Social-Aware Secret Key Generation for Secure Device-to-Device Communication via Trusted and Non-Trusted Relays

Muhammad Waqas, Manzoor Ahmed, Yong Li, *Senior Member, IEEE*, Depeng Jin, *Member, IEEE*, and Sheng Chen, *Fellow, IEEE*

***Abstract*— Physical layer security (PLS) is a promising technology in device-to-device (D2D) communications by exploiting reciprocity and randomness of wireless channels, which attracts considerable research attention in the D2D communications community. In this paper, we investigated PLS for secure key generation rate (SKGR) in D2D communications based on cooperative trusted and non-trusted relays. By leveraging social ties, we exploit three social phenomena for secure communications, i.e., trusted scenario (social trust), non-trusted scenario (social reciprocity), and partially trusted scenario (mixed social trust and social reciprocity). The coalition game theory is further utilized to select the optimal relay pairs for improving SKGR. On the basis of social ties, we develop an algorithm for SKGR that protects the keys secret from both eavesdropper and non-trusted selected relays. We incorporate secure relays selection and system wide security for D2D communications. The stability and convergence of the proposed algorithm are also proved in this paper. Both numerical and analytical results verify effectiveness and consistency of our proposed scheme, which ensures better SKGR performance in D2D communications.**

***Index Terms*— Device-to-device communication, physical layer security, key generation rate, social ties, social trust, social reciprocity.**

I. Introduction

With the dramatic increase of smart mobile devices and the proliferation of wireless communication applications, mobile traffic has continuously increased at an exponential rate. According to Cisco, global mobile data traffic grew 63 percent in 2016 and reached to 7.2 exabytes per month at the end of 2016, up from 4.4 exabytes per month at the end of 2015 [1]. Cisco also forecasts that global mobile data traffic will increase sevenfold between 2016 and 2021, reaching 49 exabytes per month by 2021 [1]. To meet this ever-increasing demand, device-to-device (D2D) communication has been actively considered as a promising technical component for the next-generation cellular network [2]. It enables mobile devices in proximity to communicate directly at high data rate, low power consumption, and low latency, without involving the cellular infrastructure. Therefore, D2D communication is an enabling technology to assist overburdened cellular networks by improving spectrum efficiency, throughput, network coverage and delay [3]. Most of the studies have focused on various technical problems in D2D communication, including mode selection [4], resource allocation [5]–[7] and interference management [8]. However, D2D security under the PLS technique in term of key generation, and by leveraging social ties that can unify security solutions is not yet matured [9].

Owing to the openness of wireless links, any receiver located within the communication range of the transmitter can receive the transmitted signal naturally. In addition, adversaries can initiate various passive and active attacks during the communication period [9]. Thus, security is a paramount concern in wireless communication [10]–[13]. Given the inherent vulnerability of wireless links, any D2D transmission can be easily obtained by unauthorized users deployed within its range. In this regard, classical encryption schemes based on secret key sharing are typically used for securing information between communicating nodes. However, this approach is less attractive for D2D communication because unlike the cellular tier that is supported by a strong centralized infrastructure, the D2D tier relies on a loosely distributed infrastructure, and a mobile device has limited computational capability. In addition, generating secret keys depends on every node possessing a public key certificate in classical encryption schemes. It is questionable that whether each mobile device in D2D communication can bear a public key certificate. Last not the least, in classical encryption schemes, the public key infrastructure also needs to be secured [14]. By contrast, a physical layer security (PLS) technique secures the communication between the two D2D devices by applying the physical characteristics of the wireless channel between the two D2D users. Since an eavesdropper does not have the knowledge of the channel variations between the two communicating D2D devices, it can be prevented from reading the transmitted messages between the D2D users. Consequently, by exploiting dynamic channel

Manuscript received July 3, 2017; revised November 21, 2017, January 19, 2018, and February 15, 2018; accepted March 13, 2018. Date of publication April 5, 2018; date of current version June 8, 2018. This work was supported in part by the National Nature Science Foundation of China under Grant 61621091 and Grant 61673237 and in part by the Research Fund of Tsinghua University–Tencent Joint Laboratory for Internet Innovation Technology. The associate editor coordinating the review of this paper and approving it for publication was M. Kountouris. *(Corresponding author: Yong Li.)*

M. Waqas, M. Ahmed, Y. Li, and D. Jin are with the Beijing National Research Center for Information Science and Technology, Department of Electronics Engineering, Tsinghua University, Beijing 100084, China (e-mail: wa-j15@mails.tsinghua.edu.cn; manzoor.achakzai@gmail.com; liyong07@tsinghua.edu.cn; jindp@tsinghua.edu.cn).

S. Chen is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K., and also with King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: sqc@ecs.soton.ac.uk).

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/TWC.2018.2817607

variations, PLS techniques [9] can overcome diverse security threats to data transmission and user privacy.

According to [15], authentication can also be achieved through secret keys by utilizing PLS techniques. The problem of impersonation attack for example can be tackled by adding the authentication signal to the message signal in such a way that the authentication signal appears as noise to the message signal based on PLS techniques. Unlike conventional cryptography which works by ensuring that all the involved entities load and execute the proper and authenticated cryptographic information, PLS takes the advantages of channel randomness nature of transmission media to achieve communication confidentiality and authentication [16]. The essence of PLS techniques is to recognize the identity information that relies on the uniqueness of the channel state information (CSI) of the transmit-receive channel medium linking the source and destination. The CSI is essentially invariant within the channel coherent time, which gives the transmitter and receiver the opportunities to emulate or acquire the correlation characteristics of their unique link [17].

Hence, information theoretic security (ITS) under the umbrella of PLS has emerged as an effective technique to achieve information confidentiality. ITS exploits randomness and reciprocity of wireless channels for secret key generation (SKG) [18]–[20]. In ITS, SKG is achieved directly from wireless channels, and therefore this approach is more promising for securing D2D communications. The randomness of a wireless channel is shared between two communicating devices according to the channel reciprocity, which is inaccessible to and thus indeterminable to the unauthorized users [21]. Hence, the randomness induced by unpredictable wireless channels can be used as the random source for generating secret keys. Mobile devices engaging in D2D communication can extract a secret key from the common channel randomness. The secret key can be generated on demand and modified continuously. However, the rate at which secret keys are generated from the wireless channel depends to a great extent on how fast the channel changes. In a static wireless environment, the channel remains the same and its randomness is very low. Thus, how to induce more channel randomness to enhance key generation rate becomes the principal problem. An effective solution for this problem is to explore some relay nodes in the vicinity of the target nodes. These relay nodes provide the additional randomness in the channel to ensure SKG between the target D2D nodes.

The exponential growth in global mobile data traffic to a large extent can be traced to the following phenomenon that people are increasingly involving in online social interactions. Various social networks, like Facebook, Twitter, WeChat and etc., have grown phenomenally. Cooperative D2D communication is a proficient technique in the social networking [22]. By leveraging the social features, social-aware D2D communication can significantly enhancing achievable performance [23]. In particular, social ties, which characterize the strengths of relationships among mobile users, define two basic social interacting environments, called social trust and social reciprocity [24]. Social trust is established among mobile users having strong social-ties such as kinship, colleague-ship and friendship, etc. In a social-trust environment, mobile devices are likely to cooperate fully, and a user can ask other trustworthy users to serve as relays in order to improve its SKG rate (SKGR). In the absence of social trust, a group of individuals can exchange mutually beneficial activities. This is called social reciprocity, which is another widely observed social phenomenon. In a social-reciprocity environment, cooperation among users has to be based on mutual benefits, e.g., mobile devices can provide relay assistance to each other in order to improve their SKGRs. It can be seen that social ties play a vital role in representing social trust or non-trust D2D communication scenarios [25]. In the real world, a social community typically involves users with mixed social interactions, i.e., with strong and weak social ties, which represents a partially social trust environment. Therefore, we can enhance secure D2D communications by exploiting diverse properties of social ties.

