Community-Structured Evolutionary Game for Privacy Protection in Social Networks

Jun Du, *Student Member, IEEE*, Chunxiao Jiang, *Senior Member, IEEE*, Kwang-Cheng Chen, *Fellow, IEEE*, Yong Ren, *Senior Member, IEEE*, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*— Social networks have attracted billions of users and supported a wide range of interests and practices. Users of social networks can be connected with each other by different communities according to professions, living locations, and personal interests. With the development of diverse social network applications, academic researchers, and practicing engineers pay increasing attention to the related technology. As each user on the social network platforms typically stores and shares a large amount of personal data, the privacy of such user-related information raises serious concerns. Most research on privacy protection relies on specific information security techniques such as anonymization or access control. However, the protection of privacy depends heavily on the incentive mechanisms of social networks, like users' psychological decisions on security execution and socio-economic considerations. For example, the desire to influence the behaviors of other people may change a user's choice of security setting. In this paper, a game theoretic framework is established to model users' interactions that influence users' decisions as to whether to undertake privacy protection or not. To model the relationship of user communities, community-structured evolutionary dynamics are introduced, in which interactions of users can only happen among those users who have at least one community in common. Then the dynamics of the users' strategies to take a specific privacy protection or not is analyzed based on the proposed community structured evolutionary game theoretic framework. Experiments show that the proposed framework is effective in modeling the users' relationships and privacy protection behaviors. Moreover, results can also help social network managers to design appropriate security service and payment mechanisms to encourage their users to take the privacy protection, which can promote the spreading of privacy behavior throughout the network.**

***Index Terms*— Community structure based evolutionary games, privacy protection, behavior spreading, social networks.**

I. Introduction

OVER the past decade there has been an unprecedented development of social network applications. Online social networks, such as Facebook, Google+, and Twitter are inherently designed to enable people to distribute and share personal and public information [1]–[4]. In addition, social connections among friends, colleagues, family members, and even strangers with similar interests are established via these online social network platforms. However, as these platforms, as well as other online applications and cloud computing, allow their users to host large amounts of personal data on their platforms, important concerns regarding the security and privacy of user-related information arise [5]–[9]. How to protect users' personal information, and encourage users to participate the privacy protection to improve the information security of the entire social network, have become one of critical problems for social network managers.

In response, many social networks have provided different privacy protection measures to try to protect their users' personal information. Take "Privacy Setting and Tools" of Facebook for instance, it allows the users to decide who can see their stuff, contact them and look them up to obtain different levels of protection. In addition, the "Privacy and safety" settings of Twitter provide some similar options for its users to determine that who can receive their Tweets, tag them in photos, etc. Furthermore, privacy protection mechanisms have been also studied from many aspects such as information collection, information processing [10]–[12], anonymity [13], access control [14], [15], etc., to improve the security of users' data. However, users' decisions, actions, and preferences regarding personal information security, and social-economic relationships, can critically influence the implementation of privacy protection on online social network platforms. On the one hand, a user's selection of security level can protect her or his own personal information, and help to preserve the privacy of others related to this user. On the other hand, users' behavior to adopt security measures can be affected by the decisions of other users and potentially spread throughout the entire social network, depending of course depends on the network topology. Thus, the privacy protection of users in the network relies on its users to make use of security services to protect their friends' and their own information, and this behavior is conditional. One user has to make a decision on whether or not to undertake privacy protection according to many considerations, such as if and how many

Manuscript received December 29, 2016; revised June 16, 2017 and September 15, 2017; accepted September 17, 2017. Date of publication October 2, 2017; date of current version December 19, 2017. This work was supported in part by the National Natural Science Foundation China under Project 61371079 and Project 61571300, in part by the U.S. Army Research Office under Grant W911NF-16-1-0448, and in part by the U.S. National Science Foundation under Grant CMMI-1435778. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Eduard A. Jorswieck. *(Corresponding author: Chunxiao Jiang.)*

J. Du and Y. Ren are with the Department of Electronic Engineering, Tsinghua University, Beijing 100084, China (e-mail: blgdujun@gmail.com; reny@tsinghua.edu.cn).

C. Jiang is with the Tsinghua Space Center, Tsinghua University, Beijing 100084, China (e-mail: jchx@tsinghua.edu.cn).

K.-C. Chen is with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: kwangcheng@usf.edu).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2017.2758756

friends of his/hers make the same choice. To understand and to model such interactions among users, game theory can be used. Particularly useful is evolutionary game theory which considers that a game is played over and over again by socially conditioned players randomly drawn from large populations. It studies population shift and evolution processes, and pays particular attention to the dynamics and stability of the strategies of the entire population. For the privacy protection issues, evolutionary game theory can be used to model the spreading of users' security behavior over social networks, which heavily depends on the interaction and friendship among the users. Thus, in this paper, we establish a community structured evolutionary game theoretic framework to analyze and reveal the interactions between users and the spreading of security behavior throughout a social network.

A. Literature Review

Game theoretic models and evolutionary game theoretic models have been introduced in the literature to comprehend and to interpret the interactions among network users regarding personal information security. In [16], the authors organized the presented works on network security and privacy into six main categories: security of the physical and medium access control (MAC) layers, security of self-organizing networks, intrusion detection systems, anonymity and privacy, economics of network security, and cryptography. In each category, they identified security problems, players, and game models, and main results such as equilibrium analysis. In [17], the authors formulated a non-cooperative cyber security information sharing game, the strategies of which are participation and sharing versus non-participation. They analyzed the game from an evolutionary game-theoretic viewpoint, and determined the conditions under which the players' self-enforced evolutionary stability can be achieved. A model of an evolutionary game between social network sites (SNS) and their users was established from the perspective of privacy concerns in [18]. In this work, the SNS tend to decide whether to disclose users' privacy or not for profit, and users tend to decide about privacy disclosure to obtain certain benefits. Authors of [19] proposed an evolutionary game theoretic framework to model the dynamic information diffusion process in social networks, and derived the closed-form expressions of the evolutionary stable network states through analyzing the proposed framework in uniform degree and non-uniform degree networks. For a better understanding of online information exposure, a deception model for online users was proposed in [20] based on a game theoretic approach characterizing a user's willingness to release, withhold or lie about information depending on the behavior of individuals within the user's circle of friends.

As mentioned previously, the influence of users' behaviors also plays an important role on the selection of privacy protection throughout the social network. In other words, behaviors of users can spread over the network according to some kind of natural selection. In the practice of a game, if the utility obtained by one strategy is larger than that by another strategy for a specific player, this strategy will be imitated by other players of high probability, which suggests this strategy is more likely being spread over the entire social network. For the user privacy concerns, it is important to analyze the spreading and influence of user behaviors that make use of the privacy protection or not. Based on such analysis, the benefit-cost mechanism can be designed to promote the use of the privacy protection among the users, and then the information security of the social network can be improved. The spreading of human behaviors has been studied from various aspects. In [21], individuals were separated into interdependent groups, and their different combinations were studied to reveal that an intermediate interdependence optimally facilitates the spreading of cooperative behavior between groups. It has been shown that there is an intermediate fraction of links between groups that is optimal for the evolution of cooperation in the prisoner's dilemma game. Results in [22] suggested that strong ties are instrumental for spreading both online and real-world behavior in human social networks. The authors demonstrated that the messages diffused in the network directly influenced political self-expression, information seeking and real world voting behavior of millions of people. Furthermore, the messages not only influenced the users who received them but also the users' friends, and friends of friends. It was suggested in [23] that if the goal of policy is to adequately protect privacy, then we need policies that protect individuals with minimal requirements of informed and rational decision making that include a baseline framework of protection. In [24], a model for small-world networks regarding information epidemics was proposed to analyze the mixed behaviors of delocalized infection and ripple-based propagation for hybrid malware in generalized social networks consisting of personal and spatial social relations. A number of other works have analyzed the spread of user behavior based on the epidemic spreading theory or social contagion [25]–[27].

B. Contribution

Most current research on privacy protection and behavior spreading considers a social network of a regular, random, and flattened topology. Based on this assumption, individuals connect with each other, and the influence of users' actions and behaviors is spread over the entire social network accordingly. However, in a real social network, the relationships among users are much more complicated than these simple models. Moreover, the interaction and influence between any two users largely depends on how close the relationship between these two users is. In this research, we model the population of social networks as a community structure in order to characterize the connections of users in a more appropriate and accurate way. By this community structure based model, we may successfully analyze the spreading of the privacy protection behavior over the social network.

The main contributions of this paper include:

- We propose a game theoretic framework to model the interaction and influence when users choose strategies that make use of the privacy protection or not. The framework reveals that the protection of the users' privacy information depends not only on the users' own strategies, but also strategies of other users. In other words, the framework can analyze the information protection through users' interactions and decision making.

- We establish a community structure based evolutionary game theory to model and analyze the privacy protection over social networks with a community structured population. This framework can characterize the dynamics of the process of the users' behaviors regarding taking the privacy protection or not. In addition, the framework can also predict the final stable behavior spreading state.
- Based on the proposed community structure based evolutionary game theory framework, we analyze the dynamics of the users' behaviors with regard to taking the privacy protection or not. The critical cost performance is analyzed for both non-triggering game and triggering game scenarios. The critical cost performance is an important parameter, exceeding the value of which the behavior of taking the privacy protection is more frequent than the behavior of not taking the privacy protection in the equilibrium distribution of the deviation-imitation process in the social network.

The rest of this paper is organized as follows. In Section II, the community structure based evolutionary game formulation of privacy protection in social networks is described. The privacy protection among users belonging to K communities and evolution of security behavior are analyzed in Section III. Then we extend the model to a triggering interaction scenario in Section IV. Simulations are shown in Section V, and conclusions are drawn in Section VI.

II. Community Structure Based Evolutionary Game Formulation

A. Basic Concept of Evolutionary Game

Consider an evolutionary game with r strategies $\chi = \{1, 2, \cdots, r\}$ and a payoff matrix $\mathbf{U}$, which is an $r \times r$ matrix with entry u_{mn} denoting the payoff for strategy m versus strategy n. The system state of the game can be denoted as $\mathbf{p} = [p_1, p_2, \cdots, p_r]^{\mathrm{T}}$. In this case, the average mean payoff within a population in state $\mathbf{q} = [q_1, q_2, \cdots, q_r]'$ against a population in state $\mathbf{p}$ is $\mathbf{q}'\mathbf{U}\mathbf{p}$.

Definition 1 (Evolutionary Stable State, ESS): A state p^* is an ESS, if and only if $\mathbf{p}^*$ satisfies following conditions for all different states $\mathbf{q} \neq \mathbf{p}$ [28]:

$$\begin{aligned} &\mathbf{q}'\mathbf{U}\mathbf{p}^* \le \mathbf{p}^{*\prime}\mathbf{U}\mathbf{p}^*, \\ \textit{if } &\mathbf{q}'\mathbf{U}\mathbf{p}^* = \mathbf{p}^{*\prime}\mathbf{U}\mathbf{p}^*, \quad \mathbf{p}^{*\prime}\mathbf{U}\mathbf{q} > \mathbf{q}'\mathbf{U}\mathbf{q}. \end{aligned} \tag{1a}$$

In Definition 1, first condition (1a) is equivalent to the Nash equilibrium condition, and ensures that the average payoff of the population in ESS $\mathbf{p}^*$ is not smaller than the average payoff of the population in a different strategy $\mathbf{q}'$ against $\mathbf{p}^*$. The second condition (1a) further guarantees the stability of ESS $\mathbf{p}^*$ in case of equality in the equilibrium condition. Solving the ESS is an important problem in an evolutionary game [29], [30]. An approach to this problem is to find the stable point

$$\mathbf{p}^* = \arg_{\mathbf{p}} \left(d\mathbf{p}/dt = 0 \right) \tag{2}$$

of the network mean dynamics, which specifies that the rate of change in the use of each strategy equals to zero [31], [32]. In this work, we analyze the frequency of users taking different strategies over several times of updates in Section III. The network evolves and updates according to the following process, which is similar to the Wright-Fisher process [33]–[35]. The users with evolutionary behaviors and community memberships are considered as discrete and non-overlapping updated generations, and the number of users is constant. All users update at the same time. Users reproduce their own decisions in the new update proportional to their fitness [36], which means that if the user has a higher fitness, he/she tends to maintain his/her current strategy and community memberships in the following update with a high probability. Consider that when an offspring user adopts the imitated user's strategy and community memberships, he/she might select the opposite strategy or different communities, which is similar to the conception of "mutation" in genetic theory [37]. Denote u as the probability with which an offspring adopts a random security strategy, i.e., selecting the security service or not. Then an offspring will adopt the imitated user's strategy with probability $1 - u$. Similarly, denote υ as the probability with which a user adopts a random community memberships, which includes that of the imitated user. Then a user adopts the imitated user's configuration with probability $1-\upsilon$. Notice that the probability that any possible configuration of community membership is selected is $\upsilon/\binom{M}{K}$.

