JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 35, 1113-1132 (2019)
DOI: 10.6688/JISE.201909_35(5).0011

Social Tie Based Cooperative Jamming for D2D Communications in the Internet of Things

YAN GAO, YONG ZENG*, ZHI-HONG LIU, JIAN-FENG MA,
YANG LIU AND YI-KAI LIU
School of Cyber Engineering
Xidian University
Xi'an, 710071 P.R. China
E-mail: {ygao; yzeng; zhhliu; jfma; yliu_9; ykliu_61}@mail.xidian.edu.cn

With the proliferation of short-range networks and the prevalence of devices connected to these networks, the Internet of Things (IoT) has held the promise of improving our lives. Devices-to-device communication is considered to be an important part of the IoT. To address the limitation of physical layer security approaches based on single-antenna systems, cooperative jamming is a promising approach to enhance efficient cooperation among devices. In this paper, we study the cooperative interference problem of a two-layer network in which the upper social network (S*) is composed of people with different social ties and the lower layer network (P*) is composed of various physical devices. S* overlays P* by a connecting degree (*Cd*). We introduce game theory to simulate the cooperation willingness of jammers in S*, and prove the existence of Nash Equilibrium (NE) and design an algorithm to calculate the secrecy outage probability (SOP). Moreover, we introduce a susceptible-infective-recovery (SIR) spreading model to evaluate the performance, which believes that each jammer's initial state is likely to participate rather than certainly participate in the cooperation. Each jammer is considered to have three states: probable participation (P-state), obligatory participation (O-state) and non-participation (N-state). Experiments show that when social ties are strong among devices, jammers would be more willing to cooperate, contribute more to communication quality and have lower computational complexity on two-lay net-work. Our methods make jammers have more choices for updating status, and show that results would be better than without SIR characteristics under the same number of jammers.

Keywords: physical layer security, cooperative jamming, secrecy outage probability, two-layer network, game theory

1. INTRODUCTION

With the advent of the Internet and smart devices, not only human beings are interrelated, and the devices are also connected with each other [1]. This shift has led to the concept of the Internet of things (IoT). The IoT ecosystem is a platform that allows devices with Internet connectivity to communicate directly with each other [2]. With the increasing demand for information transmission between humans, D2D communications have emerged as a very promising technology for IoT applications. The number of devices in IoT is increasing rapidly. And devices are the key role of the IoT. It is estimated that by 2020 there will be about 50 billion devices connected to IoT [3], which will accelerate the communication security requirements between devices.

In recent years, some technologies have paved the way for the security of D2D communications, but there are still some challenges to be solved. In order to improve the

Received October 31, 2018; revised December 3 & 27, 2018; accepted January 18, 2019.
Communicated by Xiaohong Jiang.

security of D2D communication, physical layer security has been widely studied. A promising way to improve communication performance is the cooperative jamming [4]. Specifically, this method selects helpers to transmit the artificial noise, thereby reducing the quality of the received eavesdropping signal without interfering with the legitimate receiver [5]. However, the existing cooperative jamming schemes mainly focus on the physical layer and assume that all jammers are willing to cooperate with the source or destination to improve the security performance. In many scenarios, it is not easy to achieve this goal because each jammer has the right to decide whether to help other jammers in cooperation or not. With the explosive growth of social networks, more and more people participate in the social interactions. Therefore, social relationships among people are hence extensively broadened and significantly enhanced [6]. It is feasible to enhance security D2D communication for cooperative jamming by using human social relationships. Although it is still in the early stages of development, the social characteristics of D2D communication is a potential direction to solve existing problems, which provides a novel way for the design of D2D communication system [7]. In addition, owing to game theory has been widely used in various network applications [8], the cooperative jamming problem can find an optimum solution by using game theory. Although it opens up a new way of cooperative jamming, there are still some limitations, such as computational costs, different social relationships among individuals, diversity of the initial state of the jammer, and so on.

Based on the aforementioned challenges, we emphasize that D2D system can achieve communication security through physical layer. We design a novel cooperative jamming strategy for D2D communication which can be applied to a two-layer network in which its upper-layer is a social network and the lower-layer is a physical communication network. In social networks, different users have different social connections with others. In the physical network, devices access the network through BSs or establish D2D communication links that are subject to physical and communication constraints. We can use game theory to model the jammers in the upper social network layer's willingness to cooperate. Firstly, we prove the existence of Nash equilibrium and design an algorithm to find cooperative nodes with different social ties in the social networks. Then, these cooperative nodes are mapped to the real jammers in the physical network. Under different social ties, we can obtain the secrecy outage probability in Nash equilibrium. Furthermore, in order to solve the limitation of jammers' state, we introduce the SIR spreading model to evaluate the performance and believe that each jammer can determine its own state. Unlike previous studies, each jammer can change its decision-making from an uncertain state to the obligatory participation or non-participation. We have done a series of experiments to verify our theoretical analysis. The results show that jammers are more likely to participate in cooperative jamming to enhance the secrecy performance when the social ties between users are closer, and jammers will provide more help for other jammers who have close ties with themselves. Besides, our methods can obtain more time-efficient and more universal results than previous studies.

1.1 Related Works

Most of the literatures on D2D communications focus on resource allocation, power consumption and interference management issues [9]. Ye *et al.* in [10] proposed a dy-

namic resource allocation in D2D communication to minimize the total transmission power consumption. [11] proposes a generalized two-level Stackelberg game theoretic framework to enable content sharing with multi-hop D2D communication capabilities. Xu *et al.* in [12] designed a pricing-based two-stage matching by utilizing jointly optimizing relay selection, spectrum allocation and power control. Simulation results show that the proposed scheme obtains a good performance on energy efficiency. Wang *et al.* in [13] considered the application of network coding in the underlay D2D and proposed a new interference management scheme, which can improve the spectrum efficiency and increase system throughput. Meanwhile, much effort has been made in the literature for cooperative D2D communication improve communication security. Communication security is obviously a necessary condition for IoT application, for example, commercial, industrial, government, military applications and so on [14]. D2D systems can enhance security via the physical layer. Physical Layer Security is generally defined as a technology that uses wireless channel characteristics, modulation and coding, and jamming to reduce the ability of eavesdroppers to detect and intercept sensitive communications [15, 16].

Zhang *et al.* in [17] considered physical-layer security in D2D communication with an eavesdropper. They formulate the D2D system by introducing the KM algorithm. Simulation results show that the introduction of D2D communications underlying cellular network can greatly enhance the system security capacity. Zhu *et al.* in [18] analyzed the D2D communication has the security superiority in the physical layer. Secrecy outage probability is the evaluation index. Compared with traditional communication methods, secrecy outage probability in D2D communications is lower in almost all link SNR. But when AP has a large number of antennas and perfect channel state information, secrecy outage probability in D2D communications has a disadvantage. In [19], the authors look at the problem of jointly minimizing the SOP and connection outage probability over the route. They use a flexible route metric that can trade off between SOP and COP based on the security needs of the user. However, not all existing physical-layer security technologies are suitable for D2D systems. Wireless communication system is extremely vulnerable to eavesdropping in virtue of wireless channel's openness [20]. Sun *et al.* in [21] formulated the problem of cooperative key generation in D2D communication as a coalition game, which selfless devices are strongly motivated to cooperate with others to establish secret keys. Xi *et al.* in [22] designed a secret key extraction protocol for D2D communication, which achieved high security and significantly reduced the system overhead in D2D communication.

