Modeling Privacy Settings of an Online Social Network from a Game-Theoretical Perspective

Jundong Chen, Matthias R. Brust, Ankunda R. Kiremire, and Vir V. Phoha
Center for Secure Cyberspace
Louisiana Tech University
Ruston, LA71270, USA
Email: {jdc074, mbrust, ark010, phoha}@latech.edu

***Abstract*—Users of online social networks are often required to adjust their privacy settings because of frequent changes in the users' connections as well as occasional changes in the social network's privacy policy.**

In this paper, we specifically model the user's behavior in the disclosure of user attributes in a possible social network from a game-theoretic perspective by introducing a weighted evolutionary game. We analyze the influence of attribute importance and network topology on the user's behavior in selecting privacy settings.

Results show that users are more likely to reveal their most important attributes than less important attributes regardless of the risk. Results also show that the network topology exhibits a considerable effect on the privacy in a risk-included environment but a limited effect in a risk-free environment. The provided models and the gained results can be used to understand the influence of different factors on users' privacy choices.

***Index Terms*—game theory, social network, privacy setting, network topology**

I. Introduction

Users of online social networks increase their chances of finding potential new friends, and identifying old friends, by publishing their personal information [1]. However, concerns regarding the privacy in social networks have received worldwide attention and have led to frequent public debates [2]. Social networks contain large amounts of information that can be used to uniquely identify their users as well as provide information about their habits, interests and history [3]. Revealing this information makes it accessible to potential criminals, leaving the users vulnerable to dangers such as identity thieves, sexual predators, stalkers, and inference by defrauders [4].

The risk to user privacy has caused so much concern that over 60% of social network users employ privacy increasing measures such as deleting friends and concealing profile attributes from other social network users [5]. The benefits and risks create a dilemma that every user of a social network faces: reveal more attributes to attract more friends, or reveal less attributes to become less vulnerable. Therefore, each user in a social network weighs both the risks and benefits to determine how many profile attributes to reveal. Additionally, the privacy settings of one user potentially affects the choice of privacy settings of another user.

However, little work has been done to show how all these factors are linked together. Consequently, there is a need to model the interaction of users to understand how privacy risk and relationship-building influence the level of self-disclosure.

In this paper, we propose an evolutionary game-theoretic model to study the behavior of users in regard to their privacy settings in a possible online social network.

A principle feature of our game model is the introduction of *weighted attributes*. Attaching weights to the attributes allows us to account for the fact that some attributes are more important than others. Our study conducts the simulation of user behavior in different types of network topologies, which include random, small-world and scale-free networks.

The main contributions of this paper are twofold. Firstly, our model investigates the importance of the revealed and hidden attributes for the users' behavior. By weighting the attributes, we model the fact that some attributes have a higher impact than others in self-disclosure. As an illustration, these aspects help us to investigate whether revealing a user's important attributes such as religion and sexual preferences would affect a social network more than revealing that user's less important attributes such as their favorite movies. Secondly, our model allows us to investigate what influence the network topology has on the privacy strategy of the user to model different social network properties [6]. For example, given Alice is a user in the social network and is a friend to every other user, this model investigates whether her strategy to withhold 30% of her attributes affects other users' strategies as much as Bob's decision given he is less popular with only two friends in that network.

The results show a tendency for users to reveal their most important attributes more than less important attributes. By important attributes, we refer to those attributes which have a larger impact on the *social capital* of a user [7]. Additionally, users in random and scale-free networks are more likely to reveal their attributes than users in small-world networks. Interestingly, we find that the type of network topology has a limited effect on privacy settings of a social network in the

COLLABORATECOM 2013, October 20-23, Austin, United States

DOI 10.4108/icst.collaboratecom.2013.254054

risk-free case, but has a considerable effect on the privacy in the risk-included scenario.

Our model can be used to understand and predict the dynamics of a social network based on attribute disclosure. 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 maximize the self-disclosure in a network while keeping the privacy risk under a certain threshold.