B. Community Structured Evolutionary Game Formulation

Assume that a social network can provide a higher grade of security, i.e., privacy protection, for users' privacy besides the basic services. This additional security service for user privacy protection means applying more advanced encryption and anonymization, secure database management and dissemination, and personal privacy protection techniques to data processing on the user privacy information. When users take this security service, they need to accept terms ruled by the network, such as that users have to provide more personal information, complete real-name authentication or pay for the service. Then they can get more privacy protection when other legitimate or malicious persons and organizations access or use their personal and privacy information. The more personal information provided by one user to the social network managers, the more secure authentication will be required when stealing his/her information, and as a result, the better privacy protection can be achieved for this user. In most real social networks, these kinds of additional services are not mandatory, and users are therefore free to accept such services or not, according to users' own judgements. For instance, users of many forum websites are usually required to provide a mobile phone number or e-mail address to get a higher level of the user information security service, although this service is not mandatory.[1]

[1] Current social networks have provide some privacy protection measures for their users. For instance, there are many optional settings in "Privacy Settings and Tools" of Facebook. However, such protection tends to be weak when the users' privacy information are suffering professional or specialized attacks of hackers. The privacy protection service provided by network managers mentioned in our work refers to the high-level technical protection for the user's privacy, not just simple options by users without any pay.

In current social networks, users are allowed to join multiple but a limited number of communities according to their professions, living or touring locations, expertise, or personal interests, etc. For instance, the Google Circles and Facebook Groups can be considered as establishing different communities or some kinds of relationships for their users. We consider that these users are classified by their categories of groups, which can be termed communities of the population structure, and the friendships are established among users in the same community. Therefore, each user holds multiple friendship relations with the users in the same community. The degree of closeness in the relationship between two users can be measured by the number of communities they share. Take users in Google Groups for instance, if User A and User B are both in the Group "Arts and Entertainment" and Group "Schools and Universities" at the same time, then we can consider that the relationship between A and B is stronger than that between B and C, who only belong to Group "Arts and Entertainment" in common. In addition, the information shared between A and B will typically be more than that between B and C. Assume that users are allowed to change communities, which can be influenced by their own or other users' actions. Consider that user interactions can only happen between individuals belonging to the same community, i.e., having some kinds of friend relationships in a social network. Interaction among users in this work refers to the influence of their friends and their own strategies, i.e., the payoff obtained through the game. In addition, some of users' information, such as personal information and status, is accessible only to their friends.

Based on these premises above, we assume that the information of both of a user and his/her friends can be protected by the network to some extent if the user makes use of the privacy protection, even if his/her friends do not take the same action. We assume that, the user taking the privacy protection can obtain this service by paying a price as a deal with the network manager. Meanwhile, the privacy information of his/her friends can also be protected by the network no matter whether these friends take the privacy protection service or not. Taking WeChat for instance, the Moments (similar to the Timeline of Facebook) of a user can only be seen by his/her friends, and the Group Chat can be organized by one user among his/her friends, not matter whether these friends are also friends with each other or not. In addition, Facebook provides an optional setting in "Privacy Settings and Tools": Who can see your friends list, which can illustrate that user's security behavior makes sense on the information protection of his/her friends. The closer the relationship is, the more personal information of the user can be accessed by his/her friends. If the user's friend makes use of the privacy protection or some other information security services, the accessible information of this user can be also protected at some level. The more accessible information for his/her friend, the more information can be protected, even when this user does not take the privacy protection. In this work, we assume that the privacy protection service not only protects the information of the users who select this service, but also the information these users can access, i.e., the information of their friends. Therefore, if the user does not select the service, the personal information of his/her friends will also be threatened by this user's unsafe strategies.

Privacy protection over a social network shares fundamental similarities with the strategy updating in the community-structured evolutionary game theory (EGT). We consider users in a social network as the players in the evolutionary game. Each of these users has two possible strategies, i.e., to take or not take the privacy protection provided by the network:

$$\begin{cases} \mathbf{S}_p, & \text{take the privacy protection,} \\ \mathbf{S}_n, & \text{do not take the privacy protection.} \end{cases} \tag{3}$$

The strategy taking the privacy protection can be considered as the secure behavior, and otherwise, insecure behavior. Meanwhile, the users' payoff matrix can be defined as

$$\begin{array}{ccc} & \mathbf{S}_p & \mathbf{S}_n \\ \mathbf{S}_p & \beta b - c & b - c \\ \mathbf{S}_n & b & 0 \end{array}, \tag{4}$$

where $b > 0$ is the baseline security benefit received by the user resulting from that this user or this user's friends take the privacy protection (security behavior). For existing social networks, b can be set as traditional measurements of privacy, such as disclosure risk and information loss, when applying current encryption, anonymization, secure database management and dissemination techniques. $c > 0$ denotes the cost that users taking the privacy protection need to pay for the protection service, which could be more personal information providing, real-name authentication and payment as required by current social networks. On the other hand, if the privacy protection service is provided through an application (APP) update, which is a common approach adopted by WeChat, Twetter and other existing social networks, the cost for user to take the service can be then measured by the increasing memory occupancy of the latest APP version. In addition, when both of the interacted users take strategy $\mathbf{S}_p$, two of them will obtain higher level privacy safety benefit βb as the first entry of the payoff matrix shown in (4), where $\beta > 1$. The payoff will be zero when both of the interacted friends are defectors, i.e., neither of them selects the privacy protection service, then no pay or gain for them.

Based on the definitions of the strategies and payoff above, ratio b/c or $\beta b/c$, which can be defined as the *cost performance*, is a crucial parameter. It can help the social network managers to make appropriate security service level and payment mechanism to encourage their users to accept the security service, and then promote the spreading of this secure behavior. In a community structured population well-mixed, any two individuals belonging to the same community interact with equal likelihood. Then as reflected in (4), users taking the privacy protection would be out-competed by those users doing not. Therefore, the interaction between users with security behavior and with insecurity behavior needs to be investigated, and the question that whether dynamics on a community structured population allows the evolution of security behavior needs to be figured out.

Consider a social network with N users. The number of communities operated by the social network is M.

However, users of current social networks are only allowed to join a limited number of these communities. Then we set that each user belongs to exactly K communities, where $K \leq M$. In addition, each user has a strategy index $s_i \in \{0, 1\}$, which is defined as that $s_i = 1$ when user i take the privacy protection strategy $\mathbf{S}_p$, or $s_i = 0$, otherwise. Then the state of the social network can be given by a strategy vector $\mathbf{s} = [s_1, s_2, \cdots, s_N]$ and a matrix Θ. Θ is an $N \times M$ matrix, whose entry θ_{im} ($i = 1, 2, \cdots, N$, $m = 1, 2, \cdots, M$) is 1 if user i belongs to community m, and $\theta_{im} = 0$, otherwise. Matrix Θ can be represented as $\Theta = [\theta_1, \theta_2, \cdots, \theta_N]^{\mathrm{T}}$, where θ_i is the vector giving the community membership of user i. Then the number of communities that user i and user j having in common can be expressed by the dot product of their community membership vector, as $\theta_i \cdot \theta_j$. In addition, based on the definition of K, we have $\theta_i \cdot \theta_i = K$, $\forall i$. The state of the social network can be given as $S = (\mathbf{s}, \Theta)$.

We assume the influence of user j on i $(i \neq j)$ is related to the number of communities that they share in common. Specifically, user i's fitness obtained by j is proportional to the total utility according to (4), and the proportional coefficient is the number of communities that i and j share in common. In addition, user i interacts with user j only when they share at least one community in common, i.e., $\theta_i \cdot \theta_j \neq 0$. Then the total fitness of user i of the community-structured social network can be written as

$$\begin{aligned}\pi_i &= 1 + \alpha \sum\nolimits_{j \neq i} (\theta_i \cdot \theta_j) \left[(\beta b - c) s_i s_j + (b - c) s_i \left(1 - s_j\right) \right. \\ &\quad \left. + b\,(1 - s_i)\, s_j \right] \qquad (5) \\ &= 1 + \alpha \sum\nolimits_{j \neq i} (\theta_i \cdot \theta_j) \left[(\beta - 2)\, b s_i s_j + (b - c)\, s_i + b s_j \right],\end{aligned}$$

where α represents the selection intensity, i.e., the relative contribution of the game to fitness. The case $\alpha = 1$ denotes the strong selection, which means that the payoff obtained through (4), i.e., the game among users with strategies $\mathbf{S}_p$ and $\mathbf{S}_n$, plays an dominant contribution to the total fitness of every user, and then the user with high payoff will be chosen and imitated with high probability. On the contrary, $\alpha \to 0$ denotes the weak selection [38]. Under the weak selection, the payoff obtained through (4) has limited contribution to the total fitness of each user. In this work, we only analyze the weak selection case as the results derived from weak selection are often valid approximations for stronger selection [39]. In addition, the weak selection scenario can be more helpful to reveal the user behavior spreading over social networks [19].

As an example shown in Fig. 1, there are $N = 5$ users, denoted by U_1 - U_5, over $M = 4$ communities as ellipses A, B, C and D. Each user belongs to $K = 2$ communities. The community memberships determine how users interact each other, and the broken lines indicate the weighted interaction. The structure changes as users updating in discrete time slot. In this example, U_1, U_3 and U_5 take the same security strategy, and the other users take the opposite strategy at the first time slot. During the update process, imitator U_1 picks another user U_2, and adopts U_2's security strategy and community associations.

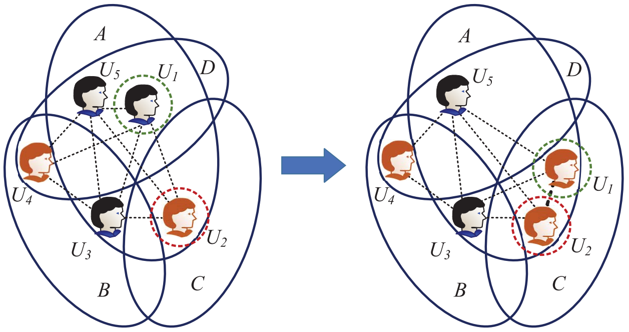


Fig. 1. An example of security strategy and associations evolution over a social network with a community structured population.

TABLE I

CORRESPONDENCE BETWEEN COMMUNITY STRUCTURED EVOLUTIONARY THEORY AND SOCIAL NETWORK

Community-structured EGT	**Social Network**
Community-structured population	Social network with friendships classified by communities
Players	Users in the social network
Strategies	$\mathbf{S}_p$: take the privacy protection $\mathbf{S}_n$: do not take the privacy protection
Fitness	Utility from taking the privacy protection or not
ESS	Stable security behavior state over users

Table I indicates the correspondence between the elements in the community structured evolutionary game theory and those in the social network, whose users hold relationships according to their interested communities. Based on the definitions above, we can derive the expression for the critical cost performance, which is an important parameter that determines the stable security behavior state of the users among the network. In the following section, we will analyze the critical cost performance for the social network where games exist among all users in the same community. In other words, the security strategy of a user can only influence the payoff of his/her friends who share at least one common community with this user. Moreover, the critical cost performance for the situation named "L-triggering game" will be further analyzed in the later part of this work.

III. Privacy Protection Among Users Belonging to K Communities

In this section, we study the evolution of users' behaviors that take the privacy protection or not over social networks using the evolutionary game theory based on the community structured population. In the uniform scenario, a social network with N users, each of whom belongs to exactly K communities, is considered in this section. We define the network user state as $(p, 1 - p)$, where p is the frequency of the users those select to take the privacy protection (choose strategy $\mathbf{S}_p$), and $1 - p$ are the others (choose strategy $\mathbf{S}_n$). Our ultimate goal is to derive the evolutionary stable network state $(p^*, 1 - p^*)$ that ensures the evolution of security behavior, i.e., users select strategy $\mathbf{S}_p$ more frequently than $\mathbf{S}_n$.

A. Evolution of Security Behavior on Communities

First, we summarize the key conceptions in the spreading of the privacy protection behavior when applying evolutionary game into social networks.

Update: Assume that users can change their community memberships and security behaviors to get better user security experience. This change can be considered as the update.

Imitation: In social networks, the imitation of other users' behaviors plays an important role in behavior spreading. By times of updates, the behavior with higher fitness can spread among the users in the network. Specifically, a user's community membership and security behavior can bring high fitness for the user, which means that the security behaviors of this user and his/her friends obtain a relative high level of privacy protection. Then for the security concern, other users will tend to imitate this user's community membership and security behavior. Similarly, the user will maintain his/her own community membership and security behavior if the current fitness is rather high, which means that the user will imitate hiself/herself.