A. Related Work

Recently, social-aware D2D communication approach has gained much attention [22], [23], [26]–[35]. Most of the researches focus on how to utilize the social features of D2D users to improve the overall D2D transmission rate and resource utilization. For example, Chen *et al.* [22] presented a relay selection scheme based on social trust and social reciprocity to improve the system throughput in D2D communication. Specifically, they proposed a coalition game theoretical approach to determine the effective D2D cooperation strategy and devised a network assisted relay selection technique. Li *et al.* [23] summarized the influence of social features on D2D communications, and quantitatively analyzed the achievable gains in a social-aware D2D communication system. The work [26] studied a reward-based Markov decision process to enable secondary users to cooperatively access the primary users' spectrum resource in cognitive radio networks. The study [27] described an imitation-based spectrum access mechanism for implementing efficient spectrum access. Cao *et al.* [28] proposed a cooperative video multi-cast scheme, called SoCast, to stimulate cooperation among mobile users by leveraging their social ties. Zhang *et al.* [29] proposed a social-aware algorithm for efficient multi-file dissemination in multi-hop D2D communication networks. In particular, the authors discussed the utilization of social network properties to serve ad-hoc peer discovery. Sun *et al.* [30] used a Bayesian approach to model the social ties for D2D mobile users and to accomplish effective data transmission among D2D users.

Furthermore, the work [36] described a PLS based SKG scheme by exploiting the reciprocity of signal envelopes. Chen *et al.* [31] proposed an allocation mechanism to improve the SKGR for two-relays based cooperative MIMO architectures. Gopinath *et al.* [32] analyzed various pre-processing techniques for PLS based key generation. The results of [32] showed that utilizing reciprocal properties of physical channel enhances the probability of agreement between the generated keys while de-correlation can mitigate key redundancy. Sadeghi *et al.* [33] investigated the impact of in-band full-duplex wireless communications on SKG. The authors proposed a scheme to improve the SKGR over multi-path

fading channels. However, these schemes do not explicitly exploit the social features for secure D2D communications. Thai *et al.* [34] presented a PLS based SKG scheme for multi-antenna authorized nodes with the help of non-trusted relays. Sun *et al.* [35] proposed a cooperative PLS based key generation method to establish the shared secret keys between D2D users. The D2D users choose some close neighbors as relays nodes to extract the secret key directly from the wireless channels among them. However, the authors did not consider trusted or non-trusted behaviors in selecting relays, and considered only the social reciprocity phenomenon [35].

It can be seen that most of the existing works did not consider how to utilize social properties to enhance secure D2D communications, and only a very few studies exploited the social reciprocity property for PLS based SKG. No work to date however has explicitly considered all the three scenarios of social ties (social trust, social reciprocity and partial trust) for cooperative relaying based secure D2D communication.

B. Our Contributions

Against the above background, in this paper, we formulate the social-aware D2D secure communication system in both physical and social domains to improve the SKGR. The SKGR is utilized to secure the system from non-trusted relay and eavesdropper. Specifically, we explicitly employ social ties' properties to formulate our cooperative two-relay selection problem for all the three scenarios of social ties. Our main contributions are summarized as follows.

- We frame the cooperative relays based scheme that plays significant role in helping SKG for D2D network. On the basis of ITS, we show that the proposed scheme is optimal for D2D communications with two relays scheme.
- We leverage social ties to encourage efficient cooperation among devices for secure cooperative D2D communication. We depict all three social scenarios of social trust, social reciprocity and partially trusted. The trusted behavior among D2D nodes not only secures the communication from eavesdropper but also from non-trusted relay nodes. Hence, in this paper we consider trusted and non-trusted as well as partially trusted behaviors of relay nodes.
- We formulate the problem of relay pairs selection based on social ties as a coalition game theory. Moreover, we design an algorithm by utilizing the coalition game theory to select an optimal relay pairs based on social ties, and prove the stability and convergence of the algorithm.
- We evaluate the influence of different social environments on the optimal relay pairs selection. We show that the SKGR based on social ties achieves the optimal result by enhancing the average user key generation rate approximately from 10% to 70%, as compared to direct key generation rate. We also confirm that different social phenomena have different optimal average user key generation rates.

The rest of the paper is organized as follows. In Section II, after presenting the system overview and the system model, we formulate our relay nodes selection problem in both physical and social domains. Section III is devoted to the coalition game formulation to our relay pair selection problem, and presents the algorithm for finding the optimal solution. Stability and convergence properties of our coalition formation algorithm are analyzed in Section IV. Section V presents the performance evaluation of our proposed scheme. The paper is concluded in Section VI.

II. System Overview, Model and Problem Formulation

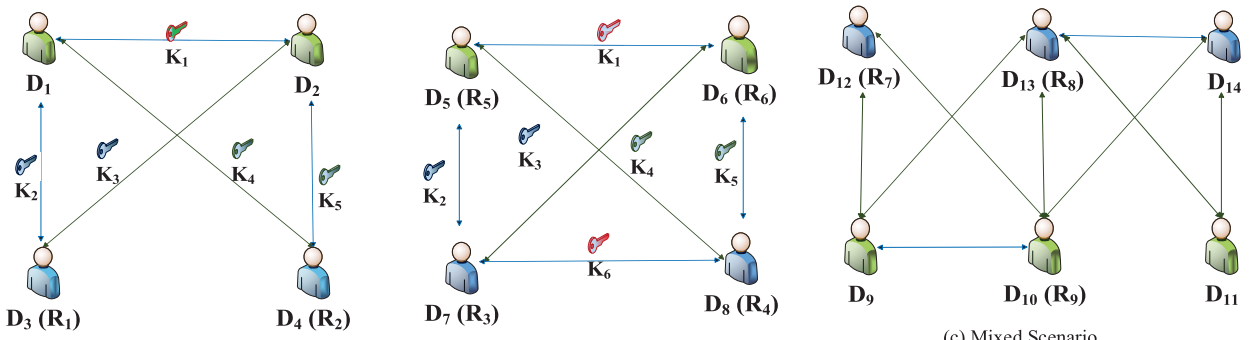
In this section, we first present the system overview for D2D cooperative SKGR with the help of multiple relays based on social ties. Then, we derive the system equations for channel estimation and achievable SKGR. Finally, we formulate the secure key agreement based on social ties.

A. System Overview

The physical layer based key generation method exploits the basic channel reciprocity concept for SKG [14]. We consider that the key generated by the PLS approach can be made uniformly distributed, and thus can be used for encryption using one time pad scheme. The two major properties of the secret keys generated by exploiting the dynamic channel variations greatly alleviate the main difficulty of implementing one-time pad encryption. **1)** The secret keys are already shared by two legitimate terminals via the generation process, which overcomes the usual challenge of key distribution in using the one-time pad encryption. **2)** These keys are replenished dynamically as wireless channels vary over time. In this way, the key rate can be improved via relay-assisted schemes which greatly improve the SKGR via the one-time pad encryption. Therefore, the PLS based approach not only produces information theoretically secure keys but also facilitates information theoretically secure encryption.

It is assumed that the D2D users send information using the public channels to their corresponding receiving users. The eavesdropper has the full access to the public channels and therefore can listen to the transmission of the D2D pairs. However, the eavesdropper is 'passive' in the SKG process between the legitimate users. The signals arriving at different wireless receivers experience different transmission paths, and hence have different random phases. The channels' gains between legitimate D2D users are also different from those between legitimate users and eavesdroppers. Therefore, even though it may know that a key agreement process is going on, an eavesdropper has no means to learn any information about the generated key. Moreover, the involvements of relay nodes in the vicinity of the D2D pairs further provide additional randomness. We consider an ergodic block fading model in which the channel gains remain unchanged for the duration of a block of T symbols, and they change randomly at the beginning of the next block. The results can be easily extended to other fading models. It is assume in this work that none of the terminals knows the values of the fading gains initially.

We also consider social-aware cooperative relays for SKG by combining the properties of physical and social domains [22]. Basically, the relay nodes are incorporated in the D2D network to increase the SKGR. These relay nodes



(a) Social Trust Scenario (Nodes D_3 & D_4 act as relay R_1 & R_2 respectively for D2D nodes D_1 & D_2)

(b) Social Reciprocity Scenario (Nodes D_7 & D_8 act as relay R_3 & R_4 respectively for D2D nodes D_5 & D_6. Reciprocally, Nodes D_5 & D_6 also act as relay R_5 & R_6 for D2D nodes D_7 & D_8).