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

II. Related work

Online social networks are built around the concept of *self-disclosure* [8], which is positively affected by factors such as *relationship-building* and *platform enjoyment*. In contrast, perceived privacy risk is a factor with a negative effect on self-disclosure [8]. The benefit of relationship-building is linked to the number of friends a user is supposed to gain by disclosing personal information. The link between the number of potential friends and revealed information is based on the *homophily* principle more commonly expressed as "birds of a feather flock together" [9]. In the context of a social network, this principle translates to users with similar attributes being more likely to establish a friendship [9]. On top of the similarity in attributes, the number of revealed attributes appears to positively affect relationship-building. Lampe et al. [10] reports that the number of a user's friends is exponentially related to the set size of the revealed attributes. This can be explained by considering that sharing more profile attributes allows more users to establish common ground that promotes interaction and encourages "friendship" [11]. However, *profile disclosing* increases the privacy risk to social network users [8]. Profile disclosing is defined as the amount of a user's profile that is visible to a third party [8].

The approach presented throughout this paper is based on an evolutionary game theoretic-model. Game theory has been used to model social networks and privacy settings [12]. Using results from a survey, Squicciarini et al. [12] build an evolutionary game theoretical model aimed at optimizing the users' long-term utility. Additionally, by investigating the evolutionary game dynamics, they reveal that social capital gained from self-disclosure influences a user's decisions more than the risk to that user's privacy.

The profile attribute privacy problem is similar to the *stag-hunt* game which exhibits both pure and mixed *Nash equilibria* [13]. The stag-hunt game is a two-player two-strategy game that captures the conflict between cooperation and safety involved in a situation where a hunter selects whether to hunt a stag or a hare without prior knowledge of another hunter's choice. This game reaps the highest benefit to both players if both players select to hunt a stag and the highest risk to one player if the other player selects otherwise. This situation is similar to the privacy in social networks between two players because the highest benefit is accrued if both players cooperate and reveal all their attributes. However, in some aspects, the profile attribute privacy problem is different from the stag-hunt game because the privacy problem involves multiple players, and multiple strategies (options).

Other works have also employed game-theoretic models to capture the relation and coordination between different user properties in different networks in a variety of applications. The networks range from online video sharing social networks [14] to mobile adhoc networks [15] and anonymous social networks [16]. The modeled applications include sharing co-owned pictures in a social network [17] and stimulating cooperation in the network [14]. In most of these works [14], [18], a two party model is derived and used as a basis to create a model that captures the dynamics of the entire network. This is because the networks can be looked at as a collection of multiple two party interactions. We employ the same reasoning when designing models to capture the interaction of user's privacy in a social network, however, we do not model the privacy settings of any specific online social network. Instead, we focus on a possible online social network model.

III. Preliminaries

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

A. Assumptions

We assume that users with more attributes in common are more likely to be friends. This assumption is based on research which shows that the homophily principle is exhibited in social networks [9]. Additionally, we assume that all users of the network attach the same importance to any given attribute, e.g. all users will consider their address attribute to be more important than their religion attribute.

These assumptions allow us to investigate the influence of global network properties while simultaneously comparing local properties such as profile attributes and their importance to users on a common ground.

B. 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. For example, if a user John Doe reveals a set of attributes $\{Doe, 34\}$ while another user Jane Doe reveals $\{Doe, Female, 34, Chicago\}$, then Jane is more distinct 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 the revealed profile attributes. As a result, the risk to John Doe's identity is reduced by Jane Doe.

C. Privacy settings

The *privacy setting* is a configuration of the users' profile information, which allows the user to enable or disable the visibility of certain profile attributes. The privacy setting of a typical social network consists of levels of visibility of different aspects such as profile attributes, activity logs, and friend lists to various types of users, e.g. friends, friends of friends, and public. In our model, we consider a single level of visibility, i.e. whether profile attributes are visible to any other user of the network.

D. Network topologies

We examine the behavior of our model on three different types of network topologies, which include a random network, a small-world network, and a scale-free network.