Deviation: Deviation means that the user does not imitate the community membership or community membership of the users being imitated, who can be himself/herself and other users with high fitness. The community and strategy deviation can also make sense on the behavior spreading. On the one hand, when a user imitate another one for a better security experience, he/she only imitates the community membership. This user might not change his/her previous security behavior, i.e., he/she still not take the privacy protection to just get security benefit brought by friends, or still take the privacy protection to get more benefit brought by new communities. On the other hand, a user might only imitate another user's security behavior but not change some or all of his/her previous communities because of interests. These two situation bring security behavior (strategy) deviation and community deviation, respectively, as mentioned in Section II-A. We still use u and v to denote the rates of strategy deviation and community deviation, respectively.

We consider that user i is an imitated user with the probability proportional to its fitness, which can be given by its payoff relative to the total payoff, i.e., $\pi_i / \sum_j \pi_j$. Assume that both the imitation and deviation are implemented independently N times in each update step. Denote the average number of imitators of user i as ω_i. After one update step, we have

$$\omega_i = \frac{N\pi_i}{\sum_j \pi_j}. \tag{6}$$

According to Equation (5), the total payoff can be written as

$$\begin{aligned}
\sum_j \pi_j &= \sum_j \left[1+\alpha \sum_{l\neq j} (\theta_j \cdot \theta_l)\, f(s_j, s_l)\right] \\
&= N+\alpha \sum_j \left[\sum_l (\theta_j \cdot \theta_l) f(s_j, s_l) - (\theta_j \cdot \theta_j) f(s_j, s_j)\right] \\
&= N+\alpha \sum_j \sum_l (\theta_j \cdot \theta_l)\, f(s_j, s_l) \\
&\quad - \alpha \sum_j K\left[(\beta-2)\, b s_j s_j + (2b-c)\, s_j\right] \\
&= N+\alpha \sum_j \sum_l (\theta_j \cdot \theta_l) f(s_j, s_l) - \alpha K\,(\beta b - c) \sum_j s_j,
\end{aligned} \tag{7}$$

where

$$f(s_i, s_j) = (\beta-2)\, b s_j s_l + (b-c)\, s_j + b s_l, \tag{8}$$

and the last term in Equation (7) is obtained considering $s_j s_j = s_j$, $\forall j$. We consider the weak selection situation, i.e., $\alpha \to 0$, because of that results derived from the weak selection often remain as valid approximations for large selection strength [40]. In addition, the weak selection assumption helps to achieve a close-form analysis of spreading process and reveal how the behavior spreads over the social network [19]. Then we can rewrite ω_i in Equation (6) as

$$\begin{aligned}
\omega_i = 1+\alpha\Big[&(\beta-2)\, b \sum_j (\theta_i \cdot \theta_j)\, s_i s_j + (b-c) \sum_j (\theta_i \cdot \theta_j)\, s_i \\
&+ b \sum_j (\theta_i \cdot \theta_j) s_j - K(\beta b - c) s_i - \frac{(\beta-2)b}{N} \sum_j \sum_l (\theta_j \cdot \theta_l) s_j s_l \\
&- \frac{2b-c}{N} \sum_j \sum_l (\theta_j \cdot \theta_l)\, s_j + \frac{K(\beta b - c)}{N} \sum_j s_j\Big] + o\left(\alpha^2\right),
\end{aligned} \tag{9}$$

where the third equality is according to Taylor's Theorem and weak selection assumption with $\alpha \to 0$. The proof of Equation (9) is provided in Appendix A.

To find out the ESS of the system state dynamic, we let p denote the frequency of the users those select to take the privacy protection. As assumed previously, there exist two situations in the update process of the social network state, one is the imitation of another user's community membership and security decision or the maintenance of his/her own, and the other is the deviation. So we need to analyze the effect of imitation and deviation on the average change in p. Because of that the average value of p is constant, the two effects must cancel [37]. Then we can get

$$\langle \hat{p} \rangle_{\text{imi}} + \langle \hat{p} \rangle_{\text{dev}} = 0, \tag{10}$$

where $\langle \hat{p} \rangle_{\text{imi}}$ and $\langle \hat{p} \rangle_{\text{dev}}$ denote the effect of imitation and deviation, respectively, and they are both the continuous functions of α.

Next, we consider the weak selection situation that $\alpha = 0$, and Taylor expansion of $\langle \hat{p} \rangle_{\text{imi}}$ can be written as

$$\langle \hat{p} \rangle_{\text{imi}} = 0 + \alpha \langle \hat{p} \rangle_{\text{imi}}^{(1)} + o\left(\alpha^2\right), \tag{11}$$

where $\langle \hat{p} \rangle_{\text{imi}}^{(1)}$ is the first derivative of $\langle \hat{p} \rangle_{\text{imi}}$ with $\alpha = 0$, and $o\left(\alpha^2\right)$ is according to Taylor's Theorem. We notice that when $\langle \hat{p} \rangle_{\text{imi}}^{(1)} > 0$, the amount of users who take the privacy protection due to the imitation increases, which means that the user's decision tends to the security behavior. On the contrary, if $\langle \hat{p} \rangle_{\text{imi}}^{(1)} < 0$, the user's decision tends to not taking the privacy protection.

B. Finding the Critical Ratio

In order to obtain the critical parameter value of cost performance, we must have $\langle \hat{p} \rangle_{\text{imi}}^{(1)} = 0$. The Lemma 1 provides the critical cost performance b/c in the limit of weak selection.

Lemma 1: In a social network with N users, every user belongs to exactly K communities. There are two strategies $\mathbf{S}_p$ and $\mathbf{S}_n$ for users. The state of the social network is given as $S = (\mathbf{s}, \Theta)$. Interactions are only allowed among users sharing communities in common. For each user, the payoff matrix is given by (4). The critical cost performance that keeps the neutral stationary state, i.e., the frequencies of users selecting strategies $\mathbf{S}_p$ and $\mathbf{S}_n$ approaches stable state, is given by

$$\left(\frac{b}{c}\right)^* = \frac{Num}{Den}, \tag{12}$$

In Equation (12),

$$Num = -K\langle f_1\rangle_0 + \frac{K}{N}\langle f_2\rangle_0 + \langle f_3\rangle_0 - \frac{1}{N}\langle f_5\rangle_0, \quad (13)$$

$$Den = -\beta K\langle f_1\rangle_0 + \frac{\beta K}{N}\langle f_2\rangle_0 + \langle f_3\rangle_0 + (\beta-1)\langle f_4\rangle_0 - \frac{2}{N}\langle f_5\rangle_0 - \frac{\beta-2}{N}\langle f_6\rangle_0, \quad (14)$$

where

$$f_1 = \sum\nolimits_i s_i, \quad f_2 = \sum\nolimits_{i,j} s_i s_j, \quad (15a)$$

$$f_3 = \sum\nolimits_{i,j}\left(\theta_i\cdot\theta_j\right)s_i, \quad f_4 = \sum\nolimits_{i,j}\left(\theta_i\cdot\theta_j\right)s_i s_j, \quad (15b)$$

$$f_5 = \sum\nolimits_{i,j,l}\left(\theta_j\cdot\theta_l\right)s_i s_j, \quad f_6 = \sum\nolimits_{i,j,l}\left(\theta_j\cdot\theta_l\right)s_i s_j s_l, \quad (15c)$$

In Equation (13) and (14), the angular bracket with a subscript zero represents the average value among all possible states S. Take f_3 for instance,

$$\left\langle\sum\nolimits_{i,j}\left(\theta_i\cdot\theta_j\right)s_i\right\rangle_0 = \sum\nolimits_S\left(\sum\nolimits_{i,j}\left(\theta_i\cdot\theta_j\right)s_i\,|_{\alpha=0}\right)\cdot q_S^{(0)}, \quad (16)$$

where q_S denotes the probability that the network is in state S [37].

Proof: See Appendix B.

Remarks: In a social network whose current state S, i.e., the users' community memberships and security behaviors, can change with every update, Equation (12) shows the threshold of the security protection cost performance. This parameter can be controlled by the social network manager, either by adjusting the price of the security service that is related to the parameter c, or by providing sufficient security services benefit that is related to the parameter b. Note that the expression of cost performance provided in Lemma 1 hold the weak selection situation i.e., $\alpha \to 0$. Compared with [37], in which a simplified Prisoners Dilemma game was analyzed, more situations are considered in our game model. Next, we will analyze the neutral stationary state and get the more general expression of cost performance. Theorem 1 states the desired term of cost performance $\beta b/c$.

Theorem 1: In a social network with N users, every user belongs to exactly K communities. There are two strategies $\mathbf{S}_p$ and $\mathbf{S}_n$ for users. Interactions are only allowed among users sharing communities in common. For each user, the payoff matrix is given by (4). The deviate rates of community membership imitation and strategy imitation are given by v and u, respectively. The critical cost performance that keeps the neutral stationary state is given by

$$\left(\frac{\beta b}{c}\right)^* = 1 + \frac{\mu+\upsilon+3}{\mu+\upsilon+1}\cdot\frac{K\upsilon\left(\mu+\upsilon+2\right)+M\left(\mu+1\right)}{K\upsilon\left(\mu+\upsilon+2\right)+M\left(\mu+2\upsilon+3\right)}, \quad (17)$$

where $\upsilon = 2Nv$ and $\mu = 2Nu$.

Proof: To proof Theorem 1, each term of Equation (15) needs to be analyzed. First, we consider that $\langle f_1\rangle_0$ is the average number of the users taking the privacy protection and can be given by

$$\langle f_1\rangle_0 = N/2. \quad (18)$$

For $\langle f_2\rangle_0$, we notice that $\langle f_2\rangle_0 = N^2\Pr\left(s_i = s_j = 1\right)$. In a neutral stationary state, the probabilities of both of user i and j select to take the privacy or not are equal, i.e., $\Pr\left(s_i = s_j = 1\right) = \Pr\left(s_i = s_j = 0\right) = \Pr\left(s_i = s_j\right)/2$. User i and j are selected randomly to be analyzed, and the replacement is allowed. So we can get

$$\langle f_2\rangle_0 = \left(N^2/2\right)\Pr\left(s_i = s_j\right). \quad (19)$$

Similar to the analysis above, we can get

$$\langle f_3\rangle_0 = N^2\left\langle\theta_i\cdot\theta_j\mathbf{1}\left(s_i = 1\right)\right\rangle_0 = \left(N^2/2\right)\left\langle\theta_i\cdot\theta_j\right\rangle_0, \quad (20)$$

where $\mathbf{1}(\cdot)$ is the indicator function, the value of which is 1 if the argument is true, and 0, otherwise. This indicator function introduces a non-zero contribution. So $\left\langle\theta_i\cdot\theta_j\mathbf{1}\left(s_i = 1\right)\right\rangle_0$ indicates the average number of communities that user i and j belong in common under the situation that the first user i takes the privacy protection. $\left\langle\theta_i\cdot\theta_j\right\rangle_0$ represents the average number of communities that the two users belong in common. With the same analysis for Equation (18) - (20), we can get other terms of (15) as follows.

$$\langle f_4\rangle_0 = \left(N^2/2\right)\left\langle\theta_i\cdot\theta_j\mathbf{1}\left(s_i = s_j\right)\right\rangle_0, \quad (21a)$$

$$\langle f_5\rangle_0 = \left(N^3/2\right)\left\langle\theta_j\cdot\theta_l\mathbf{1}\left(s_i = s_j\right)\right\rangle_0, \quad (21b)$$

$$\langle f_6\rangle_0 = \left(N^3/2\right)\left\langle\theta_j\cdot\theta_l\mathbf{1}\left(s_i = s_j = s_l\right)\right\rangle_0. \quad (21c)$$

Equation (21a) provides the average number of communities that the two random users have in common, and the case that the two users select the same security behavior (both or neither of the users take the privacy protection) give the non-zero contribution to the average. In both of Equation (21b) and (21c), three random users are considered. So the sum has N^3 terms. Equation (21b) provides the average number of communities that latter two users j and l have in common, and the non-zero contribution to the average is given by the case that first two users i and j select the same security behavior. Equation (21c) is the average number of communities that latter two users j and l have in common, and the non-zero contribution to the average is given by the case that all these three users take the same security behavior. The three users are selected randomly and with replacement.

Next, we need to calculate the terms obtained in Equation (18) - (21c) in the case that three users are selected to be analyzed without replacement, i.e., $i \neq j$ and $i \neq j \neq l$. For convenience, we give some notations as follows.

$$\varphi = \Pr\left(s_i = s_j\,|i \neq j\right), \quad (22a)$$

$$\psi = \left\langle\theta_i\cdot\theta_j\,|i \neq j\right\rangle_0, \quad (22b)$$

$$\gamma = \left\langle\theta_i\cdot\theta_j\mathbf{1}\left(s_i = s_j\right)|i \neq j\right\rangle_0, \quad (22c)$$

$$\xi = \left\langle\theta_j\cdot\theta_l\mathbf{1}\left(s_i = s_j\right)|i \neq j \neq l\right\rangle_0, \quad (22d)$$

$$\eta = \left\langle\theta_j\cdot\theta_l\mathbf{1}\left(s_i = s_j = s_l\right)|i \neq j \neq l\right\rangle_0. \quad (22e)$$

In (22), ψ is the average number of communities two different randomly picked users have in common. γ is the average number of communities the two users have in common given that only users with the same security behavior. For ξ and η, there are three different users considered. ξ is the average number of communities the latter two users belonging in common given that only the first two users have the same security behavior. η is the average number of communities the latter two users having in common given that there is a non-zero contribution to the average only when all the three users take the same security behavior.