With the growth of social networks such as Facebook and Twitter, more and more social characteristics have become the significant dimensions for the communication system [23]. Therefore, many researchers are concerned about the relationship between physical layer security and complex network theory. The introduction of user social relationships can improve the security of D2D communication. The notions of social ties and social trust degrees have drawn wide attentions of researchers in various fields, including mobile social networks, wireless network communications, and so on. For instance, social ties have also been studied for cooperative communications [24-26]. Mao *et al.* [24] investigated the joint social-position relationship based cooperation (JSPC) scheme and developed a partner selection algorithm. An optimal social-aware relay selection strategy

was proposed in [25] to maximize the capacity of the network. An optimal transmission beamformer design was considered in [26] based on the trust degrees to achieve a target rate in a multi-input single-output cooperative communication network. These existing work concentrates on efficiency and capacity analysis in these networks. Xu Chen *et al.* in [27] set up a coalition game theory framework to devise social-tie-based cooperation strategies for D2D communications. They exploited the social trust and social reciprocity to evaluate the performance of D2D communications. They also designed a network-assisted relay selection mechanism to achieve greater performance gains than traditional communication systems. Ling Tang *et al.* in [28] exploited the social tie concept to model the cooperative jammer's willingness to cooperate in the cooperation. X. Gong *et al.* in [29, 30] developed a framework for maximizing social group utility for cooperative wireless networks that makes into account both social relationships and physical coupling among users. Yong Li *et al.* in [31] proposed a social-aware enhanced D2D communication architecture that exploits social networking characteristics for system design. Zhang *et al.* in [32] developed a traffic offloading mechanism for D2D communication. It takes advantage of the social characteristics of an online social network to enhance the performance of the D2D system.

However, the study only showed based on the social characteristics, D2D system performance and dependability can be improved, but cannot improve the security of D2D system. According to our previous work, the social characteristics of human beings can be utilized to solve security issues [33]. Meanwhile, the cooperative jamming is considered as a promising physical layer security technology for D2D communication. So far, there are few works to study social ties among users in cooperative communications for PLS enhancement [34-36]. Zheng *et al.* [34] studied the secrecy routing of a multi-hop relay scheme using the average source destination distance based on social ties. On the other hand, both [35] and [36] proposed cooperative jamming schemes based on social ties. Tang *et al.* [35] discussed the SOP of a source-destination pair based cooperative jamming game. A jammer selection scheme based on mobility-impacted social interactions was proposed in [36] to maximize the worst-case ergodic secrecy rate. Based on social ties. Tang *et al.* [35] discussed the SOP of a source-destination pair based cooperative jamming game.

The common characteristics of these working areas are as follows.

The existing cooperative jamming works pay more attention to a single physical communication network, ignoring the impact of social network characteristics on secure communication. Each user has different strength of social tie with other users and has multiple devices located in different locations. Devices correlated with strong ties may be more positive to cooperate with others and have more willingness to help each other. In addition, a single physical communication network will have higher computational complexity. It's not easy to get benefits from actual physical devices, and the benefits should be attributed to their holders.

Previous studies have shown that each jammer can only be in two states: participation and non-participation. However, it is not appropriate in many scenarios. Since different devices may be in different locations and have different social ties with others, each jammer has the right to choose whether or not to participate in cooperative jamming in different social ties and communities. We introduce the SIR model and take into ac-

counts that each jamming has three states: probable participation, obligatory participation and non-participation.

Cooperative jamming is described as a game problem. Since the uncertain state does not simply represent by a fixed number, it is not easy to solve the game according to the previous method when considering the three states of jammers in a two-layer network.

1.2 Our Contributions

The main contributions of this paper are as follows:

(i) Social tie based cooperative jamming in a two-layer network: In order to better understand the interplay between social tie and jammers' cooperation and solve the problem of benefits on the physical devices, we propose a two-layer network model to promote efficient cooperation among jammers and attribute the benefit problem to devices' holders, S* is a social network composed by people with diverse social ties. P* is a physical communication network composed by diverse devices. We exploit the diverse social ties between users to model the jammers' cooperation behaviors. We investigate how social ties influence the cooperative jamming and how it can help solving the challenging problems of cooperative jamming. We not only promote the cooperation among jammers to decrease the secrecy outage probability but have a lower computational complexity.

(ii) Super-modular game solutions: To simplify and obtain better performance, we formulate the problem of cooperative jamming based social ties in a two-layer network as a game, where the set of all jammers is the set of players, jammers' state is the strategy set, and the utility function is proposed to be maximized by jammers. During the game, each jammer can update its own state as a best response to other jammers' states for maximizing the utility function. We design an algorithm to find the NE of the game and use the secrecy outage probability to evaluate the secrecy performance. We further prove that the game is a super-modular game, which admits the salient property and exists the pure strategy NE.

(iii) SIR spreading model: Aiming at the limitation of jammers' states, we introduce the SIR spreading model and believe that each jammer's initial state is likely to participate rather than certainly participate in the cooperation. Analogous to the three states of the SIR model: susceptibility (S), infection (I) and recovery (R), we consider each jammer has three states: probable participation, obligatory participation and non-participation, which a jammer can transform its state from the probable participation to obligatory participation by probability β or from the obligatory participation to the non-participation by probability γ. We regard the update of jammers' states as a spreading process. We select seed set from jammers as the spreading source by node's degree. We not only make jammers have more states to choose but exhibit better results by introducing the SIR model.

The rest of the paper is organized as follows. We first discuss the system model in Section 2 and then study the cooperative jamming game in two-layer network based social tie in Section 3. We evaluate the performance of the proposed method by simulations in Section 4, and finally conclude in Section 5.

2. SYSTEM MODEL

This section put forward a system model of cooperative jamming based on a two-layer network. As shown in Fig. 1, a two-layer network can be grouped into two parts: a social network and a physical network. Under the circumstances, we can enhance the security of communications by utilizing the more social characteristics and physical layer security technologies.

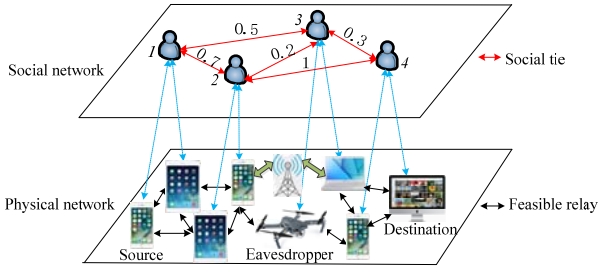


Fig. 1. Two-layer network model diagram.

2.1 Two-layer Network Model

The functionality of the two-layer network depends on both the social network and the physical network. As shown in Fig. 1, the upper-layer is a social network composed of users with diverse social ties, while the lower-layer is a physical network composed of various physical devices.