A *random network* is a graph in which the occurrence of connection between nodes follows a probability distribution [19]. A random graph can be used for modeling social networks when the node degrees follow an arbitrary probability distribution [20]. The Erdös-Rényi (ER) [21] model is considered to generate the random networks. The probabilities that edges exist between any two nodes are equal and independent. Given the probability of an edge occurrence is p and there are n nodes, the average node degree k is about $n \cdot p$.

In a *small-world network*, most of the nodes are not directly connected to each other, but most nodes can be reached by every other node within a relatively small number of intermediate nodes. Online social networks have been shown to exhibit small-world properties and can be produced using a Watts-Strogatz model [22].

A *scale-free network* is a network where the node degree distribution follows a power-law distribution, i.e. the number of nodes decreases exponentially as the node degree increases [23]. To create the scale-free network, seed nodes are placed within the network and new nodes added to the existing network incrementally. In this way, any new added node is more likely to form a link with higher degree nodes [23].

IV. Our approach

We propose a weighted evolutionary game to investigate the influence of attribute importance (weight) and network topology on the privacy of users of a social network.

Many online social networks are available today with a variety of privacy setting designs [24]. In this paper, we model a possible social network with characteristics exhibited by some of the online social networks in existence. For example, in our assumed social network and our game, every user has a profile made up of profile attributes, where each user is tasked with selecting how many and which attributes to reveal to all other users of the network. However, we do not consider categories of friends with different levels of privacy, which is a characteristic of some social networks.

A. Our models: Game and social network

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 different network types. Random, small-world, and scale-free networks are investigated as described in the previous section.

Our weighted evolutionary game acts on top of this possible social network. The utility of a user is a combination of *positive utility* and *negative utility*. The positive utility is the summation of the weighted number of attribute pairs with each of the neighbors on the network. The negative utility is 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 with a corresponding attribute weight vector $W = (w_1, w_2, ..., w_m)$ in the social network, where $a_{x,i}$ is the i^{th} attribute of User x. 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 $s_{x,i} = 0$.*

An example of an attribute vector for a default user Alice, is given by $A_{Alice} = (Name, Gender, Age, ..., Hometown)$. For simplicity, we assume all the users have the same set of profile attributes. A specific attribute *i* is referred to by $Attr\#i$. An attribute sign flag vector S_x denotes which attributes are disclosed and which are withheld. For example, $S_{Alice} = (1, 1, 0, ..., 1)$ means that Alice decides to reveal her name, gender, and hometown but withholds her age.

We capture the similarities between two users using *pairs*. Two users Alice and Bob are said to have a *pair* if they both reveal the same attribute, e.g. age. 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. Out of the m attributes, User x reveals k_x attributes while User y reveals k_y attributes. Both users reveal attributes $Attr\#1, Attr\#2, ..., Attr\#r$, which contribute to r pairs. The r pairs are denoted by $(a_{x,1}, a_{y,1})$, $(a_{x,2}, a_{y,2})$, ..., $(a_{x,r}, a_{y,r})$.

We adopt the concept of pair without considering equal value pair. In fact, common ground should be built on the number of equal value pairs. But the number of pairs still reflects the common ground, since two users have a higher chance to have more equal value pairs if they have more pairs.

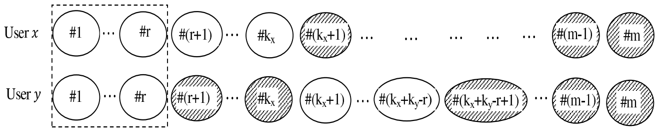


Figure 1. The figure shows a possible profile configuration for two users x and y, who disclose k_x and k_y attributes respectively out of the m possible attributes. The clear ovals represent the disclosed attributes while the shaded ovals represent withheld attributes.

In our game, utility includes benefits (positive utility) and risks (negative utility). The positive utility of a user is affected by the number and type of attributes that a user shares with the neighbors. 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.

The negative utility (risk) of a user in the weighted evolutionary game is linked to how many other users of the network can hide that user. The set of all neighbors of User x is denoted by B_x. The set B^h_x consists of all neighbors of User x that 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 contributes to the positive utility, while the set B^h_x controls how much risk a user is exposed to.