(c) Mixed Scenario (Node D_{12} act as relay R_7 for D2D nodes D_9 & D_{10} based on social-trust, While Node D_{13} act as relay R_8 for nodes D_9 & D_{10} based on social reciprocity, as D_{10} also act as relay R_9 for node D_{13}).

Fig. 1. Key generation scenarios with and without relay node. (a) Social trust scenario. (b) Social reciprocity. (c) Mixed scenario.

are other mobile nodes that provide additional randomness to D2D pairs for generating secret keys, and they are considered based on social ties. In this regard, we have three scenarios, namely, social trust, social reciprocity, and mixed social ties (social trust and social reciprocity). Social trust scenario describes a social environment where all the available nodes are sufficiently trusted by D2D pairs and they can be selected as relays, because of strong social ties. Social reciprocity based scenario characterizes as a social environment where none of the available nodes are trusted by D2D pairs to be selected as relay nodes based on social tier information along. A partially trusted environment on the other hand comprises of social trust and social non-trusted (i.e., social reciprocity) nodes.

B. System Model and Problem Formulation

As shown in Fig. 1, we consider the D2D pair consisting of d_i, $i = 1, 2$, i.e., D2D nodes D_1 and D_2, and the relay pair containing r_j, $j = 1, 2$, i.e., relay nodes R_1 and R_2. The SKG process between D2D pair and relay pair consists of three steps, channel estimation, keys generation and key agreement. In the channel estimation phase, d_i, i = 1,2, estimates the channels with the help of the selected relay pair r_j, j = 1,2. Specifically, in the first time slot, D2D node d_{i_1} transmits a training signal $s_{d_{i_1}}$ over the wireless channels, and the signals received at D2D node d_{i_2} and relay nodes r_j, j = 1,2, are given respectively as

$$y_{d_{i_2}} = g_{d_{i_1,i_2}} s_{d_{i_1}} + n_{d_{i_2}}, \quad i_1, i_2 = 1, 2, \ i_2 \neq i_i, \tag{1}$$

$$y_{r_j} = g_{d_{i_1},r_j} s_{d_{i_1}} + n_{r_j}, \quad i_1, j = 1, 2, \tag{2}$$

where $g_{d_{i_1,i_2}}$ and $g_{d_{i_1},r_j}$ are the channel gains for the links from d_{i_1} to d_{i_2} and the links from d_{i_1} to r_j, respectively, while $n_{d_{i_2}}$ and n_{r_j} are the corresponding links' additive white Gaussian noises (AWGNs), all having variance σ_n^2. In the second time slot, relay nodes r_j transmit the training signals s_{r_j}, and the signals received by d_i are given by

$$y_{d_i} = g_{r_j,d_i} s_{r_j} + n_{d_i}, \quad r_j, \ d_i = 1, 2, \tag{3}$$

where g_{r_j,d_i} are the channel gains for the links from r_j to d_i, and n_{d_i} are the links' AWGNs with variance σ_n^2. Note that for the notational simplification, we have omitted the time slot index in (1) to (3). We further assume that the wireless network adopts the time division duplexing (TDD) protocol, and therefore, the channel reciprocal property holds. Consequently, we have $g_{d_{1,2}} = g_{d_{2,1}} = g_d$, and $g_{d_i,r_j} = g_{r_j,d_i} = g_{i,j}$, i, j = 1,2. Both g_d and $g_{i,j}$ follow the normal distributions with zero mean and variances σ_d^2 and σ_r^2, respectively, that is, $g_d \sim \mathcal{N}\left(0, \sigma_d^2\right)$ and $g_{i,j} \sim \mathcal{N}\left(0, \sigma_r^2\right)$.

In this physical layer based key generation process, an eavesdropper is passive [32], [33], [36], [37], specifically, it is not a legitimate participant of the channel estimation process. True, an eavesdropper may be able to receive the transmitted signals $s_{d_{i_1}}$ and s_{r_j}. However, if the eavesdropper is more than one-half wavelength away from the targeted nodes that are trying to establish a secret key, the channels between the D2D nodes as well as the channels between the D2D nodes and the relay nodes are uncorrelated with the channels between the eavesdropper and these targeted nodes [35]. For example, in the case of wireless transmissions in the 2.4 GHz band, we only require the eavesdropper to be more than 6.25 cm away from the target nodes for these different channels to be uncorrelated. Thus, even if the eavesdropper were able to estimate the channel gains between itself and the target nodes, it could not predict the channel gains between the targeted nodes. In other words, the channel responses between the targeted devices are unavailable and also unpredictable to any eavesdropper more than one-half wavelength away from the targeted nodes. Moreover, the eavesdropper may not be able to estimate the channels between itself and the legate nodes at all, since it is not synchronized with the D2D and relay nodes, and thus its received signals are noise like.

Based on their received training signals, the D2D and relay nodes d_i and r_j can estimate the channel gains g_d and $g_{i,j}$, respectively. More specifically, at the first time slot, let the training symbol transmitted by D2D node d_{i_1} be denoted as $X_{d_{i_1}}$. The estimated channel gain at D2D node d_{i_2}, $i_2 \neq i_1$, can be expressed as

$$h_{1,d_{i_2}} = g_d + \frac{X_{d_{i_1}}^*}{\left\|X_{d_{i_1}}\right\|^2} n_{d_{i_1}} \sim \mathcal{N}\left(0, \sigma_d^2 + \frac{\sigma_n^2}{\left\|X_{d_{i_1}}\right\|^2}\right), \tag{4}$$

where $X^*_{d_{i_1}}$ is the conjugate of $X_{d_{i_1}}$. Similarly, the estimated channel gains at relay nodes r_j are given by

$$h_{1,d_{i_1},r_j} = g_{i_1,j} + \frac{X^*_{d_{i_1}}}{\left\|X_{d_{i_1}}\right\|^2} n_{r_j} \sim \mathcal{N}\left(0, \sigma_r^2 + \frac{\sigma_n^2}{\left\|X_{d_{i_1}}\right\|^2}\right). \tag{5}$$

At the second time slot, let the training symbol transmitted by relay node r_j be denoted as X_{r_j}. The estimated channel gains at D2D nodes d_i can be expressed as

$$h_{2,r_j,d_i} = g_{j,i} + \frac{X^*_{r_j}}{\left\|X_{r_j}\right\|^2} n_{d_i} \sim \mathcal{N}\left(0, \sigma_r^2 + \frac{\sigma_n^2}{\left\|X_{r_j}\right\|^2}\right). \tag{6}$$

According to [38], the optimal key generation rate between D2D pair without the involvement of relay nodes is defined as the mutual information (MI) $I\big(h_{1,d_1}; h_{1,d_2}\big)$ scaled by the channel coherence time T_c

$$\Re_{KG}^{direct} = \frac{1}{T_c} I\big(h_{1,d_1}; h_{1,d_2}\big). \tag{7}$$

Let the transmitted signal power be denoted as p. Since the channel coherence time is T_c, the optimal training session for D2D node D_i is $\frac{T_c}{2}$, where $i = 1, 2$. With this optimal training session length $\frac{T_c}{2}$, the training symbol energy is $\|X_{d_i}\|^2 = p\frac{T_c}{2}$. As detailed in Appendix A, $\Re_{KG}^{direct}$ can be expressed as

$$\Re_{KG}^{direct} = \frac{1}{T_c} \log_2\left(1 + \frac{\sigma_d^4 p^2 T_c^2}{4\big(\sigma_n^4 + \sigma_n^2 \sigma_d^2 p T_c\big)}\right). \tag{8}$$

Observe from (8) that $\Re_{KG}^{direct}$ is approximately proportional to $\frac{1}{T_c}$. Therefore, if the channel coherent time T_c is large, i.e., the channel variations are low, the achievable SKGR is low. Observe also from (8) that the achievable SKGR increases with the training signal energy $p\frac{T_c}{2}$. By introducing the relay nodes [39] in the vicinity of the legitimate D2D pair, d_1 and d_2, the training signal power can be increases and, consequently, the achievable SKGR is improved. With the involvement of the relay nodes r_1 and r_2, the achievable SKGR is given by

$$\Re_{KG}^{relay} = \frac{1}{T_c}\left(I\big(h_{1,d_1}; h_{1,d_2}\big) + \sum_{i=1}^{2}\sum_{j=1}^{2} I\big(h_{1,d_i,r_j}; h_{2,r_j,d_i}\big)\right). \tag{9}$$

For given i, where i = 1,2, the optimal training session for D2D node D_i should last $\frac{T_c}{4}$, while the corresponding optimal training session for R_j, j = 1,2, should also last $\frac{T_c}{4}$. Further assume that the powers of all the training signals are p. Therefore, similar to the derivation of (8), $\Re_{KG}^{relay}$ can be expressed as given in (10), as shown at the bottom of this page.