Given two users, the probability that the same user is chosen again in the second selection experience is $1/N$. Then we get

$$\Pr\left(s_i = s_j\right) = \frac{1}{N} + \frac{N-1}{N}\varphi, \tag{23a}$$

$$\left\langle\theta_i \cdot \theta_j\right\rangle_0 = \frac{K}{N} + \frac{N-1}{N}\psi, \tag{23b}$$

$$\left\langle\theta_i \cdot \theta_j \mathbf{1}\left(s_i = s_j\right)\right\rangle_0 = \frac{K}{N} + \frac{N-1}{N}\gamma. \tag{23c}$$

Then for the situation that three users i, j and l are given, the probability that both of the last two users are same as the first selection is $N_1 = 1/N^2$. The probability that none of the users chosen in the second and third selection is same as the one in the first selection is $N_2 = (N-1)(N-2)/N^2$. The probability that the user chosen in the second selection is same as the one in the first selection, and the third selection chooses the different user is $N_3 = (N-1)/N^2$. Then we get

$$\left\langle\theta_j \cdot \theta_l \mathbf{1}\left(s_i = s_j\right)\right\rangle_0 = N_1 K + N_2 \xi + N_3\left(\psi + \gamma + K\varphi\right), \tag{24a}$$

$$\left\langle\theta_j \cdot \theta_l \mathbf{1}\left(s_i = s_j = s_l\right)\right\rangle_0 = N_1 K + N_2 \eta + N_3 (2\gamma + K\varphi). \tag{24b}$$

According to (23a) - (24), terms in (63) can be calculated as:

$$\langle f_2\rangle_0 = \frac{N^2}{2}\left(\frac{1}{N} + \frac{N-1}{N}\varphi\right), \tag{25a}$$

$$\langle f_3\rangle_0 = \frac{N^2}{2}\left(\frac{K}{N} + \frac{N-1}{N}\psi\right), \tag{25b}$$

$$\langle f_4\rangle_0 = \frac{N^2}{2}\left(\frac{K}{N} + \frac{N-1}{N}\gamma\right), \tag{25c}$$

$$\langle f_5\rangle_0 = \frac{N^3}{2}\left[N_1 K + N_2 \xi + N_3\left(\psi + \gamma + K\varphi\right)\right], \tag{25d}$$

$$\langle f_6\rangle_0 = \frac{N^3}{2}\left[N_1 K + N_2 \eta + N_3\left(2\gamma + K\varphi\right)\right]. \tag{25e}$$

By calculating, φ is eliminated, and the critical ratio b/c expressed by ψ, γ, ξ and η is given as

$$\left(\frac{b}{c}\right)^* = \frac{\psi - \xi + \frac{\psi-\gamma}{N-2}}{\psi - 2\xi - (\beta-2)\eta + (\beta-1)\gamma + \frac{\gamma-\psi}{N-2}}. \tag{26}$$

When the population of the social network is large, i.e., $N \to \infty$, we have

$$\left(\frac{b}{c}\right)^*_{N\to\infty} = \frac{\psi - \xi}{\psi - 2\xi - (\beta-2)\eta + (\beta-1)\gamma}. \tag{27}$$

Next, we will calculate each quantity of ψ, γ ξ and η. According to the physical interpretations of these parameters, we notice that all of them cannot be written as independent products of the average number of common communities times the probability of taking the same security decision. In response, we introduce a time instant that users' most recent common user being imitated (MRCI). Then if we fix the time to the MRCI, the community deviations and strategy deviations are independent. Take γ for instance, if the time to the MRCI of users i and j is $T = t$, then we get

$$\begin{aligned}&\left\langle\theta_i \cdot \theta_j \mathbf{1}\left(s_i = s_j\right) | i \neq j, T = t\right\rangle_0 \\ &\quad = \left\langle\theta_i \cdot \theta_j \,|\, i \neq j, T = t\right\rangle_0 \cdot \Pr\left(s_i = s_j \,|\, i \neq j, T = t\right).\end{aligned} \tag{28}$$

So if the time to users' MRCI is given, we can calculate ψ, γ, ξ and η. Given some randomly selected users, Lemma 2, Lemma 3 and Lemma 4 present the probability of users' MRCI, the probability that users have the same security behavior at the time from their MRCI and the average number of communities two random users have in common, respectively. These results are summarized from [37], in which detailed explanation can be found.

Lemma 2: Consider a social network with N users. Given two random users, the probability that their MRCI is at time T = t is

$$\Pr(T = t) = \left(1 - \tfrac{1}{N}\right)^{t-1}\tfrac{1}{N}. \tag{29}$$

Given three random users, the probability that the first merging by imitating the same user's communities and strategy happens at time $t_1 \geq 1$ and the second takes $t_2 \geq 1$ more time steps is

$$\Pr(t_1, t_2) = \tfrac{3}{N^2}\left[\left(1 - \tfrac{1}{N}\right)\left(1 - \tfrac{2}{N}\right)\right]^{t_1-1}\left(1 - \tfrac{1}{N}\right)^{t_2}. \tag{30}$$

When $N \to \infty$, let $\tau = t/N$, $\tau_1 = t_1/N$ and $\tau_2 = t_2/N$, the distributions of $\Pr(T = t)$ *and* $\Pr(t_1, t_2)$ *are given by*

$$p(\tau) = e^{-\tau}, \tag{31a}$$

$$p(\tau_1, \tau_2) = 3e^{-(3\tau_1 + \tau_2)}. \tag{31b}$$

Remarks: Lemma 2 indicates that the MRCI for random two and three users situations both have exponential distributions. The physical meaning of MRCI is the the most current common user affected and imitated by another two users. Note that the introduction of MRCI is for the independence between the community deviations and strategy deviations, which makes the calculation of ψ, γ ξ and η defined in Equation (22) feasible, and time indexes τ, τ_1 and τ_2 will be removed by the integral. Equation (31a) and (31b) hold for the limit of $N \to \infty$, which is rational for social networks with large number of users.

Lemma 3: In a social network with N users, every user belongs to exactly K communities, where $K \leq M$. The deviate rate of strategy imitation is given by u. The probability that two random users have the same strategy at time t from their MRCI is given by

$$\varphi(t) = \Pr\left(s_i = s_j \,|\, T = t\right) = \frac{1}{2}\left[1 + (1-u)^{2t}\right]. \tag{32}$$

When $N \to \infty$, let $\tau = t/N$, $\tau_1 = t_1/N$ and $\tau_2 = t_2/N$, the distributions is

$$\varphi(\tau) = \frac{1}{2}\left(1 + e^{-\mu\tau}\right), \tag{33}$$

where $\mu = 2Nu$. Given that the first merging by imitating the same user happens at time $t_1 \geq 1$ and the second takes $t_2 \geq 1$ extra time steps, the distribution of the probability that three random users have the same strategy is given by

$$\varphi(\tau_1, \tau_2) = \frac{1}{8}\left[(1-e_1)^2(1-e_2) + (1+e_1)^2(1+e_2)\right], \tag{34}$$

where $e_1 = \exp\left\{-\frac{\mu}{2}\tau_1\right\}$, $e_2 = \exp\left\{-\frac{\mu}{2}(\tau_1+\tau_2)\right\}$, $\mu = 2Nu$.

Remarks: Equation (33) in Lemma 3 indicates that at $\tau < \infty$ after the time when two users imitated the same other user, these two users have the same security behavior with the probability more than 0.5. The shorter τ is, the larger the probability is, and the probability is an exponential distribution. Equation (34) has similar properties. Both of the two equations hold for the $N \to \infty$ and $u \to 0$ limits. $N \to \infty$ is reasonable for most social networks. $u \to 0$ indicates that if a user imitates another user, he/she selects this user's security behavior with high probability. This means that the security behaviors with high fitness can spread over the social network, which is a favorable state for the social network manager.

Lemma 4: Consider a social network with N users distributed over M communities. Each user belongs to exactly K communities, where $K \leq M$. The deviate rate of community membership imitation is given by υ. Then the average number of communities that two random users have in common is

$$\psi(\tau) = Ae^{-\upsilon\tau} + B, \tag{35}$$

where $A = K - \frac{K^2}{M}$, $B = \frac{K^2}{M}$ *and* $\upsilon = 2N\upsilon$.

Remarks: Lemma 4 holds for the $N \to \infty$ and $\upsilon \to 0$ limits. $\upsilon \to 0$ indicates that the users' community memberships are not stable, and users participate in the imitated user's community memberships with high probability. This corresponds to the scenarios in real social networks, where some communities providing more comfortable service, such as security and information service, can attract more and more users due to the interactions and information sharing among users.

According to Lemma 2 and Lemma 4, we can calculate that

$$\psi = \langle\theta_i \cdot \theta_j \mid i \neq j\rangle_0 = \int_0^\infty \psi(\tau)\, p(\tau)\, d\tau = \frac{A}{\upsilon+1} + B. \tag{36}$$

Next, we analyze and solve γ defined as (22c). Let

$$\gamma(\tau) = \langle\theta_i \cdot \theta_j \mathbf{1}(s_i = s_j) \mid i \neq j, T = \tau\rangle_0. \tag{37}$$

As discussed above, the deviations of community membership and security behavior are independent when the time to the MRCI of users is fixed, i.e., $\gamma(\tau) = \varphi(\tau)\psi(\tau)$. Then plug Equation (33) and (35) in and we can get

$$\begin{aligned}\gamma &= \int_0^\infty \varphi(\tau)\,\psi(\tau)\,p(\tau)\,d\tau\\ &= \frac{1}{2}\left(\frac{A}{\upsilon+1} + \frac{A}{\mu+\upsilon+1} + \frac{B}{\mu+1} + B\right).\end{aligned} \tag{38}$$

Then we need to calculate ξ, for which three users i, j and l are considered. As defined in Equation (22d), ξ indicates the amount of communities the latter two users having in common given that the first two users have the same security behavior, for three distinct random users. For any three random users, they must have an MRCI. Let $T(i,j)$ be the time up to the MRCI of i and j, and $T(j,l)$ be the time up to the MRCI of j and l. We define that

$$\xi(\tau_1,\tau_2) = \langle\theta_j \cdot \theta_l \mathbf{1}(s_i = s_j) \mid i \neq j \neq l, T_1 = \tau_1, T_2 = \tau_2\rangle_0, \tag{39}$$

where T_1 and T_2 denote the time of the first and second merging by imitating other users happen, respectively. As mentioned before, the community deviations and the strategy deviations are independent if the time to the MRCI is fixed. Therefore, $\xi(\tau_1,\tau_2)$ can be expressed as a product. By looking back the time into the past, there are three cases shown in Fig. 2 for the same imitated users of three distinct users i, j and l as follows.

1) user i and j have the same imitated user first, and then they have the same imitated user with l:

$$\xi(\tau_1,\tau_2) = \varphi(\tau_1)\,\psi(\tau_1+\tau_2); \tag{40}$$

2) user j and l have the same imitated user first, and then they have the same imitated user with i:

$$\xi(\tau_1,\tau_2) = \varphi(\tau_1+\tau_2)\,\psi(\tau_1); \tag{41}$$

3) user i and l have the same imitated user first, and then they have the same imitated user with j:

$$\xi(\tau_1,\tau_2) = \varphi(\tau_1+\tau_2)\,\psi(\tau_1+\tau_2). \tag{42}$$

Each of the three cases happens with probability 1/3, so we can get ξ as

$$\begin{aligned}\xi &= \frac{1}{3}\int_0^\infty d\tau_1 \int_0^\infty p(\tau_1,\tau_2)\,(\varphi(\tau_1)\,\psi(\tau_1+\tau_2)\\ &\quad + \varphi(\tau_1+\tau_2)\,\psi(\tau_1) + \varphi(\tau_1+\tau_2)\,\psi(\tau_1+\tau_2))\,d\tau_2\\ &= \frac{1}{2}\left[\frac{A}{\mu+\upsilon+3}\left(\frac{1}{\upsilon+1} + \frac{1}{\mu+1} + \frac{1}{\mu+\upsilon+1}\right)\right.\\ &\quad \left. + \frac{A}{\upsilon+1} + \frac{B}{\mu+1} + B\right].\end{aligned} \tag{43}$$

With the similar analysis, we can find η as

$$\begin{aligned}\eta &= \frac{1}{3}\int_0^\infty d\tau_1 \int_0^\infty \varphi(\tau_1,\tau_2)\,(\psi(\tau_1) + \psi(\tau_1+\tau_2)\\ &\quad + \psi(\tau_1+\tau_2))\,p(\tau_1,\tau_2)\,d\tau_2\\ &= \frac{1}{4}\left[\frac{A}{\mu+\upsilon+3}\left(1 + \frac{2}{\upsilon+1} + \frac{4}{\mu+2} + \frac{8}{\mu+2\upsilon+2}\right)\right.\\ &\quad \left. + \frac{A}{\upsilon+1} + \frac{3B}{\mu+3}\left(1 + \frac{4}{\mu+2}\right) + B\right].\end{aligned} \tag{44}$$

According to Equation (36), (38), (43), (44) and (27), we can obtain the critical $(b/c)^*$ as

$$\left(\frac{b}{c}\right)^* = \frac{1}{\beta}\left(1 + \frac{\mu+\upsilon+3}{\mu+\upsilon+1} \cdot \frac{K\upsilon(\mu+\upsilon+2) + M(\mu+1)}{K\upsilon(\mu+\upsilon+2) + M(\mu+2\upsilon+3)}\right),$$

which equals to

$$\left(\frac{\beta b}{c}\right)^* = 1 + \frac{\mu+\upsilon+3}{\mu+\upsilon+1} \cdot \frac{K\upsilon(\mu+\upsilon+2) + M(\mu+1)}{K\upsilon(\mu+\upsilon+2) + M(\mu+2\upsilon+3)}. \tag{45}$$

For $\mu \to 0$, we have

$$\left(\frac{\beta b}{c}\right)^* = 1 + \frac{\upsilon+3}{\upsilon+1} \cdot \frac{K\upsilon(\upsilon+2) + M}{K\upsilon(\upsilon+2) + M(2\upsilon+3)}. \tag{46}$$

This completes the proof of Theorem 1.