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

$$u_x = w_P \cdot \sum_{y \in B_x} (S_x \wedge S_y) \times W^T - w_N \cdot \frac{1}{|B^h_x|} \tag{1}$$ [1]

The *replicator rule* [25] is employed in our model for users to update their strategy between time steps according to

$$P^{t+1}_{x,y} = \begin{cases} \frac{u^t_y - u^t_x}{d_{max}}, & u^t_y > u^t_x, \\ 0, & u^t_y \leq u^t_x, \end{cases} \tag{2}$$

where $P^{t+1}_{x,y}$ is the probability that at time $t+1$, User x adopts the strategy User y had at time t. Additionally, u^t_x is the utility of User x at time t, while u^t_y is the utility of User y at time t. We use the largest difference d_{max} in payoff between any two users in the network to ensure that $P^{t+1}_{x,y} \in [0, 1]$. The expression 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.

During each iteration, all nodes, e.g. users, find candidate strategies from their neighbors that are then used during the update. Following, all nodes update their strategies in each iteration. The update results in each node either maintaining its original strategy or changing just one bit of its sign flag to mimic one neighbor. This process is repeated until there is no difference in the strategies of all nodes between two consecutive iterations. When this condition has been met, the system is said to be stable.

The probability of the users changing strategies, as provided in [25], is given by

$$Q^{t+1}_{x,y} = 1 - \prod_{y \in B_x} (1 - P^{t+1}_{x,y}) \tag{3}$$

where $Q^{t+1}_{x,y}$ is the probability that the User x actually changes their strategy between time t and $t+1$.

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

Algorithm 1 Update profile attribute sign flag

```
Initialize profile attribute sign flag for each node.
Calculate payoff value for all the nodes using Equation 1.
while <Any node changes sign flag> do
    //Each node determines which digit of its own sign flag to change.
    for <Each nodes> do
        Find neighbors with higher payoff value.
        Select neighbor with sign flag to mimic using Equation 2 and Equation 3.
        By comparing with selected neighbor, determine which digit of sign flag to change.
    end for
    Change all nodes' sign flags accordingly.
end while
```

B. Working case for risk-free scenario

In this subsection, we describe an example of a risk-free scenario, which means we only consider the positive utility. Fig. 2a shows a generated social network according to the description above, which consists of 7 users. An example of the profile attribute sign flag S_x for all 7 users is shown in Fig. 2b with the profile attributes (Name, Gender, Age,..., Hometown) and their respective weights $(w_1, w_2, w_3, ..., w_7)$ shown in Fig. 2e. A user calculates the number of pairs that it shares with its neighbors before selecting its next privacy strategy.

The positive utility associated with any neighbor is a combination of the number of pairs (obtained using a bit-wise AND-function) and the weights associated with those attributes. For example, given User 1 has profile attribute sign flag $S_1 = (1000110)$ and User 2 has $S_2 = (0110011)$, a bit-wise AND yields 0000010. The sixth bit position is the only "1" shown in the AND result which indicates that the only attribute revealed by both users is Attr#6. Using

[1] Unless otherwise stated, the notation $\wedge$ represents logic AND. We use the notation W^T to refer to the transpose of vector W.

the corresponding weight factor, we obtain the payoff value between users 1 and 2 of (w_6). Similar analysis between User 1 and User 5, where $S_5 = (1100110)$ yields a bit-wise AND-value of 1000110 and therefore a payoff value equal to $(w_1 + w_5 + w_6)$. Since User 1's payoff with User 5 $(w_1 + w_5 + w_6)$ is higher than User 1's payoff with User 2 (w_6), User 1 has a higher probability of changing his strategy to mimic User 5 in the next iteration.

After all users have compared their current strategies with their neighbors, each user is allowed to change one bit of the sign flag. An example of the system state after one iteration is shown in Fig. 2c. The figure shows that User 1's strategy has not changed and is still $S_1 = (1000110)$. However, User 6's strategy has changed from $S_6 = (0101011)$ to $S_6 = (0111011)$. The entire process is repeated until the whole system reaches stability. Stability means that no single node changes their sign flag (strategy) between two successive time steps. The state of the sample system when stability is achieved is shown in Fig. 2d. In the final state, the strategy of User 1 is given by $S_1 = (1100011)$, which is achieved after 8 iterations.