For a two-layer network with strong connectivity, the nodes in one network will be associated with more other nodes in its connected network. On the contrary, for a two-layer network with weak connectivity, the nodes in one network will be associated with fewer other nodes in its connected network [37]. In our work, we use the connecting degree to indicate the relevance of two networks. Denoting *Cd* as the connecting degree, the *Cd* of two-layer network is defined as the number of lower-layer network nodes connected to the upper-layer network node. *Cd* can be classified into two categories: the synchronous *Cd* and the asynchronous *Cd*. The synchronous connecting means that each upper-layer user node can be connected to the same number of lower-layer physical devices nodes. However, the asynchronous connecting means that the each upper-layer user node can be connected to any number of lower-layer physical devices nodes. In this paper, we only consider the synchronous connecting. We can set the connecting degree, such as in Fig. 1, the *Cd* of the two-layer network is 2. Each user is connected to 2 low-layer physical devices respectively, and their communication devices may be carried by themselves or placed in home and office. For example, user 4 has a desktop computer and a cell phone. The desktop computer is placed in his office and the cell phone is carried with him. User 2 has an iPad and a cell phone. The iPad and the phone may be with user 2 at any time, or the iPad is placed at home. Although devices belonging to user 2 and user 4 may not be in the same place, these devices would be more willing to cooperation for resisting eavesdroppers when there is a strong social tie between them.

As shown in Fig. 1, the strength of social tie between two users is represented as the

numbers annotated on the connection. When the social tie becomes stronger, the number would be larger and the user would be more likely to cooperate with each other [17]. With weak social tie, the number would be smaller and the user would be less likely to cooperate with each other. As shown in Fig. 1, the strength of social tie between user 2 and user 4 is 1, which means that the devices belonging to user 2 and user 4 are more willing to involving in the cooperative jamming in the low-layer physical communication network. The strength of social tie between user 2 and user 3 is 0.2, which means that the devices belonging to user 2 and user 3 would have less cooperation willingness between them. In our model, we can directly find the devices involved in cooperative jamming in the lower-layer physical communication network when we determine which users are closer and may help each other in the upper-layer social network. It will be more convenient and save more time by finding fewer nodes in the upper-layer social network.

2.2 Overview of Cooperative Jamming

In this part, the paper refers to the knowledge in [35]. We consider a physical network, which is made up with a pair of source and destination nodes, a group of cooperative jammers $N = 1, 2, \ldots N$ and an eavesdropper. The source, destination and the eavesdropper are equipped with a single antenna, and each jammer has at least one antenna. Here we assume that all channels are quasi-stationary and flat-fading. Let h_{sd} and h_{se} denote the channel coefficients of the source-destination and source-eavesdropper respectively. Let $\boldsymbol{h}^j_{nd}$ denote the coefficient vector of the channel between the destination and jammer n. Let $\boldsymbol{h}^j_{nes}$ denote the coefficient vector of the channel between the eavesdropper and jammer n. For the elements of h_{sd}, h_{se}, $\boldsymbol{h}^j_{nd}$, and $\boldsymbol{h}^j_{nes}$, they are independent zero-mean and unit variance complex Gaussian random variables. Let $\boldsymbol{w}_n$ with $\|\boldsymbol{w}_n\|^2 = 1$ denotes jamming signal z_n's weight vector. Let R_b denote the main channel coding rate and R_s denote the confidential information rate. This is our low-layer network, which jammers participate in cooperation. We can find the user nodes in the upper-layer social network and then correspond the lower-layer's physical devices to proceed the cooperative jamming.

We assume that $a = (a_1, a_2, \ldots, a_N)$ denotes all jammers' state sequence in the lower-layer communication physical network. Let $a_n \in [0,1]$ denotes the participation willingness of the jammer n, 0 stands for non-participation, and 1 stands for obligatory cooperation. If n between 0 and 1 indicates that jammer has some possible of cooperation. In the physical communication network, the secrecy outage probability can be as [38]:

$$\begin{aligned} p_{so} &= \Pr\left(\frac{\frac{P_s}{P_J}\left|h_{se}\right|^2}{\sum_{n=1,a_{n=1}}^{N}\left|\boldsymbol{w}_n^H \boldsymbol{h}_{ne}^j\right| + \sigma_e^2 / P_J} > 2^{R_b - R_s} - 1\right) \\ &= \int_0^{\infty}\left(\int_{(2^{R_b-R_s}-1)(y+\sigma_e^2/P_J)}^{\infty} f(x)dx\right) f(y)dy \\ &= \exp\left(\frac{\sigma_e^2(1-2^{R_b-R_s})}{P_s}\right)\left(1+\frac{2P_J 2^{R_b-R_s}}{P_s}\right)^{-\sum_{n=1}^{N} a_n} \\ &= AB^{-\sum_{n=1}^{N} a_n} \end{aligned} \tag{1}$$

where

$$A=\exp((\sigma_e^2(1-2^{R_b-R_s}))/P_s),\ B=(1+(2P_J2^{R_b-R_s})/P_s).$$

In Eq. (1), P_s and P_n denote the transmitting power of the source and the jammer n respectively, and σ_d^2, σ_e^2 denote the noise variance at the destination and eavesdropper respectively.

In the upper-layer social network, the social relationships between users is represented as the concept of the strength of social ties. Let $\boldsymbol{a}_{-n}$ stands for all other jammer's status except the jammer n. Initially, each jammer is in an unknown state, not sure whether participate in cooperative jamming. In the process of cooperative jamming, each jammer has the following state: 0 means not to participate, 1 means to participate in the cooperation, the possible state is between 0 and 1. The efficiency function of the jammer n in cooperative jamming can be expressed as:

$$U_n(a_n,\boldsymbol{a}_{-n})=\begin{cases}s_n(1-p_{so}(a_n,\boldsymbol{a}_{-n}))-c_n, a_n\in[0,1]\\ 0, \qquad\qquad\qquad a_n=0\end{cases}. \tag{2}$$

In Eq. (2), $s_n\in[0,1]$ stands for the strength of social tie among users in the upper-layer social network, while c_n is the jammer n's weig cost for participating in the cooperative jamming. The transmit power of the P_n and the consumption r_n decide on the cost c_n. As shown in Fig. 1, so stronger social tie between user 1 and user 2 that the devices carried by them are more pleased to cooperate. We assume that devices carried by user 1 and user 2 take part in the cooperation in the lower-layer communication physical network, and the connected devices in the lower-layer physical network is the real jammers involved in the cooperative jamming. On account of the social tie between user 2 and user 3 is weaker, devices belonging to user 3 has a slight possibility to participate in the cooperation between user 1 and user 2's devices, so they would not bear on the improvement of communication quality.

3. COOPERATIVE JAMMING GAME IN TWO-LAYER NETWORKS WITH SOCIAL TIE

In this section we will introduce a game theory approach to describe cooperative jamming with social ties in a two-layer network. We convert the problem into a game $\Gamma=(N, \{A_n\}_{n\in N}, \{U_n\}_{n\in N})$, in which N is a group of participants in the game, $A_n=\{0, 1\}$ is the set of strategies of the jammer n, meanwhile $U_n=(a_n, \boldsymbol{a}_{-n})$ is the maximum utility function of the jammer n. We call it the cooperative jamming game based on the two-layer network with social tie (TLNST-CJG).