C. Key Agreement Based on Social Ties

After the generation of keys among D2D pair and relay pair, the nodes involved need to make a key agreement. As mentioned previously, we consider the key agreement between D2D pair and relay pair in the three different scenarios.

1) Key agreement based on social trust (trusted environment).
2) Key agreement based on social reciprocity (non-trusted environment).
3) Key agreement based on social trust and reciprocity (mixed trusted and non-trusted environment).

1) Key Agreement Based on Social Trust: In this environment, all the nodes involved socially trust each other. Hence, the D2D users will keep the keys secret only from eavesdropper. It is obvious that in this social trust environment, not only the selection of relay nodes for SKG becomes effective for securing the communication system but also there is less chance of collusion among the selected relay nodes with the eavesdropper and others. The key generation in the social trust phenomenon is illustrated in Fig. 1 (a). Afterwards, D2D pair D_1 and D_2 agree on a key K_1 between their corresponding correlated observations. Similarly, D_1 and relay R_1 agree on a key K_2, while D_2 and R_1 agree on a key K_3. Likewise, D_1 and R_2 agree a key K_4, while D_2 and R_2 agreed on a key K_5, form their respective correlated observations as shown in Fig. 1. Then, relay pair R_1 and R_2 broadcast $K_2 \oplus K_3$ and $K_4 \oplus K_5$, respectively. Subsequently, D2D pair D_1 and D_2 have the following secret keys by concatenating $(K_1, K_2, K_3, K_4, K_5)$. However, these are not the final keys as K_2 & K_3 and K_4 & K_5 cannot simultaneously serve in the final set of keys. This is because the eavesdropper can learn K_2 & K_3 and K_4 & K_5 when they are broadcasted over the public channel. Therefore, D2D pair considers the following set of keys: either the set of $\lambda_1 = (K_1, K_2, K_4)$, if the size of K_2 and K_4 are smaller than the size of K_3 and K_5; otherwise the set of $\lambda_2 = (K_1, K_3, K_5)$ is adopted. With either set of the keys, λ_1 or λ_2, any eavesdropper can at best get insufficient information of these keys. This is because an eavesdropper experiences an independent wireless channel from that of the authorized D2D pair [38], [40]. Consequently, the key set is secure from any eavesdropper.

2) Key Agreement Based on Social Reciprocity: In this environment, D2D users do not trust the selected relay nodes socially. Hence, although the non-trusted relay nodes help the D2D pair to generate the more random keys, the D2D users are not sure these relay nodes will not collude with eavesdropper or others. Therefore, the D2D pair must keep the secret keys secure from both the eavesdropper and the selected relay nodes. In order to keep the keys secret even from both eavesdropper and the selected relay nodes, the D2D pair D_1 and D_2 implement the XOR operation on the following key

$$\Re_{KG}^{relay} = \frac{1}{T_c} \log_2\left(\left(1 + \frac{\sigma_d^4 p^2 T_c^2}{8\big(2\sigma_n^4 + \sigma_n^2 \sigma_d^2 p T_c\big)}\right) \prod_{i=1}^{2}\prod_{j=1}^{2}\left(1 + \frac{\sigma_r^4 p^2 T_c^2}{8\big(\sigma_n^4 + \sigma_n^2 \sigma_r^2 p T_c\big)}\right)\right) \tag{10}$$

sets, (K_2, K_4) and (K_3, K_5), and they agree on the secret key set, $\lambda_3 = (K_1, K_2 \oplus K_4)$ or $\lambda_4 = (K_1, K_3 \oplus K_5)$, by concatenating. It is readily seen that the key set agreed by the D2D pair, λ_3 or λ_4, satisfies the requirement of secrecy conditions given in [38] and [40]. Consequently, each relay node and eavesdropper can only achieve insufficient information about the key set agreed by the D2D pair. In other words, this key set is secured from the both relay nodes[1]. In fact, the proof is straightforward. Assume that λ_3 is agreed by the D2D pair. Note that relay R_1 has K_2 and it can also acquire $K_4 \oplus K_5$ when it was broadcasted. However, as proved in Appendix B,

$$I\big((K_2, K_4 \oplus K_5); K_2 \oplus K_4\big) = 0. \tag{11}$$

Therefore, relay R_1 is unable to generate $K_2 \oplus K_4$ from $K2$ and $K_4 \oplus K_5$, that is, $(K_1, K_2 \oplus K_4)$ is secured from relay R_1. Similarly, λ_3 is secured from relay R_2.

3) Key Agreement Based on Social Trust and Reciprocity: Assume that the D2D pair can only find a social trust node as a relay node. Then they have to select a non-trusted node as another relay node on the social reciprocity basis. In order to secure the keys from eavesdropper and the selected non-trusted relay node, the D2D pair can implement the same key agreement for the socially non-trusted case. That is, the D2D pair, D_1 and D_2, implement the XOR operation on (K_2, K_4) and (K_3, K_5), and they establish the final key set as $\lambda_3 = (K_1, K_2 \oplus K_4)$ or $\lambda_4 = (K_1, K_3 \oplus K_5)$.

D. Relay Selection Based on Social Tiers

As mentioned previously, a contribution of this work is to conceive the relay pair selection based on social tiers to secure D2D communications. In this regard, we can view the D2D aided communication system from both physical and social domains, as illustrated in Fig. 2. In physical domain, mobile devices assist each other with D2D transmissions subject to the physical constraints, while in social domain, mobile devices form a social network regulated by social relationships, such as social tiers [23].

1) Physical Domain: We construct the physical communication graph for key generation among D2D devices in physical domain. Specifically, we label the D2D users by the set $\mathcal{N} = \{1, 2, \ldots, N\}$, and we label the set of nodes that can potentially serve as relays for the nodes of $\mathcal{N}$ by $\mathcal{M} = \{1, 2, \ldots, M\}$. In order to take the physical constraints into account, we construct a graph model denoted by $G_p = (V_p, E_p)$. In this physical graph, V_p is the vertex set that denotes the D2D pairs $d_{i_1,i_2}, \forall i_1, i_2 \in \mathcal{N}$ and $i_1 \neq i_2$, as well as the potential relay node pairs $r_{j_1,j_2}, \forall j_1, j_2 \in \mathcal{M}$ and $j_1 \neq j_2$, while E_p is the edge set that represents the physical links between the D2D pairs and the potential relay pairs. The entries of E_p are denoted by $\alpha^p_{d_{i_1,i_2},r_{j_1,j_2}}, \forall d_{i_1,i_2}, r_{j_1,j_2} \in V_p$. Specifically, $\alpha^p_{d_{i_1,i_2},r_{j_1,j_2}} = 1$ indicates that there exist the physical links or connections between the two D2D nodes of d_{i_1,i_2} and the two potential relay nodes of r_{j_1,j_2}, while $\alpha^p_{d_{i_1,i_2},r_{j_1,j_2}} = 0$ indicates that no such physical link exists. Therefore, the set of feasible relay pairs for D2D pair d_{i_1,i_2} is specified by $\mathcal{R}_p\big(d_{i_1,i_2}\big) = \Big\{\forall r_{j_1,j_2} \in V_p : \alpha^p_{d_{i_1,i_2},r_{j_1,j_2}} = 1\Big\}$. Clearly, if $\mathcal{R}_p\big(d_{i_1,i_2}\big)$ is empty, the D2D pair d_{i_1,i_2} have to generate keys directly without the assistance of any relay pair, and its achievable SKGR is given in (8). By contrast, if $\mathcal{R}_p\big(d_{i_1,i_2}\big)$ is not empty, d_{i_1,i_2} will be able to select a relay pair from $\mathcal{R}_p\big(d_{i_1,i_2}\big)$ to assist the key generation, and its achievable SKGR in this case is given in (4). Thus, with the physical constraints, the achievable SKGR for D2D pair d_{i_1,i_2} is summarized as given in (12), as shown at the bottom of this page.