V. Simulations and Results

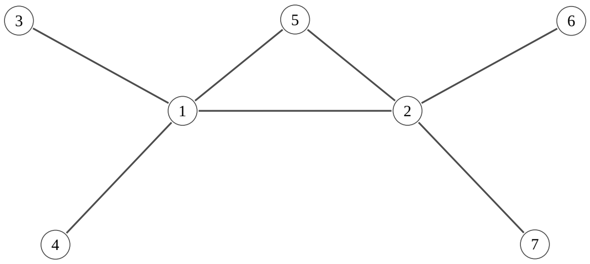
In this section, we describe the underlying simulation settings and discuss the derived results. The simulations deal with risk-included and risk-free cases of the weighted evolutionary game.

A. Simulations settings

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. The number of users is set to be 100. 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 100 users of the network. Each user has three options for each attribute during each iteration. These options are that the user can select to reveal, withhold, or maintain the status of any attribute.

We set the ratio of positive utility to negative utility to be 1:10 (cf. Table I), which is determined by w_P and w_N. While all the attributes are assigned to different weights, we assume that the weight vector for the attributes is the same for every user of the network. Additional simulation settings are shown in Table I. The simulation results of 500 runs are averaged to determine the dynamics of the model in each of the considered networks, which include random, small-world and scale-free networks. The average node degree for each network is 4.



(a)

$Node$	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

(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	1	1	0	1	1
User 7	0	0	1	0	1	0	0

(c)

$Node$	w_1	w_2	w_3	w_4	w_5	w_6	w_7
User 1	1	1	0	0	0	1	1
User 2	0	1	1	0	0	1	1
User 3	1	1	0	0	0	1	1
User 4	1	1	0	0	0	1	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

(d)

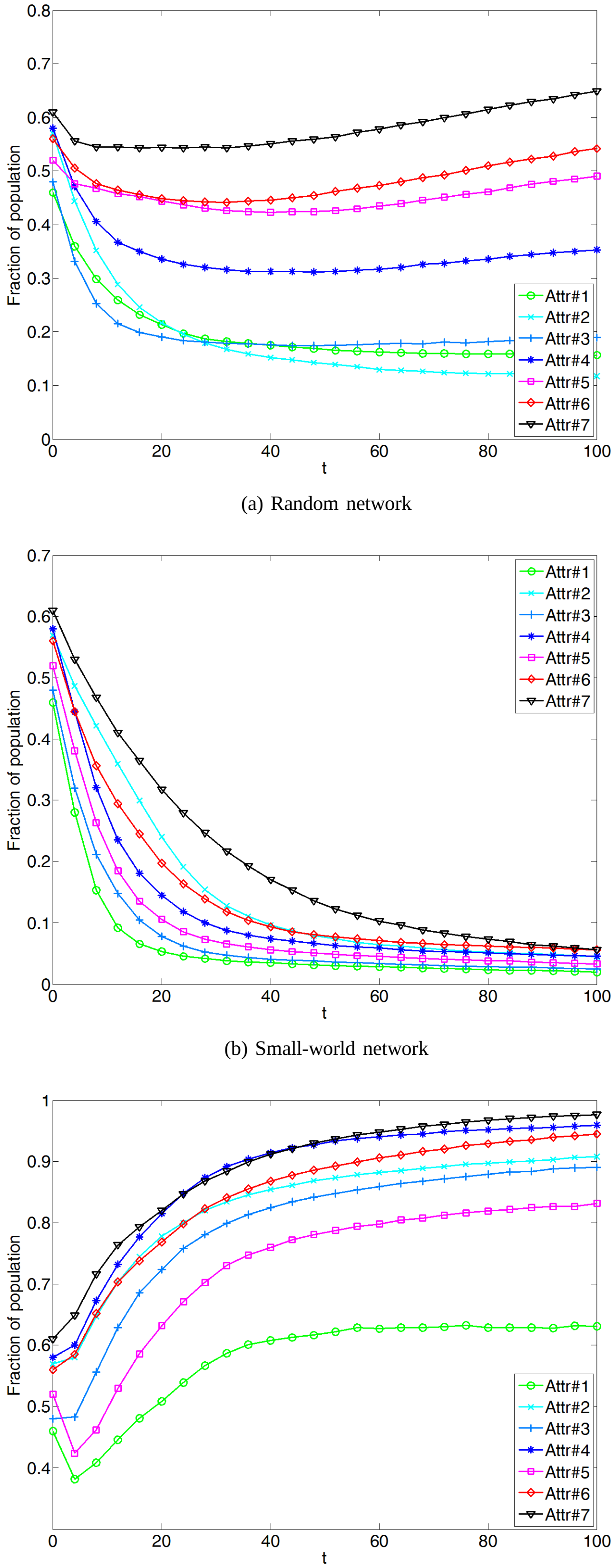
w_1	w_2	w_3	w_4	w_5	w_6	w_7
Name	Gender	Age	Religion	Education	Occupation	Hometown