Remarks:

1) *Properties:* Theorem 1 gives the critical cost performance $(b/c)^*$ or $(\beta b/c)^*$. In the equilibrium distribution of the imitation-deviation process, if the cost performance exceeds this critical value, the users in the social network will select the strategy of privacy protection more frequently than the

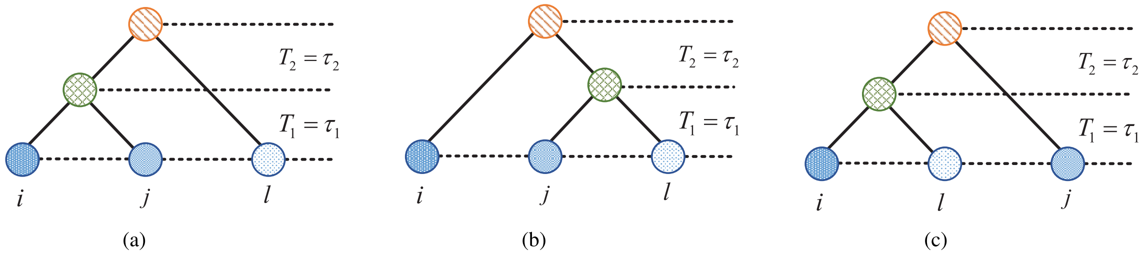


Fig. 2. Three cases of imitated users for three distinct random users i, j and l by looking back the time into the past. (a) $T(i,j)=\tau_1$, $T(j,l)=\tau_1+\tau_2$. (b) $T(i,j)=\tau_1+\tau_2$, $T(j,l)=\tau_1$. (c) $T(i,j)=\tau_1+\tau_2$, $T(j,l)=\tau_1+\tau_2$.

other strategy, i.e., not take the privacy protection, which will promote the diffusion of security behaviors among the network. Moreover, consider $(\beta b/c)^*$ provided in Theorem 1 as a function of K/M, and we take the derivative of $(\beta b/c)^*$ with respect to K/M, then get $\frac{\partial(\beta b/c)^*}{\partial(K/M)}>0$. So $(\beta b/c)^*$ increases with increasing K/M. Hence, for a social network with M communities, the best choice for social network managers to set the minimize $(\beta b/c)^*$ is allowing their users to belong to only one community, i.e., $K=1$.

2) *Feasibility and Flexibility:* The obtained critical cost performance gives suggestions on privacy protection quality and "pricing" strategy for the social network managers from the perspective of economics to incentive their users to take the high quality of privacy protection service. These suggestions are feasible and realizable to be introduced into the social networks, according to the definitions of b and c discussed in the previous section. In addition, it is also flexible to apply these suggestions to the existing social networks, such as WeChat and Facebook. Specifically, the high quality of privacy protection service for the users can be more rigorous backstage verification and authorization when some uncertain users manage to access the personal space, information or photo of legitimate users. In addition, to improve the security benefit or reduce the cost of users, some other security related service can also be provided. Take WeChat for instance, a user can know how many of his/her friends have followed a certain official account, which is a necessary and helpful message for users to choose this official account or not. However, this information can only be obtained if this user has update his/her APP to the latest version, which can guarantee safe enough privacy protection to provide such personal information of users' friends. This service above can only bring benefit and better experience to users who take the service, and to their friends who also update the APP and take the service. Therefore, the brought benefit can be considered as the reduction of cost c, but not as the increasing of b. Meanwhile, in this case, the increasing cost of users to obtain the service can be measured by the memory occupancy increment to update the APP.

IV. Privacy Protection Among Users With L-Triggering Game

In a social network, the interaction between two users sometimes depends on the strength of their connection, which could be measured by the number of communities that they have in common. In other words, some interactions, especially behavior to take security functions, can only happen among users belonging to multiple common communities. Specifically, user i and j are sharing a close relationship, which means that they have many interested communities in common. As a result, most information of user j are accessed for user i. In this case, if user i selects the privacy protection, user j's personal information even privacy information can be protected to a great extent. Conversely, if the amount of the two users' common communities is really small, for instance, user i and j coming from different countries just join the same travel community because of their annual leaves, then the relationship between the two users is actually quite weak and there is little personal information can be accessed for each other. In this case, user j cannot benefit from user i's selection of privacy protection.

In response, we generalize the model, in which the users' interaction happens as long as they have at least one communities in common, into a *L-triggering game* situation in this section. In the extended model, users only influence each other if they have at least a minimum number of common communities, L. In a social network, if a user taking the privacy protection i meets another user j in $\theta_i\cdot\theta_j$ communities, then i interact $\theta_i\cdot\theta_j$ times if $\theta_i\cdot\theta_j\geq L$, otherwise, the game between them is not triggered. We call this mechanism as *L-triggering game*. We notice that $L=1$ degenerates to the previous model. The analysis of cost performance at the end of this section indicates that large values of L lead to that users with security behavior are more imitative in choosing with whom to imitate. Next, we will analyze the impact of L-triggering game on the critical cost performance.

A. L-Triggering Game

Given $1\leq L\leq K$. When $L=1$ the model is same as of Section III. Then the fitness of user i formulated as Equation (5) can be rewritten as

$$\pi_i=1+\alpha\sum\nolimits_{j\neq i}\chi_{ij}\left(\theta_i\cdot\theta_j\right)\left[(\beta-2)bs_is_j+(b-c)\,s_i+bs_j\right],\quad(47)$$

where $\chi_{ij}=1$ if $\theta_i\cdot\theta_j\geq L$, and $\chi_{ij}=0$, otherwise.

We notice that $\varphi(\tau)$, which indicates the distribution of the probability that two random users have the same security behavior at the time τ from their MRCI, and $\varphi(\tau_1,\tau_2)$, the distribution of the probability that three random users have the same security behavior, are unchanged. However, $\psi(\tau)=\left\langle\theta_i\cdot\theta_j\,|i\neq j,T=\tau\right\rangle_0$ now changes to $\hat{\psi}(\tau)=\left\langle\chi_{ij}\theta_i\cdot\theta_j\,|i\neq j,T=\tau\right\rangle_0$, which denotes the average number of communities that two random users have in common when they have at least L communities in common. Consequently, ψ, γ, ξ and η will all change with the same physical interpretation, but under the constrain that related users have at least L common communities, which can be rewritten as

$$\hat{\psi} = \int_0^{\infty} \hat{\psi}(\tau) \, p(\tau) \, d\tau, \tag{48a}$$

$$\hat{\gamma} = \int_0^{\infty} \hat{\psi}(\tau) \, \varphi(\tau) \, p(\tau) \, d\tau, \tag{48b}$$

$$\begin{aligned} \hat{\xi} = \frac{1}{3} \int_0^{\infty} d\tau_1 \int_0^{\infty} \Big(&\varphi(\tau_1) \, \hat{\psi}(\tau_1 + \tau_2) + \varphi(\tau_1 + \tau_2) \, \hat{\psi}(\tau_1) \\ &+ \varphi(\tau_1 + \tau_2) \, \hat{\psi}(\tau_1 + \tau_2) \Big) \, p(\tau_1, \tau_2) \, d\tau_2, \end{aligned} \tag{48c}$$

$$\begin{aligned} \hat{\eta} = \frac{1}{3} \int_0^{\infty} d\tau_1 \int_0^{\infty} \varphi(\tau_1, \tau_2) \Big(&\hat{\psi}(\tau_1) + \hat{\psi}(\tau_1 + \tau_2) \\ &+ \hat{\psi}(\tau_1 + \tau_2) \Big) \, p(\tau_1, \tau_2) \, d\tau_2. \end{aligned} \tag{48d}$$

Next, we will find $\hat{\psi}(\tau)$. The probability that two users have $i \leq K$ common communities at time $T = \tau$ from their MRCI is

$$\kappa_i(\tau) = \begin{cases} e^{-\upsilon\tau} + \left(1 - e^{-\upsilon\tau}\right) / \binom{M}{K}, & i = K; \\ \left(1 - e^{-\upsilon\tau}\right) \binom{K}{i} \binom{M-K}{K-i} / \binom{M}{K}, & i < K. \end{cases} \tag{49}$$

Then we have

$$\hat{\psi}(\tau) = \left\langle \chi_{ij} \theta_i \cdot \theta_j \, | i \neq j, T = \tau \right\rangle_0 = \sum\nolimits_{i=L}^{K} i \kappa_i(\tau). \tag{50}$$

1) Case 1 ($L = 1$): According to Vandemonde convolution formula, we have

$$\begin{aligned} \hat{\psi}(\tau) &= \sum\nolimits_{i=1}^{K} i \kappa_i(\tau) \\ &= K e^{-\upsilon\tau} + \left(1 - e^{-\upsilon\tau}\right) \sum\nolimits_{i=1}^{K} i \binom{K}{i} \binom{M-K}{K-i} / \binom{M}{K} \\ &= K e^{-\upsilon\tau} + \left(1 - e^{-\upsilon\tau}\right) K \binom{M-1}{K-1} / \binom{M}{K} \\ &= e^{-\upsilon\tau} K (1 - K/M) + K^2/M. \end{aligned} \tag{51}$$

The result is same as the previous model provided in Lemma 4.

2) Case 2 ($1 < L \leq K$): Let $\hat{K} = \frac{M}{K} \sum\nolimits_{i=L}^{K} i \binom{K}{i} \binom{M-K}{K-i} / \binom{M}{K}$, we get [37]

$$\hat{\psi}(\tau) = e^{-\upsilon\tau} K \left(1 - \hat{K}/M\right) + K \hat{K}/M. \tag{52}$$

Then the critical cost performance formulated in Equation (46) turns to

$$\left(\frac{\beta b}{c}\right)^* = 1 + \frac{\upsilon + 3}{\upsilon + 1} \cdot \frac{\hat{K} \upsilon (\upsilon + 2) + M}{\hat{K} \upsilon (\upsilon + 2) + M (2\upsilon + 3)}, \tag{53}$$

in case that $N \to \infty$ and $\mu \to 0$. Notice that $\hat{K} = K$, if $L = 1$.

Remarks: Comparing with Equation (46), the expressions of $(\beta b/c)^*_{\min}$ for non-triggering game and L-triggering game are much the same, except that $\hat{K} \leq K$, and the equality hold up if and only if $L = 1$.

B. Analysis of Cost Performance

Setting appropriate cost performance can facilitate the security behavior, i.e., the action of taking the privacy protection, among the entire social network. In this part, we will find the minimum cost performance that can make users to choose the privacy protection more frequently than not.