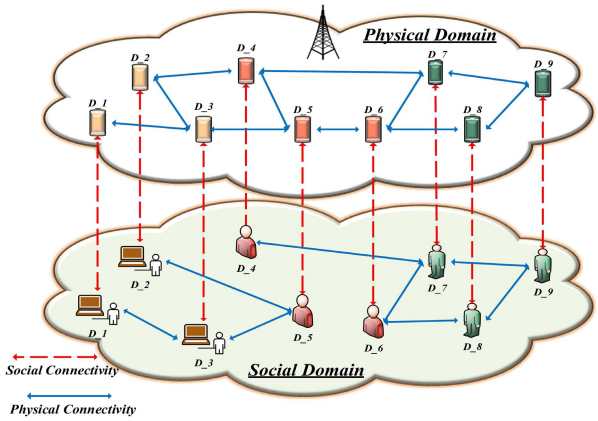


Fig. 2. D2D assisted communication system as seen from physical and social domains.

2) Social Domain: We introduce the social link graph $G_s = (V_s, E_s)$ to model the social relationships among the D2D pairs and the potential relay node pairs. In this social graph, the vertex set V_s contains all the D2D pairs and the potential relay node pairs, similar to V_p, while the edge set E_s represents the social links or connections between the D2D pairs and the potential relay node pairs, according to a specific social relationship metric.

a) Social trust: In this senario, the social trust is chosen to be the social relationship metric. The entries of E_s

[1]The secure key set, λ_3 or λ_4, agreed by the D2D pair is referred to as the private key and is shown to be secure from the relay nodes in [40].

$$\Re_{KG}\big(d_{i_1,i_2}\big) = \begin{cases} \Re_{KG}\big(d_{i_1,i_2}|\text{no relay}\big) = \Re^{direct}_{KG}\ (8), & \mathcal{R}_p\big(d_{i_1,i_2}\big)\ \text{empty}, \\ \Re_{KG}\big(d_{i_1,i_2}|r_{1,2}\big) = \Re^{relay}_{KG}\ (4), & r_{1,2} \in \mathcal{R}_p\big(d_{i_1,i_2}\big)\ \text{selected} \end{cases} \tag{12}$$

$$\mathcal{R}_{p\cap s}\big(d_{i_1,i_2}\big) = \begin{cases} \Big\{\forall r_{j_1,j_2} \in V_{p\cap s} : \alpha^p_{d_{i_1,i_2},r_{j_1,j_2}} \cdot \beta^s_{d_{i_1,i_2},r_{j_1,j_2}} = 1\Big\}, & \text{Trust}, \\ \Big\{\forall r_{j_1,j_2} \in V_{p\cap s} : \alpha^p_{d_{i_1,i_2},r_{j_1,j_2}} \cdot \gamma^s_{d_{i_1,i_2},r_{j_1,j_2}} = 1\Big\}, & \text{Reciprocity}, \\ \Big\{\forall r_{j_1,j_2} \in V_{p\cap s} : \alpha^p_{d_{i_1,i_2},r_{j_1,j_2}} \cdot \theta^s_{d_{i_1,i_2},r_{j_1,j_2}} = 1\Big\}, & \text{Mixed} \end{cases} \tag{13}$$

are denoted by $\beta^s_{d_{i_1,i_2},r_{j_1,j_2}}$, $\forall d_{i_1,i_2}, r_{j_1,j_2} \in V_s$, where $\beta^s_{d_{i_1,i_2},r_{j_1,j_2}} = 1$ indicates that there exist the social-trust connections between the two D2D nodes of d_{i_1,i_2} and the two potential relay nodes of r_{j_1,j_2}, while $\beta^s_{d_{i_1,i_2},r_{j_1,j_2}} = 0$ means that no such social-trust connection exists.

b) Social reciprocity: In this senario, none of the potential relay pairs is socially trusted by the D2D pairs. Cooperation among users has to be based on mutual benefits, and hence the social reciprocity is chosen to be the social relationship metric. In this case, we denote the entries of E_s by $\gamma^s_{d_{i_1,i_2},r_{j_1,j_2}}$, $\forall d_{i_1,i_2}, r_{j_1,j_2} \in V_s$, where $\gamma^s_{d_{i_1,i_2},r_{j_1,j_2}} = 1$ indicates that there exist the social-reciprocity connections between the two D2D nodes of d_{i_1,i_2} and the two potential relay nodes of r_{j_1,j_2}, while $\gamma^s_{d_{i_1,i_2},r_{j_1,j_2}} = 0$ means that no such social-reciprocity connection exists.

c) Mixed social trust and social reciprocity: In this senario, we denote the entries of E_s by $\theta^s_{d_{i_1,i_2},r_{j_1,j_2}}$, $\forall d_{i_1,i_2}, r_{j_1,j_2} \in V_s$, where $\theta^s_{d_{i_1,i_2},r_{j_1,j_2}} = 1$ indicates that one node of r_{j_1,j_2} has the social-trust connections with the two D2D nodes of d_{i_1,i_2} as well as the other node of r_{j_1,j_2} has the social-reciprocity connections with the two D2D nodes of d_{i_1,i_2}, while $\theta^s_{d_{i_1,i_2},r_{j_1,j_2}} = 0$ means that no such social connection exists.

3) Relay Pair Selection: In relay pair selection, the physical constraints, namely, the physical graph, must be taken into consideration. Moreover, we can incorporate the social 'constraints', namely, the social graph, to achieve better relay pair selection. To this end, we can define the combined graph of $G_{p\cap s} = \left(V_{p\cap s}, E_{p\cap s}\right) = \left(V_p \bigcap V_s, E_p \bigcap E_s\right)$. The set of feasible relay pairs for D2D pair $d_{i_1,i_2} \in V_{p\cap s}$ can then be specified by (13), as shown at the bottom of the previous page.

The optimal social-aware relay pair selection for the D2D pair d_{i_1,i_2} can be formulated as the following optimization problem

$$r^{\star}_{j_1,j_2} = \arg \max_{\forall r_{j_1,j_2} \in \mathcal{R}_{p\cap s}\left(d_{i_1,i_2}\right)} \Re_{KG}\left(d_{i_1,i_2} | r_{j_1,j_2}\right). \quad (14)$$

Direct solving this challenging optimization problem for all the D2D pairs is intractable. Not least, different D2D pairs may have conflict-of-interest of wanting the same relay pair in order to maximize their individual achievable SKGRs. In the next section, we develop a coalition game framework to address the selection of the optimal relay pairs for all the D2D pairs efficiently.

III. Coalition Game Framework

A. Introduction to Game Formulation

Coalition game [41] is utilized to find the social-aware optimal relay pairs for D2D secure communications. For notational convenience, we denote the set of D2D pairs by $\mathcal{D} = \left\{\bar{d}_i, 1 \le i \le N_{pa}\right\}$ and the set of potential relay pairs by $\mathcal{R} = \left\{\bar{r}_i, 1 \le i \le M_{pa}\right\}$. In this coalition game, the players are D2D pairs who seek coalition with relay pairs that can offer them higher SKGRs. Specifically, The formulation of coalition game is outlined by the quartet $\mathcal{G} = \left(\mathcal{D}, \mathcal{R}, \mathcal{X}_{\mathcal{N}}, \mathcal{V}\right)$, in which

- Players: In our proposed game, the D2D pairs are the game players, who seek coalition with the potential relay pairs.
- Cooperation Strategy: $\mathcal{X}_{\mathcal{N}}$ represents the space of feasible cooperation strategies among all players in the coalition with all potential relay pairs.
- Characteristic Function: In our proposed game, game players use the characteristic function $\mathcal{V}$ to map every nonempty subset $\mathcal{U} \subseteq \mathcal{R}$ onto a subset of feasible cooperation strategies $\mathcal{V}(\mathcal{U}) \subseteq \mathcal{X}_{\mathcal{N}}$.
- Coalition Partition: The players set a coalition partition $\mathcal{U} = \left\{\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_{N_{pa}}\right\}$, where $\forall i$, $\mathcal{V}(\mathcal{U}_i) \subseteq \mathcal{X}_{\mathcal{N}}$, while $\mathcal{U}_i \bigcap \mathcal{U}_{i'} = \emptyset$, for $i \neq i'$, and $\bigcup_{i=1}^{N_{pa}} \mathcal{U}_i = \mathcal{R}$. This represents the best cooperation strategy among the players in coalition with $\mathcal{R}$.