(e)

Figure 2. (a) A sample network consisting of 7 users connected to each other, (e) each user has a profile with 7 attributes which are assigned different weights $w_1, w_2, ..., w_7$, (b) the randomly assigned sign flags for all 7 users that indicate which attributes are revealed and which attributes are withheld (a "1" indicates an attribute revelation while a "0" indicates an attribute withholding), (c) after every user compares his strategy with that of his neighbors, every user updates their strategy, (d) the illustrated system converges after 8 iterations and gives the resultant sign flags for all users.

B. Results

The dynamics of the attributes in different network topologies are shown in Fig. 3 and Fig. 4 for the risk-included and risk-free cases. The figures show the proportions of the population that select to reveal specific attributes and how these proportions change with each iteration. Initially, randomly chosen 7-bit attribute sign flags are assigned to each user.

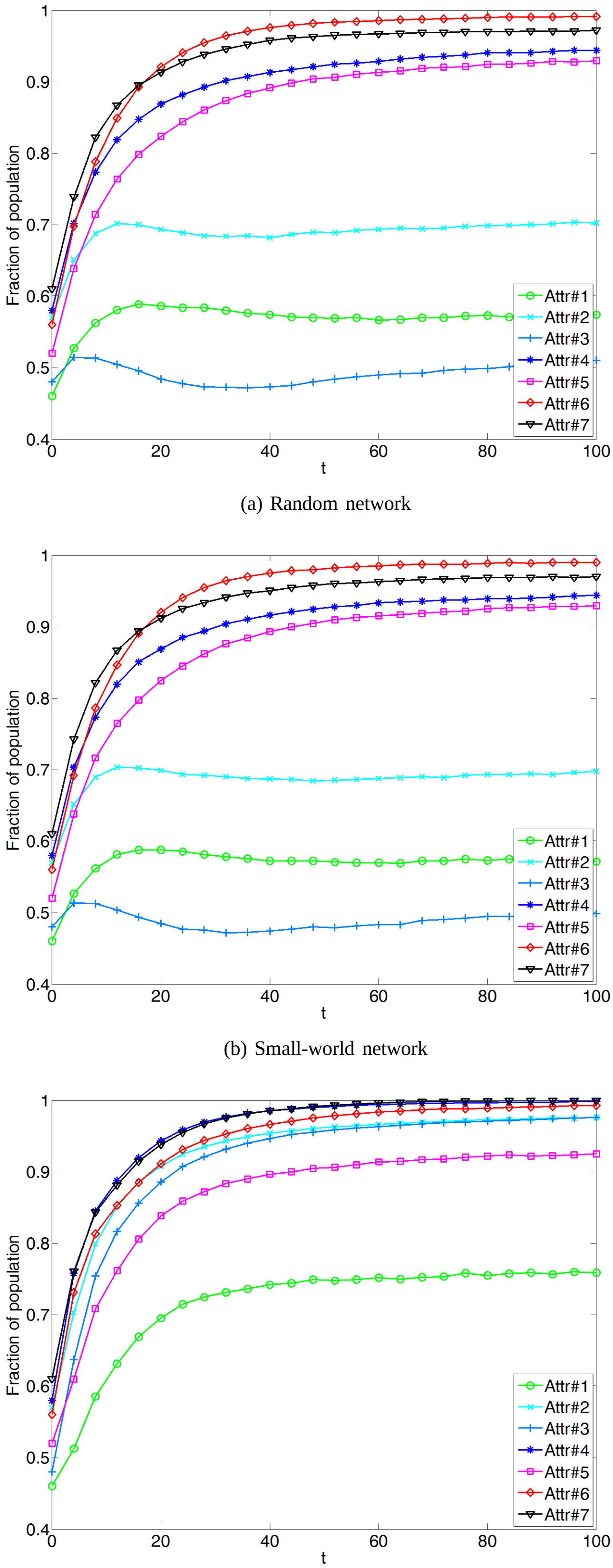


(a) Random network

(b) Small-world network

(c) Scale-free network

Figure 3. Attribute dynamics for the weighted evolutionary game in the risk-included scenario with different underlying topologies.



(a) Random network

(b) Small-world network

(c) Scale-free network

Figure 4. Attribute dynamics for the weighted evolutionary game in the risk-free scenario with different underlying topologies.

TABLE I. VALUES ASSIGNED TO SPECIFIC PARAMETERS IN ORDER TO OBTAIN THE PRESENTED RESULTS

Parameter	Weighted evolutionary game
$\|N\|$	100
m	7
w_P	1
w_N	10
W	$(0.02, 0.06, 0.10, 0.14, 0.18, 0.22, 0.28)$

Results in Fig. 3 show the difference in the risk-included cases with regard to the network topologies. For example, Fig. 3a shows that even though all attributes experience an initial drop in popularity, the attributes Attr#7, Attr#6, and Attr#5 end up being revealed by more than 50% of the network users. From Table I, we see that these attributes correspond to the higher attribute weight values. This shows that the users in a random graph are more likely to reveal their important attributes and withhold their less important attributes.