According to the last two sections, we notice that the result of the cost performance shown in Equation (53) is general, since that the L-triggering game becomes the non-triggering game when $L = 1$. So we only analyze the model with the L-triggering game. $(\beta b/c)^*$ given by Equation (53) has a minimum value as a function of υ. Then let $r(\upsilon) = (\beta b/c)^*$, and we take the derivative of $r(\upsilon)$ with respect to υ. Set the result equal to zero and we get

$$\frac{M}{\hat{K}} = \frac{\upsilon^2 \left(\upsilon^2 + 4\upsilon + 4\right)}{\upsilon^2 + 6\upsilon + 6}, \tag{54}$$

according to which, optimal solution υ^* must satisfies $\sqrt{M/\hat{K}} < \upsilon^* < \sqrt{M/\hat{K}} + 1$. If $M/\hat{K}$ is large, solution υ^* to obtain the minimum cost performance is

$$\upsilon^* = \sqrt{M/\hat{K}}, \tag{55}$$

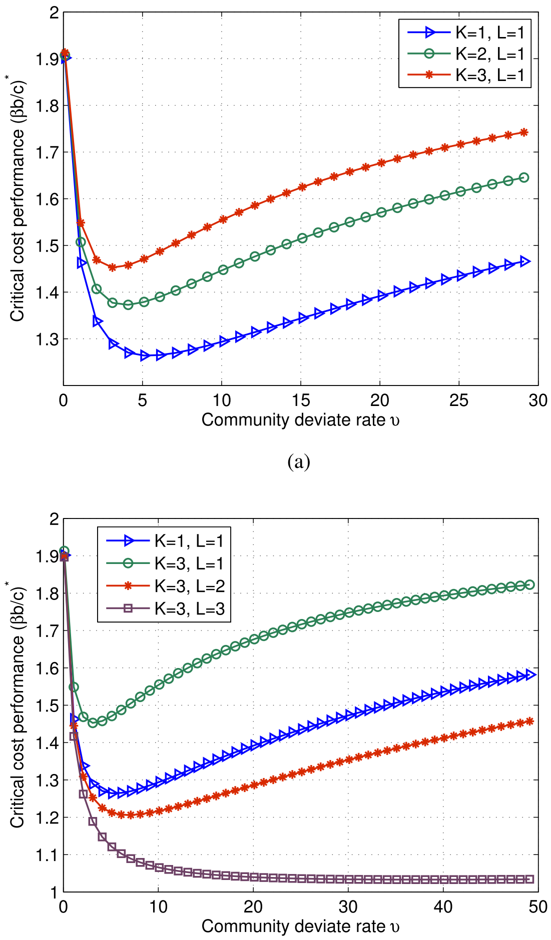
and the minimum cost performance is

$$\left(\frac{\beta b}{c}\right)^*_{\min} = 1 + \frac{\sqrt{M/\hat{K}} + 3}{\left(\sqrt{M/\hat{K}} + 1\right)^2}. \tag{56}$$

Remarks: According to Equation (56), $(\beta b/c)^*_{\min} \sim \sqrt{\hat{K}/M}$, which means that small values of $\hat{K}$ and large values of M can promote the evolution of security behavior among the social network. For non-triggering game situation, i.e., $\hat{K} = K$, we can notice that given number of communities M, it is best if users belong to only one community ($K = 1$). The larger K is, it is harder for users who take the privacy protection to avoid the exploitation by users who do not take the privacy protection. For L-triggering game situation, $\hat{K} < K$ if M is fixed according to the definition of $\hat{K}$ in section IV-A.2, then smaller $(\beta b/c)^*_{\min}$ can be gotten. So large values of L lead to that users with security behavior are more imitative in choosing with whom to imitate.

V. Simulation Results

The critical cost performance is an important parameter that helps the social network managers to make appropriate security service level and payment mechanism to encourage their users to accept the security service, and then promote the spreading of this secure behavior. In this part, we perform numerical simulation experiments to analyze properties and performances of the critical cost performance and its influential factors such as the community deviate rate, population and number of communities of the social network. First, the community deviate rate υ reflects the subjective selectivity for community memberships. If users select communities depending on their own interest mostly, but not on those users with high fitness, then υ is large. Otherwise, υ is small. Then we analyze the effect of the community deviate rate $\upsilon = 2N\upsilon$ for different selections of K and L, which denote the number of communities that a user is allowed to belong



(a)

(b)

Fig. 3. Critical cost performance $(\beta b/c)^*$ versus the community deviate rate $\upsilon = 2N\upsilon$. The population size is large, $N = 10^4$. The strategy deviate rate is $u = 10^{-4}$. The number of communities is $M = 20$. (a) Non-triggering game. (b) L-triggering game.

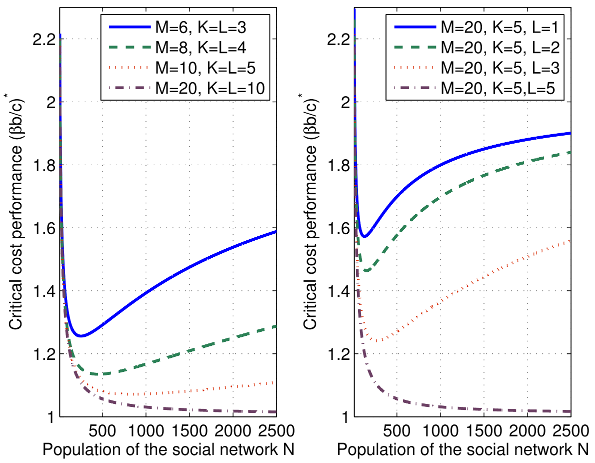


Fig. 4. Critical cost performance $(\beta b/c)^*$ versus the population of the social network N under the non-triggering game and L-triggering game, respectively. The strategy deviate rate is $u = 10^{-4}$, and the community deviate rate is $\upsilon = 0.01$.

to and the minimum number of common communities that game can be triggered. The population of the social network is large, i.e., $N = 10^4$ ($N \to \infty$), and the number of communities is set as $M = 20$. We set the strategy deviate rate as $u = 10^{-4}$ ($u \to 0$). We consider the population of the network is constant. Simulation results of non-triggering game and L-triggering game are shown in Fig. 3 (a) and Fig. 3 (b), respectively. As shown in the results, the critical cost performance $(\beta b/c)^*$ is a U-shaped function of community deviate rate υ. When υ is small, $(\beta b/c)^*$ tend to be large and all users belong to the same community. Conversely, when υ is large, the community affiliations cannot persist for a long time. Moreover, the results of numerical analysis shown in Equation (55) and (56) can be demonstrated by the simulations results shown in Fig. 3.

As shown in Fig. 3 (a), we notice that for a fixed number of communities M, small values of K can facilitate the evolution of the security behavior, which means that the selection of taking the privacy protection is promoted in the evolution process. This conclusion is consistent with the numerical analysis shown in Equation (56). Consequently, when the number of communities is given, the best choice for users is to belong to $K = 1$ community. With the increasing of K, it is hard for users taking the privacy protection to avoid the exploitation by users not taking the privacy protection. But according the results of the L-triggering game situation shown in Fig. 3 (b), for $K = 3$, if $L = 2$ or $L = 3$, the critical cost performance is smaller than $K = 1$. These results indicate that belonging to more communities, i.e., $K > 1$, can also facilitate the evolution of the security behavior when the game only happen if users have a certain minimum number of common communities L.

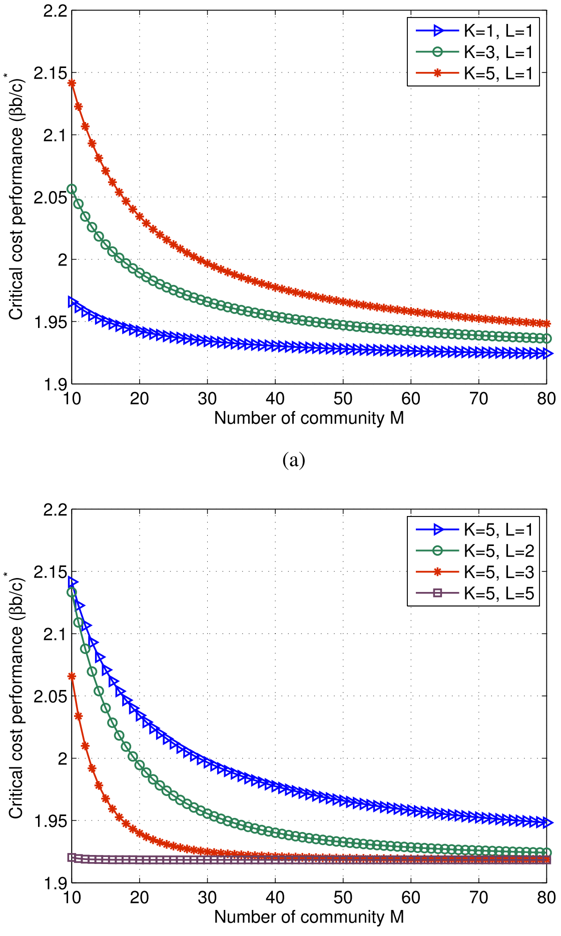
We test the effects of the population of the network on the critical cost performance, and the results are shown in Fig. 4. We set the strategy deviate rate as $u = 10^{-4}$, and the community deviate rate as $\upsilon = 0.01$. Parameter settings of M, K and L are shown in the figures. Results illustrate that for both non-triggering game and L-triggering game cases, the critical cost performance is a convex function of population N. According to the results, we notice that if the population of the network is too small, then the effect of spite tends to be strong, so the critical cost performance $(\beta b/c)^*$ has to be very large. If $N = 2$, it will never pay to users with security behavior, which means that users will not take the privacy protection to ensure their information security. When N is large, all the communities that get population by users who take the privacy protection and not take the privacy protection cannot persist for long. In addition, the lower bound of the critical cost performance is 1, which is consistent with the result in Equation (56).

As shown in Fig. 5, the cost performance decreases as the number of communities M increasing. These results indicate that more communities is helpful for the spreading of security behavior, which mean that adding community number will help users to take privacy protection more frequently.

Next, we simulate the evolution process of the strategies that taking the privacy protection or not in the social network. The topology we used in this simulation is based on Flickr, a real-world online social network database. There are 5,899,882 edges connecting 80,513 users in the Flickr graph dataset, and the edge represents the connection between two users. In order to test the performance of the evolutionary

TABLE II
PARAMETERS SETTING OF THE SIMULATION FOR DIFFERENT CASES

Case	M	K	L	α	p_0	$(\beta b/c)^*$
1	15	1	1	0.05	0.5	1.8416
2	15	1	1	0.2	0.5	1.8416
3	20	2	1	0.05	0.5	1.8850
4	20	2	1	0.2	0.5	1.8850
5	15	1	1	0.05	0.4	1.8416
6	15	1	1	0.2	0.4	1.8416
7	20	2	1	0.05	0.4	1.8850
8	20	2	1	0.2	0.4	1.8850



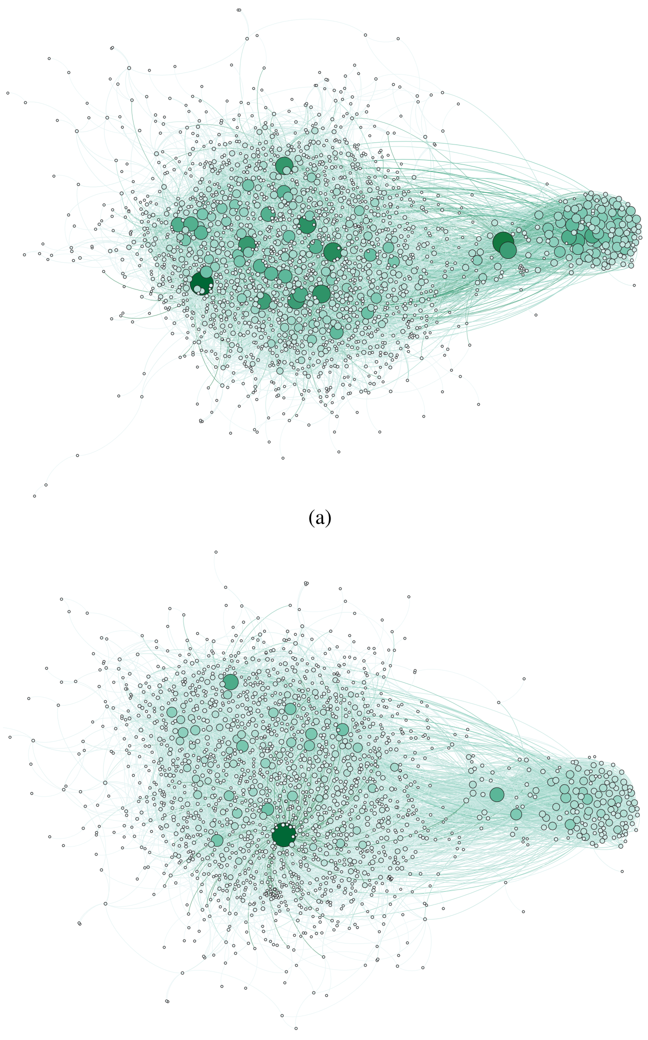
(a)

(b)

Fig. 5. Critical cost performance $(\beta b/c)^*$ versus the number of communities M. The population size of the social network is set as $N = 15$. The strategy deviate rate is $u = 10^{-4}$, and the community deviate rate is $\upsilon = 0.01$. (a) Non-triggering game. (b) L-triggering game.