The procedure in coalition partition formulation is to enable the players in the formation to seek coalition based on the well-defined preference order. Specifically, each player should be able to compare and order its potential coalitions based on which to choose its preferred coalition members. Hence, we need to define the conception of preference order [41].

Definition 1: For any D2D pair $\bar{d}_i \in \mathcal{D}$, the preference order $\succ_{\bar{d}_i}$ is defined as the reflexive, complete and transitive binary relation over the set of whole possible relay pairs $\bar{r}_j \in \mathcal{R}$ so that the D2D pair $\bar{d}_i$ can form the cooperative coalition $\mathcal{U}_i \subseteq \mathcal{R}$, which satisfies

$$\mathcal{U}_i \bigcap \mathcal{U}_{i'} = \emptyset, \forall i \neq i', \text{ and } \bigcup_{i=1}^{N_{pa}} \mathcal{U}_i = \mathcal{R}. \quad (15)$$

In our coalition partition formation, D2D pair $\bar{d}_i$ prefer the relay pair $\bar{r}_j$ over the relay pair $\bar{r}_{j'}$ if and only if selecting $\bar{r}_j$ can offer higher SKGR than $\bar{r}_{j'}$. Therefore the preference order in our proposed game is defined by

$$\bar{r}_j \succ_{\bar{d}_i} \bar{r}_{j'} \Leftrightarrow \Re_{KG}\left(\bar{d}_i | \bar{r}_j\right) > \Re_{KG}\left(\bar{d}_i | \bar{r}_{j'}\right). \quad (16)$$

B. Coalition Formation Algorithm for Selecting Optimal Relay Pairs

We are now ready to present our proposed coalition formation algorithm for selecting optimal relay pairs, which is summarized in Algorithm 1. Specifically, at Stage 1 of Algorithm 1, every D2D pair $\bar{d}_i$ forms the initial coalition $\mathcal{U}_i$ with the relay pairs by randomly selecting those relay pairs who can offer it higher SKGRs than its direct secrete rate of no relay assistance. The crucial Stage 2 of Algorithm 1 is based on coalition formation game, where D2D pairs make new coalitions with the relay pairs to enhance their SKGRs based on the preference order defined in (16). More specifically, in every iteration, a randomly selected D2D pair $\bar{d}_i$ compares a randomly picked relay pair from its current coalition, $\bar{r}_j \in \mathcal{U}_i$, with a randomly selected relay pair from a different coalition, $\bar{r}_{j'} \in \mathcal{U}_{i'}$, $i' \neq i$. If the preference order $\bar{r}_j \succ_{\bar{d}_i} \bar{r}_{j'}$ is not satisfied, the D2D pair $\bar{d}_i$ switches its coalition with $\bar{r}_j$, i.e., deselects $\bar{r}_j$ from $\mathcal{U}_i$, and forms a new coalition with $\bar{r}_{j'}$, i.e., adds $\bar{r}_{j'}$ in $\mathcal{U}_i$. This preference order based switching operation enables every D2D pair to find a preferred relay pair and to form a new preferable coalition.

Algorithm 1 Coalition formation algorithm for selecting optimal relay pairs

Initialization
Construct the physical graph and social graph to compute all $\alpha^{p}_{\bar{d}_i,\bar{r}_j}$ and $\beta^{s}_{\bar{d}_i,\bar{r}_j}/\gamma^{s}_{\bar{d}_i,\bar{r}_j}/\theta^{s}_{\bar{d}_i,\bar{r}_j}$, $\forall i,j$;
Set the iteration index $t=0$; Set $\mathcal{U}_i=\emptyset$, $\forall i$;
end initialization

Stage 1: Relay nodes selection

if Flag == 1 $\longleftarrow$ Social link
 repeat
  Set $t = t+1$.
  Randomly select D2D pair $\bar{d}_i \in \mathcal{D}$;
  Randomly select $\bar{r}_j \in \mathcal{R}$;
  Check for social trust, social reciprocity or mixed social trust and reciprocity;
  Compute $\Re_{KG}\big(\bar{d}_i|\bar{r}_j\big)$;
  if $\Re_{KG}\big(\bar{d}_i|\bar{r}_j\big) > \Re_{KG}\big(\bar{d}_i|\text{no relay}\big) \longrightarrow \mathcal{U}_i = \mathcal{U}_i \bigcup \{\bar{r}_j\}$;
   Go to step 6;
  else
   go to step 9;
  end if
 until All D2D pairs select their relay nodes;
else Flag == 0, $\forall \bar{d}_i$, compute $\Re_{KG}\big(\bar{d}_i|\text{no relay}\big)$;
end if

Stage 2: Optimal relay pairs selection

repeat
 Randomly select coalition $\mathcal{U}_i$, i.e., $\bar{d}_i$ and $\bar{r}_j \in \mathcal{U}_i$;
 Randomly select another coalition $\mathcal{U}_{i'}$, $i' \neq i$;
 Check preference order of $\bar{d}_i$ for $\bar{r}_j \in \mathcal{U}_i$ and $\bar{r}_{j'} \in \mathcal{U}_{i'}$ based on (16);
 if (16) NOT satisfies
  go to step 29;
 else
  go to step 22;
 end if
 D2D pair $\bar{d}_i$ splits from its current coalition and forms a new coalition;
 Update the current coalition;
until Convergence to the final Nash-stable partition.

After repeating switch operations based on preference order, the coalition formation game will converge to a stable and optimal coalition partition, which allows all the D2D pairs collaboratively find their optimal relay pairs, namely, cooperatively solve the optimization problem (14).

It can be observed that the switch operation in this coalition game relies on 'local' D2D pairs instead of all the D2D pairs of the system. Hence, the complexity of Algorithm 1 is lower than a centralized solution. After finite number of switching operations, the system partition will converge to the final Nash-stable partition, which is analyzed in the next section.

IV. Theoretical Analysis

We now analyze the stability and convergence rate of the proposed coalition formulation game, Algorithm 1, as well as the optimality of the solution obtained.

A. Stability and Convergence Rate

First, we have the following well-known concept of Nash-stability.

Definition 2: A coalition formation $\mathcal{U} = \{\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_{N_{pa}}\}$ *is Nash-stable if* $\forall \bar{d}_i \in \mathcal{D}$ *and* $\bigcup_{i=1}^{N_{pa}} \mathcal{U}_i = \mathcal{R}$, $\bar{r}_j \succ_{\bar{d}_i} \bar{r}_{j'}$ *hold* $\forall \bar{r}_j \in \mathcal{U}_i$ *and* $\forall \bar{r}_{j'} \in \mathcal{U} \backslash \mathcal{U}_i$.

According to Definition 2 and the concepts of hedonic games [42], it can be shown that the final coalition partition calculated by Algorithm 1 is Nash-stable.

Theorem 3: Starting from any random initial coalition partition $\mathcal{U}^{(0)}$*, the proposed coalition formulation algorithm will converge to the Nash-stable coalition partition* $\mathcal{U}^{(\mathrm{ns})}$ *in a final number of random switching operations with probability one.*

Proof: In every switching process of Algorithm 1, the new partitions are formed according to the selected relay pairs. Since the relay pairs in the set $\mathcal{R}$ are final, the number of partitions for the given set of D2D pairs $\mathcal{D}$ is a Bell number [30]. Consequently, the random switching operations will end with probability one. Thus, the algorithm converges to or stops at a final coalition partition $\mathcal{U}^{(\mathrm{ns})}$ after finite random switching operations with probability one.

Next we prove $\mathcal{U}^{(\mathrm{ns})} = \left\{\mathcal{U}_1^{(\mathrm{ns})}, \mathcal{U}_2^{(\mathrm{ns})}, \ldots, \mathcal{U}_{N_{pa}}^{(\mathrm{ns})}\right\}$ is Nash-stable by contradiction. Assume that $\mathcal{U}^{(\mathrm{ns})}$ is not Nash-stable.