3.1 TLNST-CJG Nash Equilibrium

Definition 1: When there is a set of strategies $\boldsymbol{a}^*=(a_1^*, ..., a_N^*)$ so that no other jammers increase their own effectiveness by unilaterally changing their own decisions, namely:

$$U_n(a_n^*, \boldsymbol{a}_{-n}^*) \geq U_n(a_n^*, \boldsymbol{a}_{-n}^*), \forall a_n \in A_n, n \in N \tag{3}$$

$\boldsymbol{a}^* = (a_1^*, ..., a_N^*)$ is called a Nash equilibrium of the game.

Proposition 1: The utility function $U_n = (a_n, a_{-n})$ of the jammers exhibits an increasing diversity and is super-modular in a_n, $\forall n \in N$.

***Proof*:** Let the initial state of jammer n be $a_n \in \{0, 1\}$. According to the Eq. (3) of the security outage probability and the utility function of the jammer, for two different states a and a', we have

$$\begin{aligned} &U_n(1, \boldsymbol{a}_{-n}) - U_n(0, \boldsymbol{a}_{-n}) - (U_n(1, \boldsymbol{a}'_{-n}) - U_n(0, \boldsymbol{a}'_{-n})) \\ &= -S_n A B^{-\sum_{n=1}^{N} a_n} + S_n A B^{-\sum_{n=1}^{N} a'_n}. \end{aligned} \tag{4}$$

Let $a \leq a'$, then $a_n \leq a'_n$, $\forall n \in N$. Based on Eq. (4), if $a_{-n} \leq a'_{-n}$, we have

$$U_n(1, \boldsymbol{a}_{-n}) - U_n(0, \boldsymbol{a}_{-n}) \leq U_n(1, \boldsymbol{a}'_{-n}) - U_n(0, \boldsymbol{a}'_{-n}). \tag{5}$$

It manifests that the benefit function $U_n = (a_n, a_{-n})$ is increasing. Since the strategy space of TLNST-CJG game is one-dimensional, this incremental difference indicates that the game is super-modular. By Proposition 1, it can be known that TLNST-CJG is a super-modular game, *i.e.*, the process of cooperative jamming in a two-layer network meets the super-modular game. Super-modular game has a notable characteristic, which is the existence of pure strategy Nash equilibrium.

Proposition 1 depicts that there exists NEs with different secrecy performance in the proposed TLNST-CJG game. To achieve the best NE with the minimum secrecy outage probability among all NEs, we design an algorithm for calculating the optimal NE.

Here we assume that the sequence of jammers is 1, 2, ..., N. We give a probable participation sequence with a normal distribution in the initial state for all jammers. We designed an algorithm to acquire the NE under diverse social ties. As described by Algorithm 1, in each iteration, the uncertain jammers update their states asynchronously and there no two jammers update in the meantime. In the kth iteration, make a_{-n}^k denotes the state of other jammers. We hold the opinion that jammers improve their own efficiency when $U_n(1, a_{-n}^k) - U_n(0, a_{-n}^k) < 0$. By Proposition 1, the state of the jammer is not going back to the original state. The state of jammer n is fixed, even though in the following iterations. The algorithm stopped iterating when $a^{k+1} = a^k$.

On account of the upper limit of the maximum number of uncertain jammers is N, the computational complexity of each iteration is $O(N)$. Each iteration confirms the state of Cd jammers at least. Hence, Algorithm 1 terminate after N/Cd iterations consequentially, and the upper limit of complexity is $O(N^2/Cd)$. If the same algorithm 1 is used to perform the cooperative jamming in a single physical communication network purely. Each iteration determines the state of a jammer at least. Algorithm 1 terminate after N iterations consequentially and the upper limit of complexity is $O(N^2)$. It can be seen that, compared to a single physical communication network, the time complexity of a two-layer network is reduced by $1/Cd$.

Algorithm 1: Calculate NE for TLNST-CJG

initialization: the iteration number $k=0$, jammers set $\bar{N}=N$
  loop until $\boldsymbol{a}^{k+1}=\boldsymbol{a}^{k}$
    loop for jammer $n \in \bar{N}$
      if $(U_n(1, \boldsymbol{a}_{-n}^{k}) - U_n(0, \boldsymbol{a}_{-n}^{k}) < 0)$ **then**
        assign $\boldsymbol{a}^{k+1}=0$ and **remove** n from $\bar{N}$
      else assign $\boldsymbol{a}^{k+1}=1$
      end if
    end loop
set $k=k+1$.
end loop

3.2 The Combination of SIR Model and Game Theory

In the SIR model, each individual is in the one of the following states: susceptible, infected or recovered. Susceptible individuals represent those who lack of immunity but not sick. Infected individuals represent infected with diseases which can be transmitted to susceptible members. Recovered individuals are isolated or have immunity by recovering from an illness. Individual's state can be changed by the SIR spreading mechanism. To be specific, a susceptible individual will recover with an average recovery probability γ after infected with the infection probability β [39].

The SIR model speeding process can be divided into three stages as follow:

- Setting the seed node. The seed node is used as an informational source and diffuse information according to the SIR spreading mechanism. The seed node is in infection state after receiving information. The rest of nodes is in susceptibility state. There are no recovered nodes at this stage.
- Contact stage: At each time step of the spreading process, the nodes make contact through the connected edges. Infected nodes affect the adjacent susceptible nodes. If is successful, the adjacent nodes change to the infected state. The probability of successful infection is infection rate β.

Immunization stage: At each step, infective node has the ability to change to the recovery state, then, no longer participates in the spreading process. The self-healing ability is the recovery rate γ.

Therefore, we have opinion that jammers have the right to choose whether or not to cooperate with others. Jammer's decision may be influenced by a number of factors, for instance, the strength of social, the community and so on. In order to make our research more efficient than previous research. Here we bring in the SIR spreading model. We have opinion that the initial state is indeterminate for all jammers. And jammers can choose state from Probable participation, Obligatory participation or Non-participation. Similar to the three stages of SIR spreading process, we divide the process of jammers' states transform into three phases as follow:

- Setting the initial state phase: We choose the seed jammers by DC algorithm [40]. Except for the seed jammers, all other jammers' state is in Probable participation.
- Contact phase. At each time step, Obligatory participation jammers affected the adjacent Probable participation jammers. If it is successful, the adjacent jammers change to the

Obligatory participation. The probability of successful change is the infection rate β.

- Immunization phase: At each time step, Obligatory participation jammers can change to the Non-participation. If itis successful, no longer participate in the process of updating states. The probability of successful change is self is the recovery rate γ.