game theoretic framework we proposed, the topology of Flickr is modified. The communities are established based on the users with most importance in the network, i.e., with largest betweennesses or having largest amounts of one-hop and two-hop neighborhoods. In addition, each user is allowed to join limited K communities. If one user belongs to more than K communities, the topology will be modified as the following rules: The connection between user i and community k is established with probability

$$p_{ik} = \frac{M_k}{\sum_{j \in J_i} M_j}, \tag{57}$$

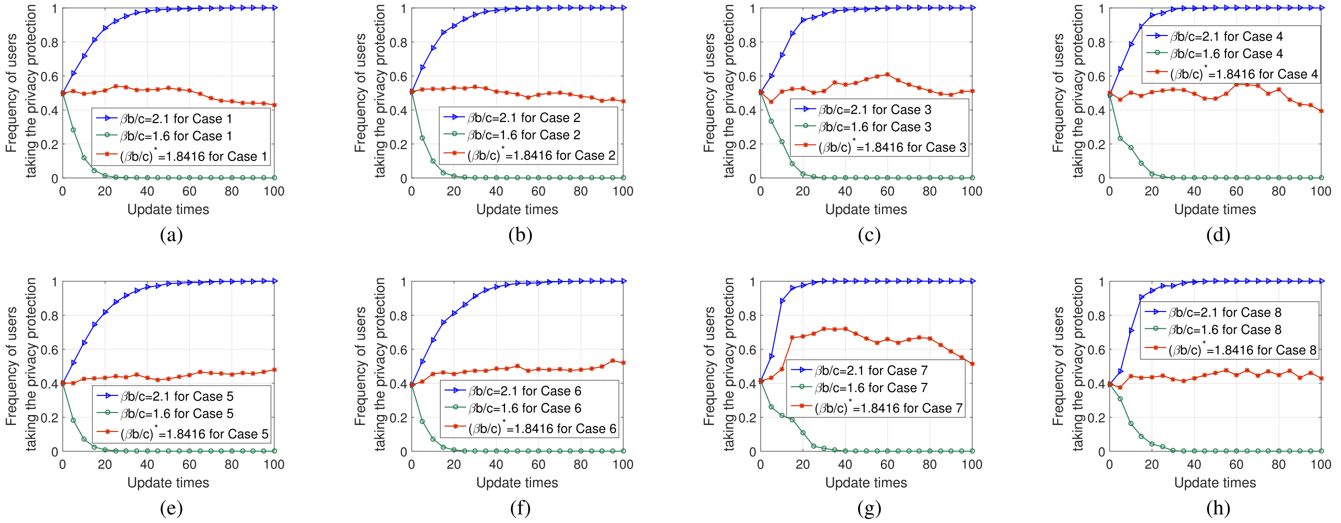


(a)

(b)

Fig. 6. Graph structures of the modified Flickr network used for simulation. (a) $N = 50,000$, $M = 15$, $K = 1$. Case 1, 2, 5, 6. (b) $N = 50,000$, $M = 20$, $K = 2$. Case 3, 4, 7, 8.

where M_k is the number of users belonging to community k, and J_i is the set of all communities belonged by user i. For the network, we use $N = 50,000$ users in Flickr distributing over $M = 15$ or $M = 20$ communities. Each user belongs to $K = 1$ or $K = 2$ communities. The graph structures of the modified Flickr network are depicted in Fig. 6. We set the strategy deviate rate and community deviate rate as $u = 10^{-4}$ and $\upsilon = 0.01$, responsibility. The parameter settings for the eight cases are shown in Table II. In Table II, $\alpha = 0.05$ and $\alpha = 0.2$ denote different intensities of selection, $p_0 = 0.5$ and $p_0 = 0.4$ indicate the different initialized frequencies of the users who select to take the privacy protection, and $(\beta b/c)^*$ is obtained according to Equation (46). In our simulation, the network updates 100 times. Evolutions of the privacy protection in the network with different cost performance are shown in Fig. 7, in which $c = 1$, $\beta = 2$, and b varies to realize different $\beta b/c$. As accepted, the evolutionary stable state of the frequency of users taking the privacy protection is 1 when $\beta b/c > (\beta b/c)^*$, otherwise, 0. These results demonstrate that when the cost performance exceeds the critical cost performance, thenusers



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 7. Evolution of the privacy protection in the network with a population of size $N = 50,000$. The strategy deviate rate is $u = 10^{-4}$, and the community deviate rate is $\upsilon = 0.01$. Other parameters values are set as Table II. (a) Case 1. (b) Case 2. (c) Case 3. (d) Case 4. (e) Case 5. (f) Case 6. (g) Case 7. (h) Case 8.

select to take the privacy protection more frequently than not. In addition, the evolutionary stable state of the network cannot be achieved if $\beta b/c = (\beta b/c)^*$, and the frequency is around 0.5.

Remarks: For a social network with given number of community and number of community that each user is allowed to belong to, the critical cost performance can be obtained through Theorem 1 and Equation (53). Social network managers have to make appropriate security service b and payment mechanism c to ensure that $\beta b/c > (\beta b/c)^*$. Then their users can be encourage to accept the security service, and the spreading of the secure behavior can be promoted over the social network. Besides, we notice that the convergence speed of evolutionary stable state depends on many factors, such as M, the number of communities in the network, and K, the number of communities each user belongs to. Given the same cost performance, L, α and p_0, small values of M/K result in fast convergence. This result is reasonable. On the one hand, if M is fixed, larger values of K increase dimensions of the relationship among users, then each user might have more new friends, and the closeness to his/her old friends might be stronger. These changes can help the spreading of user behaviors, i.e., taking the privacy protection if $\beta b/c > (\beta b/c)^*$, otherwise, not taking the privacy protection. On the other hand, for fixed K, smaller M means that there might be more common communities among every two users. Therefore, the closeness between users tends to be stronger, which can help the spreading of user behaviors. After social network managers release a new security service, such as the privacy protection in our work, security service b and cost c for users are determined. Then the speed of revenue for managers and the set up of privacy protection at the network platform depend on how fast that all users take the privacy protection, which is concerned with the convergence speed. It will help the network managers to make network structure and service plan, and the storage and processing capacities of network server can also be planed for the improvement of the user information security.

VI. Conclusion

In this paper, we analyze the privacy protection behaviors of social network users by a community structured evolutionary game theoretic framework. The players, strategies, payoff matrix and the topology structure of users are defined in this framework. We obtain the critical cost performance, which is an important parameter that can help social networks to design incentive mechanisms to facilitate the privacy protection behavior among their users. Simulation results demonstrate that the proposed theoretic framework is effective in modeling the users' relationship and privacy protection behavior.

Appendix A
Proof of Equation (9)

Proof: Similar to the derivation of Equation (7), we get:

$$\pi_i = 1 + \alpha \sum\nolimits_j \left(\theta_i \cdot \theta_j\right) f\left(s_i, s_j\right) - \alpha K \left(\beta b - c\right) s_i. \quad (58)$$

For $\alpha = 0$, the Taylor expansion of ω_i can be given by:

$$\omega_i = \frac{N\pi_i}{\sum_j \pi_j} = \omega_i\left(0\right) + \alpha\omega_i^{(1)}\left(0\right) + o\left(\alpha^2\right), \quad (59)$$

where $\omega_i^{(1)}(0) = \partial\omega_i(\alpha)/\partial\alpha$.

According to Equation (5) and (7), we have

$$\frac{\partial \sum_j \pi_j}{\partial \alpha}|_{\alpha=0} = \sum\nolimits_j \sum\nolimits_l \left(\theta_j \cdot \theta_l\right) f\left(s_j, s_l\right) - K\left(b\beta - c\right) \sum\nolimits_j s_j. \quad (60)$$

Then $\omega_i^{(1)}(0)$ can be calculated as

$$\omega_i^{(1)}\left(0\right) = \frac{N^2\left[\sum_j \left(\theta_i \cdot \theta_j\right) f\left(s_i, s_j\right) - K\left(\beta b - c\right) s_i\right]}{N^2} - \frac{N\left[\sum_j \sum_l \left(\theta_j \cdot \theta_l\right) f\left(s_j, s_l\right) - K\left(b\beta - c\right)\sum_j s_j\right]}{N^2}$$

$$
\begin{aligned}
&= \sum\nolimits_j \left(\theta_i \cdot \theta_j\right)\left[(\beta-2)\, b s_i s_j + (b-c)\, s_i + b s_j\right] - K\,(\beta b - c)\, s_i \\
&\quad - \frac{1}{N}\Big[\sum\nolimits_j \sum\nolimits_l \left(\theta_j \cdot \theta_l\right)\left[(\beta-2)\, b s_j s_l + (b-c)\, s_j + b s_l\right] \\
&\quad - K\,(b\beta - c)\sum\nolimits_j s_j\Big] \\
&= (\beta-2)\, b \sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_i s_j + (b-c)\sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_i \\
&\quad + b \sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_j - K\,(\beta b - c)\, s_i \\
&\quad - \frac{(\beta-2)\, b}{N}\sum\nolimits_j \sum\nolimits_l (\theta_j \cdot \theta_l) s_j s_l - \frac{b-c}{N}\sum\nolimits_j \sum\nolimits_l (\theta_j \cdot \theta_l) s_j \\
&\quad - \frac{1}{N}\sum\nolimits_j \sum\nolimits_l \left(\theta_j \cdot \theta_l\right) s_l + \frac{K\,(b\beta - c)}{N}\sum\nolimits_j s_j .
\end{aligned}
$$

Then we can rewrite ω_i in Equation (59) as

$$
\begin{aligned}
\omega_i &= 1+\alpha\Big[(\beta-2)\, b\sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_i s_j + (b-c)\sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_i \\
&\quad + b\sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_j - K\,(\beta b - c)\, s_i - \frac{(\beta-2)\, b}{N}\sum\nolimits_j \sum\nolimits_l (\theta_j \cdot \theta_l) s_j s_l \\
&\quad - \frac{2b-c}{N}\sum\nolimits_j \sum\nolimits_l \left(\theta_j \cdot \theta_l\right) s_j + \frac{K\,(\beta b - c)}{N}\sum\nolimits_j s_j\Big] + o\left(\alpha^2\right).
\end{aligned}
$$

This completes the proof of Equation (9).

Appendix B
Proof of Lemma 1

Proof: We pursuit the stable state by calculating $\langle \hat{p} \rangle_{\text{imi}}$, which can be given by

$$
\begin{aligned}
\omega_i &= 1+\alpha\Big[(\beta-2) b\sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_i s_j + (b-c)\sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_i \\
&\quad + b\sum\nolimits_j \left(\theta_i \cdot \theta_j\right) s_j - K\,(\beta b - c) s_i - \frac{(\beta-2) b}{N}\sum\nolimits_j \sum\nolimits_l (\theta_j \cdot \theta_l) s_j s_l \\
&\quad - \frac{2b-c}{N}\sum\nolimits_j \sum\nolimits_l \left(\theta_j \cdot \theta_l\right) s_j + \frac{K\,(\beta b - c)}{N}\sum\nolimits_j s_j\Big] + o\left(\alpha^2\right).
\end{aligned}
$$

We plug Equation (9) into $\sum_i s_i \frac{d\omega_i}{d\alpha}$ and get

$$
\begin{aligned}
\sum\nolimits_i s_i \frac{d\omega_i}{d\alpha} &= -\, K\,(\beta b - c) f_1 - \frac{K\,(\beta b - c)}{N} f_2 + (b-c) f_3 \\
&\quad + (\beta-1) b f_4 - \frac{2b-c}{N} f_5 - \frac{(\beta-2)\, b}{N} f_6,
\end{aligned}
\tag{61}
$$

where f_i $(i = 1, 2, \cdots, 6)$ are defined by (15). Then plug can calculate and gain the first derivative of $\langle \hat{p} \rangle_{\text{imi}}$ as follows

$$
\begin{aligned}
\langle p \rangle_{\text{imi}}^{(1)} &= \frac{1}{N}\Big[-K(\beta b - c)\langle f_1\rangle_0 - \frac{K(\beta b - c)}{N}\langle f_2\rangle_0 + (b-c)\langle f_3\rangle_0 \\
&\quad + (\beta-1) b\langle f_4\rangle_0 - \frac{2b-c}{N}\langle f_5\rangle_0 - \frac{(\beta-2)\, b}{N}\langle f_6\rangle_0\Big].
\end{aligned}
\tag{62}
$$

As the derivation process above, we can obtain the critical cost performance b/c when Equation (62) equals zero. The obtained $(b/c)^*$ can be given by

$$
\left(\frac{b}{c}\right)^* = \frac{-K\langle f_1\rangle_0 + \frac{K}{N}\langle f_2\rangle_0 + \langle f_3\rangle_0 - \frac{1}{N}\langle f_5\rangle_0}{f\,(f_1, f_2, f_3, f_4, f_5, f_6)}, \tag{63}
$$

where $f\,(f_1, f_2, f_3, f_4, f_1, f_6) = -\beta K\langle f_1\rangle_0 + \frac{\beta K}{N}\langle f_2\rangle_0 + \langle f_3\rangle_0 + (\beta-1)\langle f_4\rangle_0 - \frac{2}{N}\langle f_5\rangle_0 - \frac{\beta-2}{N}\langle f_6\rangle_0$. This completes the proof of Lemma 1.