Fig. 3b reveals that the values of all attributes drop in popularity when the game is applied in a small-world network for the case with risk. This indicates that users will withhold their attributes in this type of network. However, more important attributes are revealed more often than less important attributes, even though less people are revealing their attributes. When the game is applied to a scale-free network, the result is different. Compared to Fig. 3a and 3b, Fig. 3c shows that most users reveal their attributes in a scale-free environment.

The risk-included scenario shows that users in a social network tend to reveal or withhold their profile attributes depending on the way the network is connected.

From the risk-free case in Fig. 4, we observe that the type of network has a limited effect on the eventual strategies deployed by the network users. In Fig. 4a, 4b and 4c, the general trend is for users to reveal all 7 attributes. This means that if risk is not included, the way users are connected to each other does not play a significant role in determining which attributes to reveal. Interestingly, similar to the risk-included case, users are more likely to reveal their more important attributes than their less important attributes.

VI. 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. Users are able to adjust their privacy settings according to certain strategy options. In order to make the model more realistic, we include weights which correspond to the user's importance for certain attributes.

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

Results show that users are more likely to reveal more important attributes than less important attributes. This observation is more pronounced in random and scale-free networks than in small-world networks. Results also suggest that the network topology has limited effect on the privacy dynamics of the network in the absence of risk, given risk is defined as the probability of one user's identity being inferred.

The approach presented in this paper provides an initial approach to study and comprehend the dynamics of privacy settings in social networks. Additionally, the nature of the transitions reveals the influence of certain factors in the short and long run in social network privacy.

As future work, we plan to investigate the performance of our model on a larger variety of networks as well as compare it with data from real world social networks. Additionally, we intend to investigate multi-level privacy settings where users reveal different sets of attributes to different users of the network.

ACKNOWLEDGMENT

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

REFERENCES

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

[2] J. Guynn, "New facebook information sharing features cause privacy concerns," http://articles.latimes.com/2011/sep/27/business/la-fi-facebook-privacy-20110927, September 27, 2011.

[3] F. Ben Abdesslem, I. Parris, and T. Henderson, "Reliable Online Social Network Data Collection," in *Computational Social Networks*. London, UK: Springer, 2012, ch. 8, pp. 183–210.

[4] Y. Liu, K. P. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in *Proc. of the Usenix/ACM Internet Measurement Conf. (IMC)*, 2011, pp. 61–70.

[5] M. Madden, "Privacy management on social media sites," http://pewinternet.org/Reports/2012/Privacy-management-on-social-media/Summary-of-findings.aspx, 2012.

[6] A. Antonioni and M. Tomassini, "Cooperation on social networks and its robustness," *Advances in Complex Systems*, vol. 15.

[7] N. B. Ellison, C. Steinfield, and C. Lampe, "The benefits of facebook "friends:" social capital and college students' use of online social network sites," *Journal of Computer-Mediated Communication*, vol. 12, no. 4, pp. 1143–1168, 2007.

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

[9] M. Miller, L. S. Lovin, and J. M. Cook, "Birds of a feather: Homophily in social networks," *Annual Review of Sociology*, vol. 27.

[10] C. Lampe, N. Ellison, and C. Steinfield, "A familiar face(book): Profile elements as signals in an online social network," in *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, 2007, pp. 435–444.

[11] A. Mislove, B. Viswanath, K. P. Gummadi, and P. Druschel, "You are who you know: Inferring user profiles in online social networks," in *Proc. of the ACM Int'l Conf. on Web Search and Data Mining*, 2010, pp. 251–260.

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

[13] B. Skyrms, *The Stag Hunt and the Evolution of Social Structure*. Cambridge University Press, Dec. 2003.

[14] W. Lin, H. Zhao, and K. Liu, “Cooperation stimulation strategies for peer-to-peer wireless live video-sharing social networks,” *IEEE Trans. Image Processing*, vol. 19, no. 7, pp. 1768–1784, July 2010.

[15] W. Yu and K. Liu, “Secure cooperation in autonomous mobile ad-hoc networks under noise and imperfect monitoring: A game-theoretic approach,” *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2.

[16] S. Xu, X. Li, T. Parker, and X. Wang, “Exploiting trust-based social networks for distributed protection of sensitive data,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 1, pp. 39–52, March 2011.

[17] A. C. Squicciarini, M. Shehab, and F. Paci, “Collective privacy management in social networks,” in *Proc. of the Int’l World Wide Web Conf.*, April 2009, pp. 521–530.

[18] C. Kamhoua, N. Pissinou, and K. Makki, “Game theoretic modeling and evolution of trust in autonomous multi-hop networks: Application to network security and privacy,” in *Proc. of the IEEE Int’l Conf. on Comms. (ICC)*, 2011, pp. 1–6.

[19] A. K. C. Wong and D. E. Ghahraman, “Random graphs: Structural-contextual dichotomy,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 2, no. 4, pp. 341–348, April 1980.

[20] M. E. J. Newman, D. J. Watts, and S. H. Strogatz, “Random graph models of social networks,” *Proc. Natl. Acad. Sci. USA*, vol. 99, pp. 2566–2572, 2002.

[21] P. Erdös and A. Renyi, “On the evolution of random graphs,” *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, pp. 17–61, 1960.

[22] D. J. Watts and S. H. Strogatz, “Collective dynamics of small-world networks,” *Nature*, vol. 393, no. 6684, pp. 440–442, June 1998.

[23] A.-L. Barabási and R. Albert, “Emergence of Scaling in Random Networks,” *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.

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

[25] C. P. Roca, J. A. Cuesta, and A. Sánchez, “Evolutionary game theory: Temporal and spatial effects beyond replicator dynamics,” *Phys. Life Rev.*, vol. 6, no. 4, pp. 208 – 249, 2009.