The idea of the DC algorithm is to get the ordered sequence of nodes based on the degree value, then directly choose the first k elements as the seed set. The DC value of node i is defined as:

$$C_{DC}(i) = k(i). \tag{6}$$

Here $k(i)$ is the degree of node i. The degree of a node is defined as the total number of edges directly connected to it. Let N denotes the number of node, a_{ij} tag the edges between node i and node j. If there is an edge between i and j, $a_{ij}=1$, otherwise $a_{ij}=0$. The degree of node i is given by Eq. (7)

$$k(i) = \sum_{1\le j\le N} a_{ij}. \tag{7}$$

We convert the cooperative jamming in a two-layer network with SIR characteristic problem into a game $\Omega=(N, \{A_n\}_{n\in N}, \{U_n\}_{n\in N})$, which N is the set of participants in the game, $A_n=[0, 1]$ is the set of strategies of the jammer n, and $U_n=(a_n, a_{-n})$ is the maximum utility function of the jammer n. We call it as the cooperative jamming, which based on the two-layer network with social tie and SIR characteristic (TLNSTSIR-CJG). As shown in Definition 1, proved that there is still exist a Nash equilibrium after introducing the SIR model. Let $a_n\in[0, 1]$ denotes the participation willingness of the jammer n, which 0 means non-participation, and 1 means to obligatory cooperation. Another situation between 0 and 1 indicates that jammer is possible cooperation. By the formula of the security outage probability and the utility function of the jammer, we demonstrated the important property of the utility of jammers, and given the following proposition.

Proposition 2: The utility function $U_n = (a_n, a_{-n})$ of the jammers exhibits an increasing diversity and is super-modular in a_n, $\forall n\in N$ when each jammer's initial state is in [0, 1].

There are two situations to prove it. In the first case, the jammer updates own state from the probable participation state to the non-participation state. In the second case, the jammer updates own state from the probable participation to the obligatory participation, and then to the non-participation with a certain probability.

***Proof*:** Let $t\in(0,1)$ denotes the initial state sequence of jammers. On the one hand, given two states a and a', we have

$$U_n(t,\boldsymbol{a}_{-n}) - U_n(0,\boldsymbol{a}_{-n}) - (U_n(t,\boldsymbol{a}'_{-n}) - U_n(0,\boldsymbol{a}'_{-n})) = -s_n AB^{-\sum_{n=1}^{N} a_n} + s_n AB^{-\sum_{n=1}^{N} a'_n}. \tag{8}$$

Let $a\le a'$, then $a_n\le a'_n$, $\forall n\in N$. Based on Eq. (8), if $a_{-n}\le a'_{-n}$, we have

$$U_n(t,\boldsymbol{a}_{-n}) - U_n(0,\boldsymbol{a}_{-n}) - (U_n(t,\boldsymbol{a}'_{-n}) - U_n(0,\boldsymbol{a}'_{-n})) = -s_n AB^{-\sum_{n=1}^{N} a_n} + s_n AB^{-\sum_{n=1}^{N} a'_n} \le 0. \tag{9}$$

On the other hand, given two states a^o and a^Δ, we proved it through contradiction. Assume the utility function $U_n = (a_n, a_{-n})$ would not show an increasing characteristic when the initial state of jammer changes from the probable participation to the obligatory participation. In other words, $a_n \le a'_n$, $\forall n \in N$.

$$U_n(t, \boldsymbol{a}_{-n}^{\Delta}) - U_n(1, \boldsymbol{a}_{-n}^{\Delta}) - (U_n(t, \boldsymbol{a}_{-n}^{o}) - U_n(1, \boldsymbol{a}_{-n}^{o})) \ge 0 \tag{10}$$

However, the utility of jammers increases or decreases when jammers change states in the cooperation, which can be expressed as:

$$\begin{aligned} &U_n(t, \boldsymbol{a}_{-n}^{\Delta}) - U_n(1, \boldsymbol{a}_{-n}^{\Delta}) - (U_n(t, \boldsymbol{a}_{-n}^{o}) - U_n(1, \boldsymbol{a}_{-n}^{o})) \\ &= -s_n AB^{-\sum_{n=1}^{N} a_n^{\Delta}} + s_n AB^{-\sum_{n=1}^{N} a_n^{\Delta}} - s_n AB^{-\sum_{n=1}^{N} a_n^{o}} + s_n AB^{-\sum_{n=1}^{N} a_n^{o}} = 0. \end{aligned} \tag{11}$$

On account of the characteristic of SIR, some jammers would not take part in cooperative jamming with a certain γ probability. Then the benefit of jammers would be lost. Which explains the utility function would exhibit an increasing characteristic and supermodular.

By Proposition 2, there exists NEs with different secrecy performance for the proposed CNSTSIR-CJG game. In order to achieve the best NE with the minimum secrecy outage probability among all NEs, we design an algorithm, as described in Algorithm 2.

Likewise, the upper limit of complexity of Algorithm 2 is $O(N2/C)$. The time complexity of a two-layer network is reduced by $1/Cd$ compared to a single physical communication network.

Algorithm 2: Calculate NE for TLNSTSIR-CJG

initialization: the iteration number $k = 0$, jammers set $\bar{N} = N$, jammers' initial states $\boldsymbol{t}$, the updated state $\boldsymbol{t}'$
loop until $\boldsymbol{a}^{k+1} = \boldsymbol{a}^k$
loop for jammer $n \in N$
  if $(\boldsymbol{t}' = 0)$
    if $(U_n(\boldsymbol{t}, \boldsymbol{a}_{-n}^k) - U_n(\boldsymbol{t}', \boldsymbol{a}_{-n}^k) < 0)$ **then**
      assign $\boldsymbol{a}^{k+1} = 0$ and **remove** n from $\bar{N}$
    else assign $\boldsymbol{a}^{k+1} = t$
    end if
  else if $(\boldsymbol{t}' = 1)$
    if $(U_n(\boldsymbol{t}, \boldsymbol{a}_{-n}^k) - U_n(\boldsymbol{t}', \boldsymbol{a}_{-n}^k) < 0)$ **then**
assign $\boldsymbol{a}^{k+1} = 1$ and **remove** n from $\bar{N}$
    else assign $\boldsymbol{a}^{k+1} = t$
    end if
  end if
end loop
set $k = k+1$.
end loop

4. RESULTS

In this section, we simulate the previous methods and compare with the methods proposed in this paper. We assume that the transmitter power of each jammer is 10 dB,

and the transmitting power of the source is $P_s = 20$dB. The noise at each receiving node is 1 and $R_b = 2$, $R_s = 1$. The $c_n s$ are uniformly generated in the interval [0, 0.5]. In addition to jammers seeds, the strength of social tie is evenly generated in the interval (0, 1). The number of nodes is 50 in the upper social network, and the number of nodes is 100 in the lower one. The upper social network is the ER network. The degree distribution of the upper social network as shown in Fig. 2.

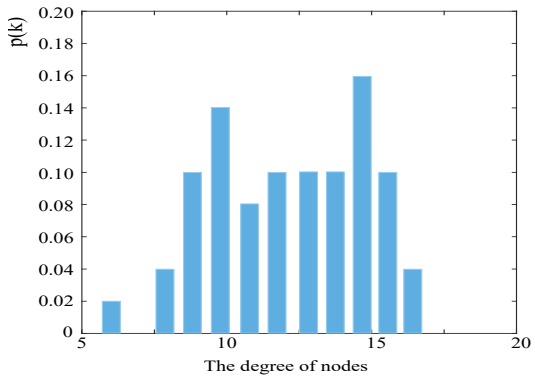


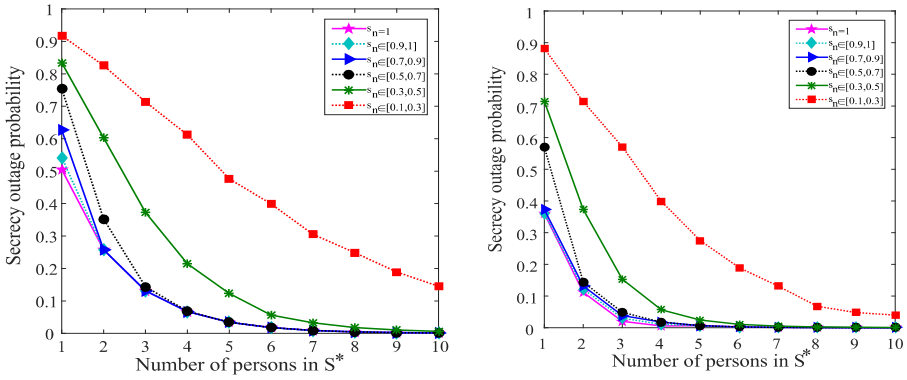
Fig. 2. The degree distribution nodes in the upper social network.