References

[1] E. Serrano, C. A. Iglesias, and M. Garijo, "A survey of twitter rumor spreading simulations," in *Computational Collective Intelligence*. Cham, Switzerland: Springer, 2015, pp. 113–122.

[2] M. Madejski, M. Johnson, and S. M. Bellovin, "A study of privacy settings errors in an online social network," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops)*, Mar. 2012, pp. 340–345.

[3] I. Heimbach, B. Schiller, T. Strufe, and O. Hinz, "Content virality on online social networks: Empirical evidence from Twitter, Facebook, and Google+ on German news websites," in *Proc. 26th ACM Conf. Hypertext Social Media*, Ankara, Turkey, Sep. 2015, pp. 39–47.

[4] A. Dhami, N. Agarwal, T. K. Chakraborty, B. P. Singh, and J. Minj, "Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook," in *Proc. IEEE 3rd Int. Adv. Comput. Conf. (IACC)*, Ghaziabad, India, Feb. 2013, pp. 465–469.

[5] R. L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Process. Mag.*, vol. 30, no. 1, pp. 82–105, Jan. 2013.

[6] I. Krontiris, M. Langheinrich, and K. Shilton, "Trust and privacy in mobile experience sharing: Future challenges and avenues for research," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 50–55, Aug. 2014.

[7] J. M. Such, A. Espinosa, and A. García-Fornes, "A survey of privacy in multi-agent systems," *Knowl. Eng. Rev.*, vol. 29, no. 3, pp. 314–344, May 2014.

[8] C. Bettini and D. Riboni, "Privacy protection in pervasive systems: State of the art and technical challenges," *Pervasive Mobile Comput.*, vol. 17, pp. 159–174, Feb. 2015.

[9] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," *MIS Quart.*, vol. 35, no. 4, pp. 989–1016, Dec. 2011.

[10] L. Xu, C. Jiang, Y. Chen, J. Wang, and Y. Ren, "A framework for categorizing and applying privacy-preservation techniques in big data mining," *Computer*, vol. 49, no. 2, pp. 54–62, Feb. 2016.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 1, pp. 222–233, Jan. 2014.

[12] L. Xu, C. Jiang, Y. Qian, Y. Zhao, J. Li, and Y. Ren, "Dynamic privacy pricing: A multi-armed bandit approach with time-variant rewards," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 271–285, Feb. 2017.

[13] R.-H. Hwang, Y.-L. Hsueh, and H.-W. Chung, "A novel time-obfuscated algorithm for trajectory privacy protection," *IEEE Trans. Serv. Comput.*, vol. 7, no. 2, pp. 126–139, Apr./Jun. 2014.

[14] B. Greschbach, G. Kreitz, and S. Buchegger, "The devil is in the metadata—New privacy challenges in decentralised online social networks," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PERCOM Workshops)*, Lugano, Switzerland, Mar. 2012, pp. 333–339.

[15] H. Hu, G. J. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms," *IEEE Trans. Knowl. Data Eng.*, vol. 25, no. 7, pp. 1614–1627, Jul. 2013.

[16] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Basar, and J. Hubaux, "Game theory meets network security and privacy," *ACM Comput. Surv.*, vol. 45, no. 3, p. 25, 2013.

[17] D. Tosh, S. Sengupta, C. Kamhoua, K. Kwiat, and A. Martin, "An evolutionary game-theoretic framework for cyber-threat information sharing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 7341–7346.

[18] L. R. Wu and X. Chen, "Modeling of evolutionary game between SNS and user: From the perspective of privacy concerns," in *Proc. 21st Annu. Conf. Int. Conf. Manage. Sci. Eng. (ICMSE)*, Arunachal Pradesh, India, Aug. 2014, pp. 115–119.

[19] C. Jiang, Y. Chen, and K. J. R. Liu, "Graphical evolutionary game for information diffusion over social networks," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 4, pp. 524–536, Aug. 2014.

[20] A. C. Squicciarini and C. Griffin, "An informed model of personal information release in social networking sites," in *Proc. Int. Conf. Privacy, Secur., Risk Trust (PASSAT), Int. Conf. Social Comput. (SocialCom)*, Amsterdam, The Netherlands, Sep. 2012, pp. 636–645.

[21] L.-L. Jiang and M. Perc, "Spreading of cooperative behaviour across interdependent groups," *Sci. Rep.*, vol. 3, p. 2483, Aug. 2013.

[22] R. M. Bond *et al.*, "A 61-million-person experiment in social influence and political mobilization," *Nature*, vol. 489, no. 7415, pp. 295–298, Sep. 2012.

[23] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science*, vol. 347, no. 6221, pp. 509–514, 2015.

[24] S.-M. Cheng, W. C. Ao, P.-Y. Chen, and K.-C. Chen, "On modeling malware propagation in generalized social networks," *IEEE Commun. Lett.*, vol. 15, no. 1, pp. 25–27, Jan. 2011.

[25] C. Jiang, Y. Chen, and K. J. R. Liu, "Evolutionary dynamics of information diffusion over social networks," *IEEE Trans. Signal Process.*, vol. 62, no. 17, pp. 4573–4586, Sep. 2014.

[26] C. L. Apicella, F. W. Marlowe, J. H. Fowler, and N. A. Christakis, "Social networks and cooperation in hunter-gatherers," *Nature*, vol. 481, no. 7382, pp. 497–501, 2012.

[27] Y. Jiang and J. C. Jiang, "Understanding social networks from a multiagent perspective," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 10, pp. 2743–2759, Oct. 2014.

[28] C. Jiang, Y. Chen, and K. J. R. Liu, "Distributed adaptive networks: A graphical evolutionary game-theoretic view," *IEEE Trans. Signal Process.*, vol. 61, no. 22, pp. 5675–5688, Nov. 2013.

[29] C. Jiang, Y. Chen, Y. Gao, and K. R. Liu, "Joint spectrum sensing and access evolutionary game in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 2470–2483, May 2013.

[30] C. Jiang, Y. Chen, and K. J. R. Liu, "On the equivalence of evolutionary stable strategies," *IEEE Commun. Lett.*, vol. 18, no. 6, pp. 995–998, Jun. 2014.

[31] W. H. Sandholm, *Population Games and Evolutionary Dynamics*. Cambridge, MA, USA: MIT Press, 2010.

[32] R. Cressman, *Evolutionary Dynamics and Extensive Form Games*, vol. 5. Cambridge, MA, USA: MIT Press, 2003,

[33] W. J. Ewens, *Mathematical Population Genetics 1: Theoretical Introduction*, vol. 27. Springer, 2012,

[34] S. Wright, "Evolution in mendelian populations," *Genetics*, vol. 16, no. 2, pp. 97–159, Jan. 1931.

[35] R. A. Fisher, *The Genetical Theory of Natural Selection: A Complete Variorum Edition*. London, U.K.: Oxford Univ. Press, 1930.

[36] J. Hofbauer and K. Sigmund, *Evolutionary Games and Population Dynamics*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

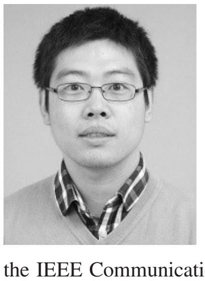
[37] C. E. Tarnita, T. Antal, H. Ohtsuki, and M. A. Nowak, "Evolutionary dynamics in set structured populations," *Proc. Nat. Acad. Sci. USA,* , vol. 106, no. 21, pp. 8601–8604, May 2009.

[38] M. A. Nowak, A. Sasaki, C. Taylor, and D. Fudenberg, "Emergence of cooperation and evolutionary stability in finite populations," *Nature*, vol. 428, no. 6983, pp. 646–650, Apr. 2004.

[39] P. Shakarian, P. Roos, and A. Johnson, "A review of evolutionary graph theory with applications to game theory," *Biosystems*, vol. 107, no. 2, pp. 66–80, Feb. 2012.

[40] G. Wild and A. Traulsen, "The different limits of weak selection and the evolutionary dynamics of finite populations," *J. Theor. Biol.*, vol. 247, no. 2, pp. 382–390, Jul. 2007.

Jun Du (S'16) received the B.S. degree in information and communication engineering from the Beijing Institute of Technology, Beijing, China, in 2009, and the M.S. degree in information and communication engineering from Tsinghua University, Beijing, in 2014, where she is currently pursuing the Ph.D. From 2016 to 2017, she was a Sponsored Researcher, during which she visited Imperial College London, U.K. Her research interests are mainly in resource allocation and system security of heterogeneous networks and space-based information networks.



Chunxiao Jiang (S'09–M'13–SM'15) received the B.S. degree (Hons.) in information engineering from Beihang University in 2008 and the Ph.D. (Hons.) in electronic engineering from Tsinghua University in 2013. From 2013 to 2016, he held a post-doctoral position with the Department of Electronic Engineering, Tsinghua University, during which he visited University of Maryland College Park and the University of Southampton. He is a recipient of the IEEE Globecom Best Paper Award in 2013, the IEEE GlobalSIP Best Student Paper Award in 2015, and the IEEE Communications Society Young Author Best Paper Award in 2017.

Kwang-Cheng Chen (M'89–SM'94–F'07) received the B.S. degree from the National Taiwan University in 1983, and the M.S. and Ph.D. degrees from the University of Maryland, College Park, USA, in 1987 and 1989, all in electrical engineering, respectively. From 1987 to 1998, he was with the SSE, COMSAT, IBM Thomas J. Watson Research Center, and National Tsing Hua University, working on the mobile communications and networks. From 1998 to 2016, he was a Distinguished Professor with the National Taiwan University, Taipei, Taiwan and also served as the Director with the Graduate Institute of Communication Engineering, as the Director with the Communication Research Center, and an Associate Dean for Academic Affairs with the College of Electrical Engineering and Computer Science from 2009 to 2015. Since 2016, he has been with the Department of Electrical Engineering, University of South Florida, Tampa, USA. He has been actively involved in the organization of various IEEE conferences as General/TPC chair/Co-Chair, and has served in editorships with a few IEEE journals. He also actively participates in and has contributed essential technology to various IEEE 802, Bluetooth, and LTE, and LTE-A wireless standards. He has received a number of awards including the 2011 IEEE COMSOC WTC Recognition Award, 2014 IEEE Jack Neubauer Memorial Award, and 2014 IEEE COMSOC AP Outstanding Paper Award. His recent research interests include wireless networks, cybersecurity, cyber-physical systems, social networks, and data analytics.

Yong Ren (SM'16) received the B.S, M.S, and Ph.D. degrees in electronic engineering from the Harbin Institute of Technology, China, in 1984, 1987, and 1994, respectively. From 1995 to 1997, he held a post-doctoral position with the Department of Electronics Engineering, Tsinghua University, China. He is currently a Professor with the Department of Electronics Engineering and the Director of the Complexity Engineered Systems Laboratory, Tsinghua University. He holds 12 patents, and has authored or co-authored over 100 technical papers in the behavior of computer networks, P2P networks, and cognitive networks. His current research interests include complex systems theory and its applications to the optimization and information sharing of the Internet, Internet of Things and ubiquitous network, cognitive networks, and Cyber-Physical Systems. He serves as a Reviewer of *IEICE Transactions on Communications*, *Digital Signal Processing*, *Chinese Physics Letters*, *Chinese Journal of Electronics*, *Chinese Journal of Computer Science and Technology*, and *Chinese Journal of Aeronautics*.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University in 1977. From 1977 to 1990, he was with the Faculty, University of Illinois at Urbana–Champaign. Since 1990, he has been on the faculty at Princeton, where he is currently the Michael Henry Strater University Professor of Electrical Engineering. From 2006 to 2016, he served as the Dean of Princeton's School of Engineering and Applied Science. He has also held visiting appointments at several other institutions, most recently at Berkeley and Cambridge. His research interests are in the areas of information theory and signal processing, and their applications in wireless networks and related fields. Among his publications in these areas is the recent book *Information Theoretic Security and Privacy of Information Systems* (Cambridge University Press, 2017). He is a member of the National Academy of Engineering and the National Academy of Sciences, and a foreign member of the Royal Society. In 1990, he served as President of the IEEE Information Theory Society. He received the Technical Achievement and Society Awards of the IEEE Signal Processing Society in 2007 and 2011, respectively. Recent recognition of his research includes the 2017 IEEE Alexander Graham Bell Medal, a D.Sc. honoris causa from Syracuse University in 2017, and election as an Honorary Professor at Peking University and at Tsinghua University. From 2004 to 2007, he was the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY.