **25**: 109–125.

[13] Lauw, H.W., Shafer, J., Agrawal, R. and Ntoulas, A. (2010) Homophily in the digital world: A livejournal case study. *IEEE Internet Computing* **14**(2): 15–23.

[14] Mathematica (2012) *SocialMediaData, Version 9.0* (Champaign, Illinois: Wolfram Research, Inc.).

[15] McPherson, M., Lovin, L.S. and Cook, J.M. (2001) Birds of a feather: Homophily in social networks. *Annual Review of Sociology* **27**(1): 415–444.

[16] Narayanam, R. and Narahari, Y. (2011) A shapley value-based approach to discover influential nodes in social networks. *IEEE Trans. Autom. Sci. Eng.* **8**(1): 130–147.

[17] Newman, M.E.J., Watts, D.J. and Strogatz, S.H. (2002) Random graph models of social networks. *Proc. Natl. Acad. Sci. USA* **99**: 2566–2572.

[18] Osborne, M. (2004) *An introduction to game theory* (Oxford Univ. Press).

[19] Roca, C.P., Cuesta, J.A. and Sánchez, A. (2009) Evolutionary game theory: Temporal and spatial effects beyond replicator dynamics. *Phys. Life Rev.* **6**(4): 208 – 249.

[20] Scott, C. (May 11, 2012) Facebook proposes more changes to privacy policy, http://www.pcworld.com/businesscenter/article/255518/facebook_proposes_more_changes_to_privacy_policy.html.

[21] Skyrms, B. (2003) *The Stag Hunt and the Evolution of Social Structure* (Cambridge Univ. Press).

[22] Squicciarini, A.C., Shehab, M. and Paci, F. (2009) Collective privacy management in social networks. In *18th International Conference on World Wide Web*: 521–530.

[23] Squicciarini, A.C. and Griffin, C. (2012) An informed model of personal information release in social networking sites. In *ASE/IEEE Conf. on Privacy, Security, Risk and Trust*: 636–645.

[24] Szabó, G. and Fath, G. (2007) Evolutionary games on graphs. *Physics Reports* **446**(4-6): 97–216.

[25] Watts, D.J. and Strogatz, S.H. (1998) Collective dynamics of small-world networks. *Nature* **393**(6684): 440–442.

[26] Wolfram, S. (August 30, 2012) Wolfram|alpha personal analytics for facebook, http://blog.wolframalpha.com/2012/08/30/wolframalpha-personal-analytics-for-facebook/.

[27] Wolfram, S. (November 28, 2012) Mathematica 9 is released today!, http://blog.stephenwolfram.com/2012/11/mathematica-9-is-released-today/.

[28] Wong, A.K.C. and Ghahraman, D.E. (1980) Random graphs: Structural-contextual dichotomy. *IEEE Trans. Pattern Anal. Mach. Intell.* **2**(4): 341–348.