4.1 The Secrecy Outage Probability in Two-layer Network with Different Social Ties

In Algorithm 1, we simulate the change of secrecy outage probability with the number of jammers. The strength of the social ties is uniformly generated in the interval [0.9, 1], [0.7, 0.9], [0.5, 0.7], [0.3, 0.5], [0.1, 0.3], [1, 1]. The results are shown in Figs. 3 (a)-(b) and Figs. 4 (a)-(b).

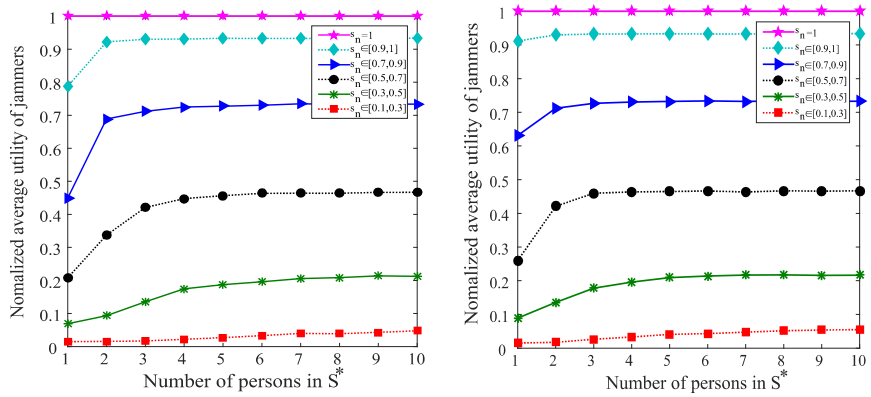
From Figs. 3 (a)-(b), we can see that the secrecy outage probability decreases as the number of jammers increases. With stronger social tie, the secrecy outage probability would be closer to the minimum secrecy outage probability with all jammers participating. It can be seen from Figs. 4 (a)-(b) that the average efficiency of jammers increases with the number of jammers. Moreover, the larger the connecting degree, the smaller the secrecy outrage probability. This is because when social ties are stronger, each jammer is more likely to participate in cooperation, that is, when a user has a strong social tie with others, they will get more help to enhance their own ability to cooperate. On the contrary, when it has weak social ties with others, it will obtain less help. The users correlated to strong ties may be expected to offer more communication cooperation and have higher secrecy performance than those with weak ties.

Figs. 5 (a)-(b) and Figs. 6 (a)-(b) are the comparison of single network and two-layer network. As can be seen from these figures, the secrecy outage probability in the upper social network decreases with the increase of the number of people, and the secrecy outage probability in two-layer network is lower. Since our two-layer network enables one person to have multiple diverse devices. Compared with the single layer network, the computational complexity of the two-layer network is reduced by $1/Cd$.



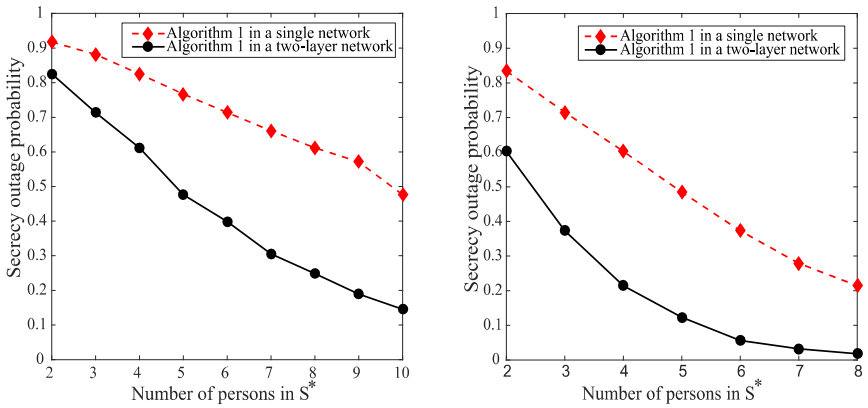
(a) $Cd=2$ (b) $Cd=3$

Fig. 3. The secrecy outage probability in the two-layer network with different social ties.



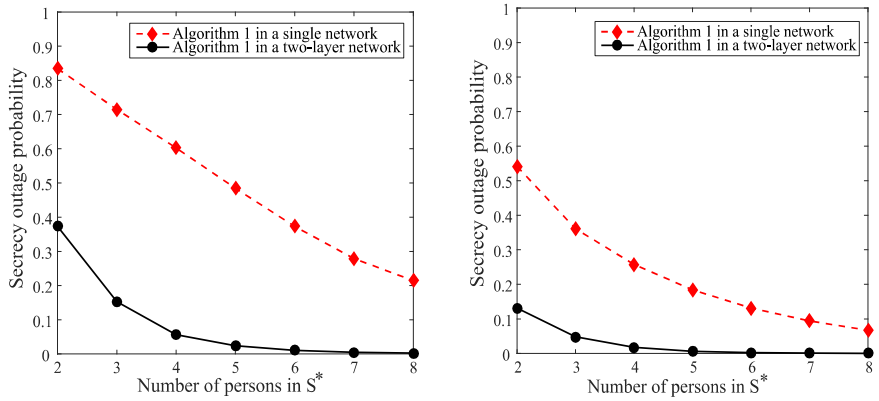
(a) $Cd=2$ (b) $Cd=3$

Fig. 4. The normalized average utility of jammers.



(a) $Cd=2$, $s_n\in[0.1,0.3]$ (b) $Cd=2$, $s_n\in[0.3,0.5]$

Fig. 5. Comparison of the two-layer network with the single network.

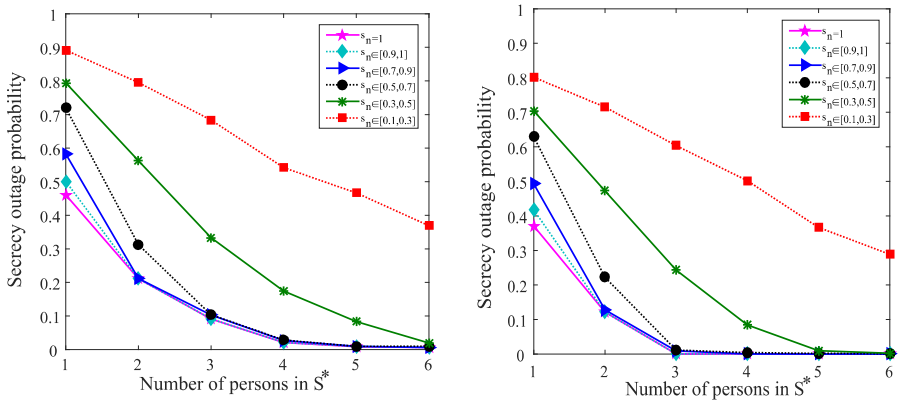


(a) $Cd=3$, $s_n \in [0.3,0.5]$ (b) $Cd=3$, $s_n \in [0.9,1]$

Fig. 6. Comparison of the two-layer network with the single network.

4.2 Cooperative Jamming with the SIR

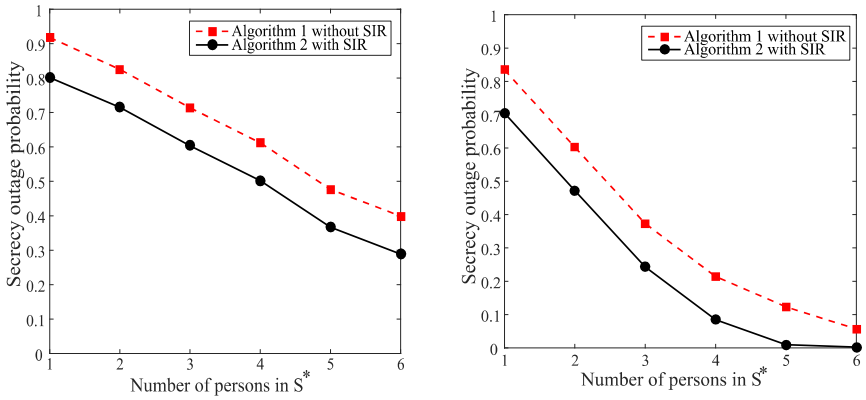
Let $\beta=0.2$, $Cd=2$, and $\gamma=1$. According to the process of jammers' states transform and the TLNSTSIR-CJG, the results after introducing the SIR characteristic is shown in Figs. 7-9 (a)-(b).



(a) $\beta=0.08$ (b) $\beta=0.2$

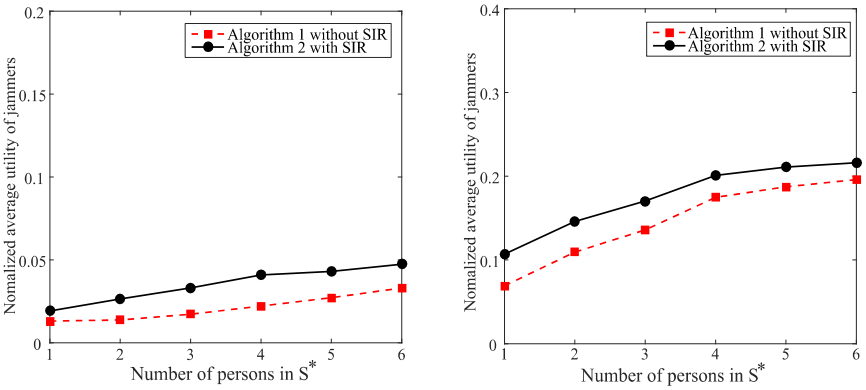
Fig. 7. Cooperative jamming in the two-layer network with SIR characteristic.

Figs. 7 (a)-(b) show that with the increase of the number of jammer, secrecy outage probability decreases. The influence is greater when $\beta=0.2$. From Figs. 9-10 (a)-(b) we can see that the cooperation efficiency with the SIR characteristic would be slightly better than the situation where each jammer has only two states. This is due to the fact that the SIR spreading mechanism will first make a pre-judgment on the jammers' initial, and then we can use Algorithm 2 to calculate the benefits of jammers. Moreover, it is closer to our real life scenarios and more universal.



(a) $s_n \in [0.1,0.3]$ (b) $s_n \in [0.3,0.5]$

Fig. 8. Comparison cooperative jamming based on the SIR model with the traditional method.



(a) $s_n \in [0.1,0.3]$ (b) $s_n \in [0.3,0.5]$

Fig. 9. Comparison the normalized average utility of jammers based on the SIR model with the traditional method.

5. CONCLUSIONS

In this paper, we have developed the two-layer network model based on social ties and SIR characteristic to research the cooperative jamming. We transform the problem into a game. The result shows that with the increase of social ties, the cooperative jamming in the two-layer network improves the communication quality. When jamming has a stronger social tie, it would get more help to enhance its ability to cooperate, and when jamming has a weak social connection, it would get less help. Compared with previous studies, our algorithm's computational complexity is reduced by $1/Cd$. Furthermore, we introduced the SIR spreading model. Each jammer has three states to update, which is not so absolute and more universal. The results show that the cooperation efficiency with SIR characteristics is slightly better than that of each jammer in only two states.

We believe that the cooperative jamming in the two-layer network is more conducive to improving the communication quality. Our work needs to be further improved,

not only the synchronous *Cd* but also the asynchronous *Cd* during the connecting process. The topology of social networks deserves further attention. In addition, we believe that cooperative jamming in the two-layer network will open a new door for future by exploiting social characteristics such as centrality, community and others.

REFERENCES

1. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, Vol. 29, 2013, pp. 1645-1660.
2. L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, Vol. 54, 2010, pp. 2787-2805.
3. D. Lake, A Rayes, and M. Morrow, "The Internet of Things," *Internet Protocol Journal*, Vol. 15, 2012, pp. 10-19.
4. Y. Xu, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Physical layer security-aware routing and performance tradeoffs in ad hoc networks," *Computer Networks*, Vol. 123, 2017, pp. 77-87.
5. Y. Zhang, Y. Shen, H. Wang, and X. Jiang, "Friendship-based cooperative jamming for secure communication in poisson networks," *Wireless Networks*, 2016, pp. 1-19.
6. N. Kayastha, D. Niyato, P. Wang, and E. Hossain, "Applications, architectures, and protocol design issues for mobile social networks: A survey," *Proceedings of the IEEE*, Vol. 99, 2011, pp. 2130-2158.
7. X. Chen, *et al.*, "Social trust and social reciprocity based cooperative D2D communication," in *Proceedings of the 14th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2013, pp. 187-196.
8. E. Altman, T. Boulogne, R. EI-Azouzi, T. Jimenez, and L. Wynter, "A survey on networking games in telecommunications," *Computers & Operations Research*, Vol. 33, 2006, pp. 286-311.
9. D. Feng, L. Lu, Y. Yuan-Wu, G. Y. Li, G. Feng, and S. Li, "Device-to-device communications underlaying cellular network," *IEEE Transactions on Communications*, Vol. 61, 2013, pp. 3541-3551.
10. Z. Ye, *et al.*, "A dynamic bandwidth and power allocation scheme for cooperative D2D communications," in *Proceedings of IEEE 28th Annual International Symposium on Personal*, *Indoor*, *and Mobile Radio Communications*, 2017, pp. 1-6.
11. Y. Fang, Y. Zhou, X. Jiang, D. Zhang, and Y. Zhang, "Game theoretic D2D content Sharing: Joint participants selection, routing and pricing," in *Proceedings of the 26th International Conference on Computer Communication and Networks*, 2017, pp. 1-9.
12. C. Xu, *et al.*, "Joint relay selection and resource allocation for energy-efficient D2D cooperative communications using matching theory," *Applied Sciences*, Vol. 7, 2017, pp. 491-491.
13. S. Wang, *et al*., "A novel interference management scheme in underlay D2D communication," in *Proceedings of Vehicular Technology Conference*, 2015, pp. 1-5.
14. J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, Vol. 17, 2015, pp. 1294-1312.

15. M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*, Cambridge University Press, UK, 2011.
16. Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Processing Magazine*, Vol. 30, 2013, pp. 29-40.
17. H. Zhang, T. Wang, and L. Song, "Radio resource allocation for physical-layer security in D2D underlay communications," in *Proceedings of IEEE International Conference on Communications*, 2014, pp. 2319-2324.
18. D. Zhu, A. L. Swindlehurst, and S. A. A. Fakoorian, "Device-to-device communications: The physical layer security advantage," in *Proceedings of IEEE International Conference on Acoustics*, *Speech and Signal Processing*, 2014, pp. 1606-1610.
19. Y. Xu, J. Liu, Y. Shen, X. Jiang, and T. Taleb, "Security/QoS-aware route selection in multi-hop wireless ad hoc networks," in *Proceedings of IEEE International Conference on Communications*, 2016, pp. 1-6.
20. Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C.-H. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Communications*, Vol. 18, 2011, pp. 66-74.
21. J. Sun, X. Chen, J. Zhang, Y. Zhang, and J. Zhang, "SYNERGY: A game-theoretical approach for cooperative key generation in wireless network," in *Proceedings of IEEE International Conference on Computer Communications*, 2014, pp. 997-1005.
22. W. Xi, X. Li, C. Qian, J. Han, S. Tang, J. Zhao, and K. Zhao, "KEEP: Fast secret key extraction protocol for D2D communication," in *Proceedings of IEEE 22nd International Symposium of Quality of Service*, 2014, pp. 350-359.
23. J. Kleinberg, "The convergence of social and technological networks," *Communications of the ACM*, Vol. 51, 2008, pp. 66-72.
24. H. Mao, W. Feng, Y. Zhao, and N. Ge, "Joint social-position relationship based-cooperation among mobile terminals," *IEEE Communications Letters*, Vol. 18, 2014, pp. 2165-2168.
25. M. Zhang, X. Chen, and J. Zhang, "Social-aware relay selection for cooperative networking: An optimal stopping approach," in *Proceedings of IEEE International Conference on* Communications, 2014, pp. 2257-2262.
26. J. Y. Ryu, J. Lee, and T. Q. S. Quek, "Trust degree based beamforming for MISO cooperative communication system," *IEEE Communications Letters*, Vol. 19, 2015, pp. 1957-1960.
27. X. Chen, B. Proulx, and X. Gong, "Exploiting social ties for cooperative D2D communications: A mobile social networking case," *IEEE/ACM Transactions on Networking*, Vol. 23, 2015, pp. 1471-1484.
28. L. Tang, H. Chen, and Q. Li, "Social tie based cooperative jamming for physical layer security," *IEEE Communications Letters*, Vol. 19, 2015, pp. 1790-1793.
29. X. Gong, X. Chen, and J. Zhang, "Social group utility maximization in mobile networks: From altruistic to malicious behavior," *Information Sciences and Systems*, 2014, pp. 1-6.
30. X. Chen, X. Gong, L. Yang, and J. Zhang, "Exploiting social tie structure for cooperative wireless networking: A social group utility maximization framework," *IEEE/ACM Transactions on Networking*, Vol. 24, 2016, pp. 3593-3606.
31. Y. Li, T. Wu, P. Hui, D. Jin, and S. Chen, "Social-aware D2D communications:

Qualitative insights and quantitative analysis," *IEEE Communications Magazine*, Vol. 52, 2014, pp. 150-158.
32. Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, and Z. Han, "Social network aware device-to-device communication in wireless networks," *IEEE Transactions on Wireless Communications*, Vol. 14, 2015, pp. 177-190.
33. Z. Yan and M. Wang, "Protect pervasive social networking based on two-dimensional trust levels," *IEEE Systems Journal*, Vol. 11, 2014, pp. 207-218.
34. K. Zheng, *et al.*, "Secrecy capacity scaling of large-scale networks with social relationships," *IEEE Transactions on Vehicular Technology*, Vol. 66, 2017, pp. 2688-2702.
35. L. Tang, H. Chen, and Q. Li, "Social tie based cooperative jamming for physical layer security," *IEEE Communications Letters*, Vol. 19, 2015, pp. 1790-1793.
36. L. Wang, H. Wu, and G. L. Stüber, "Cooperative jamming-aided secrecy enhancement in P2P communications with social interaction constraints," *IEEE Transactions on Vehicular Technology*, Vol. 66, 2017, pp. 1144-1158.
37. M. Gong, L. Ma, Q. Cai, and L. Jiao, "Enhancing robustness of coupled networks under targeted recoveries," *Scientific Reports*, Vol. 5, 2015, No. 8349.
38. X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Communications Letters*, Vol. 15, 2011, pp. 302-304.
39. L. Lu, T. Zhou, Q.-M. Zhang, and H. E. Stanley, "The H-index of a network node and its relation to degree and coreness," *Nature Communications*, Vol. 7, 2016, No. 10168.
40. L. C. Freeman, "Centrality in social networks conceptual clarification," *Social Networks*, Vol. 1, 1978, pp. 215-239.

Yan Gao (高燕) received her B.Sc. degrees from Xi'an University of Science, China in 2015 and Technology and M.S. degrees from Xidian University, China, in 2018.

Yong Zeng (曾勇) received his B.Sc, M.S., and Ph.D. degrees from Xidian University in 2000, 2003, and 2008, respectively. Since 2007 he has been with Xidian University as an Associate Professor. His research interests include cryptography, physical-layer security, and complex network.

Zhi-Hong Liu (刘志宏) received his B.Sc. degree from National University of Defense Technology, China, in 1989, his M.S. degree in Computer Science from Air Force Engineering University, China, in 2001, and his Ph.D. degree in Cryptography from Xidian University in 2009. Now he is with the School of Cyber Engineering at Xidian University. His research areas include mobile computing and information security.

Jian-Feng Ma (马建峰) received his B.Sc. degree from Shaanxi Normal University, China, in 1985, and his M.Sc. and Ph.D. degrees in Computer Software and Communications Engineering from Xidian University in 1988 and 1995, respectively. He is currently a Professor and Ph.D. supervisor at the School of Computer Science and Technology, Xidian University. His current research interests include information and network security and computer networks. He has published more than 200 refereed articles in these areas and coauthored more than 10 books. He is a Senior Member of the Chinese Institute of Electronics.

Yang Liu (刘洋) received the bachelor's degree from Yunnan University, China, in 2018, and is currently pursuing the master's degree at Xidian University, China.

Yi-Kai Liu (刘易凯) received his B.Eng degree from ShanXi University, China, in 2018.