Then there exists a D2D pair $\bar{d}_i \in \mathcal{D}$, $\bar{r}_j \succ_{\bar{d}_i} \bar{r}_{j'}$ does not hold for some $\bar{r}_j \in \mathcal{U}_i^{(\mathrm{ns})}$ and some $\bar{r}_{j'} \in \mathcal{U}^{(\mathrm{ns})} \backslash \mathcal{U}_i^{(\mathrm{ns})}$. Thus D2D pair $\bar{d}_i$ should and can switch coalition. This contradicts to the fact that no more switching of coalition can be found. This completes the proof. ■

B. Optimality of Solution

Theorem 4: The final coalition partition $\mathcal{U}^{(\mathrm{ns})} = \left\{\mathcal{U}_1^{(\mathrm{ns})}, \mathcal{U}_2^{(\mathrm{ns})}, \ldots, \mathcal{U}_{N_{pa}}^{(\mathrm{ns})}\right\}$ *obtained by Algorithm 1 according to coalition game* $\mathcal{G}$ *for the social link based relay pair selection scheme represent the optimal relay pairs for the set of D2D pairs* $\mathcal{D}$.

Proof: For any $\bar{d}_i \in \mathcal{D}$, its coalition set of the selected relay pairs is $\mathcal{U}_i^{(\mathrm{ns})}$. Since we have

$$\Re_{KG}\left(\bar{d}_i|\bar{r}_j\right) > \Re_{KG}\left(\bar{d}_i|\bar{r}_{j'}\right), \quad \forall \bar{r}_j \in \mathcal{U}_i^{(\mathrm{ns})}, \quad \forall \bar{r}_{j'} \in \mathcal{U}^{(\mathrm{ns})} \backslash \mathcal{U}_i^{(\mathrm{ns})}, \tag{17}$$

the selected relay pairs in the coalition $\mathcal{U}_i^{(\mathrm{ns})}$ with $\bar{d}_i$ are optimal for the D2D pair $\bar{d}_i$. Hence, through coalition game $\mathcal{G}$, all the D2D pairs have collaboratively found their optimal relay pairs, in terms of SKGRs. ■

V. Performance Evaluation

We evaluate the performance of the proposed cooperative D2D key generation method with the aid of the selected relay nodes in a simulation study. In particular, we evaluate the security enhancement gained by the social-ties based relay pair selection. In the simulation, we consider randomly scattered nodes in the square area of $1000 \times 1000\,\mathrm{m}^2$. We set $\sigma_d^2 = \sigma_r^2 = 1$ and thus all the channel gains are generated according to the normal distribution of $\mathcal{N}(0,1)$, and we further set $\sigma_n^2 = 1$ for all the AWGNs. The users' transmission power during training is set to $p = 23\,\mathrm{dBm}$, and the channel coherence time T_c spans the duration of 20 symbols. We construct the physical graph by setting $\alpha^p_{\bar{d}_i,\bar{r}_j} = 1$, if and only if the distance between the D2D pair $\bar{d}_i$ and the relay pair $\bar{r}_j$ is not greater than a threshold of 500 m. The relatively large distance threshold is set due to the fact that the detection of neighboring relay pairs can be significantly enhanced with the assistance of the base station in D2D communications [43]. The minimum and maximum distances between the node pairs are taken to be 10 m and 500 m, respectively. For the social graph model, we consider Erdős-Rényi (ER) graph model [44]. In ER graph model, a social link exists between nodes with a probability of P_{sl}. For a given value of the social link probability P_{sl}, we average the results over 1000 random runs. As the benchmark, we also compute the direct SKGRs between D2D nodes without considering relay pair. Unless otherwise stated, we use $P_{sl} = 0.5$ in most of the simulation experiments. But we also vary the value of P_{sl} to evaluate the impact of the social link density of the social graph [44] to the achievable SKGR performance.

Fig. 3 depicts the number of social links formed in the social graph as the function of the number of nodes in the network or physical graph. We assume that half of the network nodes are D2D nodes and the other half are relay nodes.

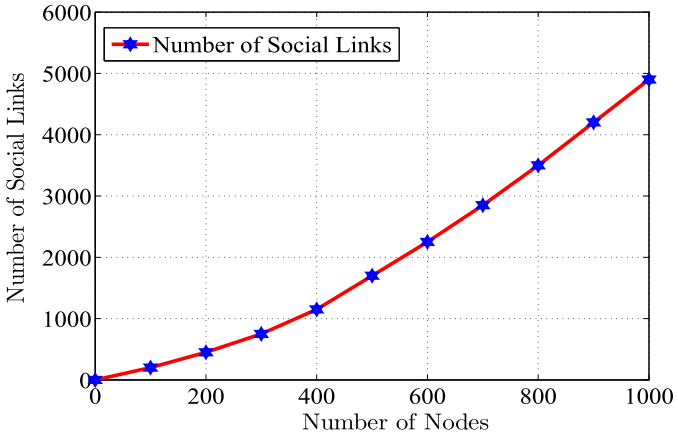


Fig. 3. Number of social links increases with the number of nodes.

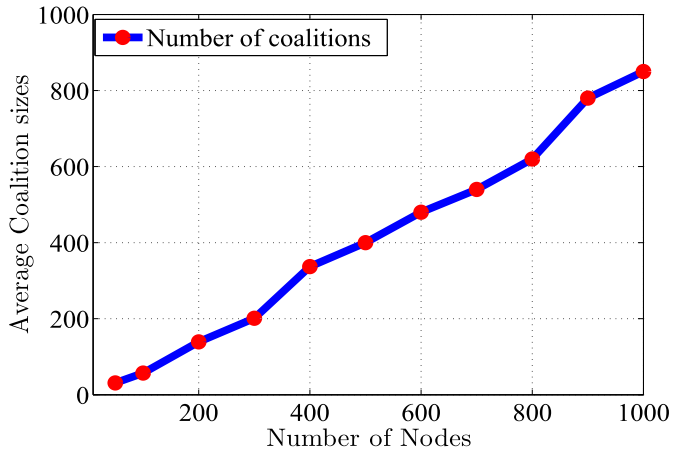


Fig. 4. Average coalition size by varying the number of nodes.

It can be seen clearly from Fig. 3 that the number of social links increases exponentially as the number of network nodes increases. Obviously, more users enable more social links to be constructed in the social graph based on the social ties relationship among these nodes. These increased social connections in turn can be utilized by D2D users to form coalition with relay nodes in order to improve their SKGRs. Therefore, Fig. 4 describes the average coalition size with respect to the number of nodes. Not surprisingly, we observe that as the number of nodes increases, the average coalition size increases. To recap, as the number of nodes increases, the number of social link increases. Consequently, the average coalition sizes increases. This means that D2D users have more opportunities to select and make coalition with their respective relay pairs to enhance their SKGRs.

In Fig. 5, we compare the average user's SKGRs for various schemes by considering the secrecy constraints for different number of relay nodes. The upper-bound average user SKGR in Fig. 5 is the maximally achievable average user SKGR under the idealized conditions of the maximum social link probability $P_{sl} = 1$ and the maximum system signal to noise ratio (SNR) with $p \to \infty$. Observe from Fig. 5 that the average user key rates of the social ties based relay pair selection schemes increase with the number of network nodes. This is

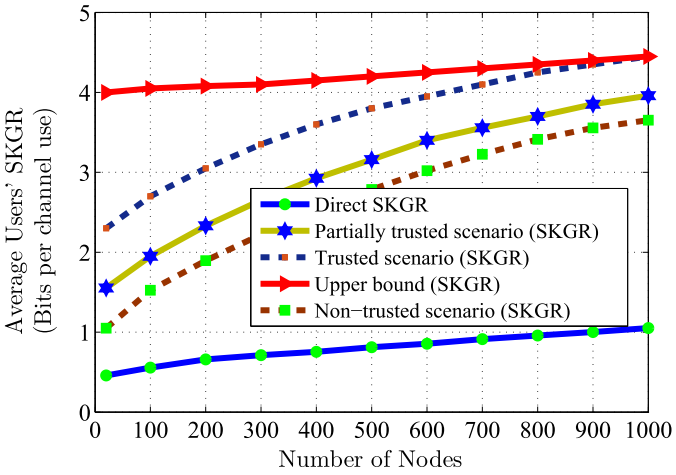


Fig. 5. Comparison of average user's SKGRs for various schemes. The network has half D2D pairs and other half relay pairs.

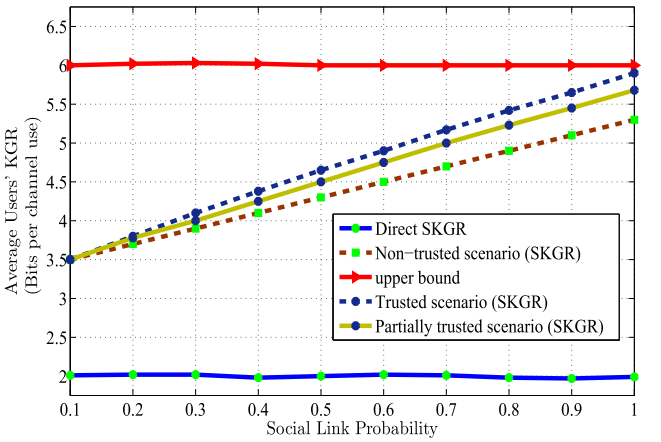


Fig. 7. Impact of social link probability P_{sl} on average user's SKGR. The network has 300 D2D nodes and 300 relay nodes.

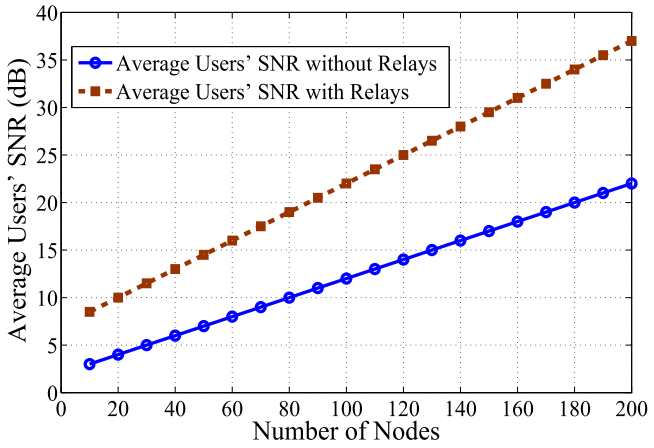


Fig. 6. Comparison of average user's SNRs with and without assistance of relay pairs.

because more cooperation opportunities among the D2D users and relay pairs are available when the number of network nodes increases.

Furthermore, all the social ties based relay selection schemes outperform the direct SKG generating scheme without the assistance of relay pairs. Even the relay assisted scheme under the socially non-trusted environment achieves a significantly higher average user SKGR than the direct SKG generating scheme. Not surprisingly, the relay assisted SKG scheme under the social trust environment attains the best performance. Specifically, its average user SKGR is 10% higher than the relay assisted scheme under the mixed social trust and non-trust environment, 16% greater than the relay pair selected scheme under the social non-trust environment, and 70% greater than the direct SKGR. Observe from Fig. 5 that the upper bound can only be approached from below under a near idealized socially trusted environment of sufficiently large number of nodes that trust each other and are willingly cooperate with each other.

Fig. 6 compares the average user's SNR achieved with the assistance of relay pairs with that achieved without the assistance of relay pairs. Note that in the case of relay assistance, the social ties of the selected relay pairs with the D2D pairs do not influence the average user's SNR. Therefore, in Fig. 6, we only have two curves, the one with assistance of relay pairs and the other without assistance of relay pairs. Observe from Fig. 6 that the average user SNR increases dramatically with the increase of network nodes in the both cases. This is because in a denser network, the average distance between communicating D2D users is shorter, which results in higher SNR. Moreover, the average user's SNR with the assistance of relay pairs is 25% to 40% higher than that without the assistance of relay pairs. Evidently, in a denser network, not only the distance between communicating D2D users is shorter but also the distance between D2D users and their relays is shorter. Consequently, the SNR gain of the relay assistance case over the case of no relay assistance is higher for denser network.

Next, we simulate a network with 300 D2D nodes and 300 relay nodes, and investigate the impact of the social link probability P_{sl} on the achievable average user's SKGR. Fig. 7 shows the average user's SKGRs as the functions of P_{sl} for various schemes. Obviously, the social link probability P_{sl} has no influence on the direct SKG scheme, while the upper-bound SKGR is obtained with P_{sl} =1. Clearly, larger P_{sl} results in more social connections in the social graph. This provides more and better opportunities for D2D users to collaborate with relay pairs, which in turn leads to better SKGR performance for all the three relay assisted scenarios, as can be seen clearly from Fig. 7. In particular, at $P_{sl} = 1$, the SKGR performance of the social trust, social reciprocity, and mixed social trust and social reciprocity based relay-pair selection schemes are 63%, 60% and 55% higher than the direct SKG scheme, respectively.

The physical constraints of the network or the connections of the physical graph clearly have significant impact on the achievable average user's SKGR. Fig. 8 depicts the influence of the distance threshold on the average user's SKGR, where the network has 200 D2D nodes and 200 relay nodes. For a large distance threshold, the physical graph contains connections with long distances These long-distance connections

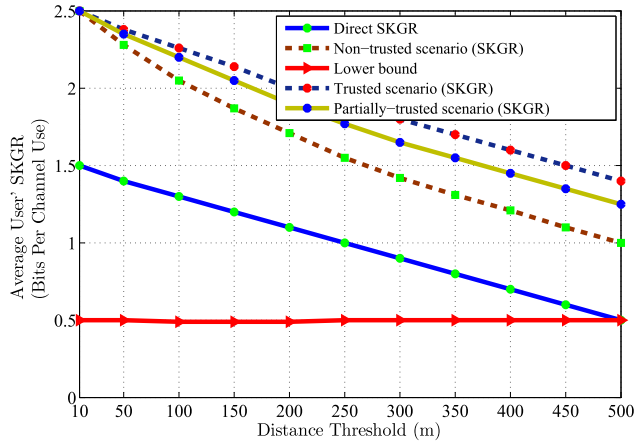


Fig. 8. Impact of distance threshold on average user's SKGR. The network has 200 D2D nodes and 200 relay nodes.

have low SNR values and therefore, the average user SKGR calculated based on these low-SNR connections will also be low. This explains the phenomenon shown in Fig. 8, where we observe that the average user SKGRs decrease as the distance threshold increases for all the four schemes. In Fig. 8, the lower-bound SKGR is obtained at the minimum SNR corresponding to the largest distance threshold of 500 m and without the cooperation of relay pairs, i.e., $P_{sl} = 0$. Again and not surprisingly, the average SKGR performance of the three relay assisted scenarios are significantly higher than the direct SKG scheme, and the social trusted senario attains the best performance.

Summary of the Results: Evidently, denser network not only provides more and better physical connections but also offers more and better social connections, both factors will contribute to higher SKGR performance. The results clearly show that the relay assisted SKGR performance under the socially trusted environment is better than those under the socially non-trusted environment and the partially trusted environment. More importantly, our study has convincingly revealed that under all the three social ties environments, the relay assisted SKGR performance are significantly higher than the direct SKGR obtained without the assistance of relays. This demonstrates the effectiveness of our proposed social-aware secret key generation approach for secure D2D communications via trusted and non-trusted relays.

VI. Conclusion

In this paper, we have investigated how to improve information confidentiality through secret key generation for D2D communications by introducing relay pairs based on social ties relationship. We have presented physical-layer security issues on both physical and social domains in order to meet physical constraints for D2D cooperation and to exploit social relationship among devices for securing D2D communications. More specifically, by leveraging social ties, we have exploited three social phenomena, namely, social trust scenario, social reciprocity and mixed social trust and social reciprocity, for secure D2D communications with the assistance of relay pairs. Moreover, we have utilized coalition game theory and have proposed an algorithm to select the optimal relay pairs for improving SKGR, while protecting the keys secret from both eavesdropper and non-trusted selected relays. Our analytical and numerical results have demonstrated that the proposed SKG generating scheme with the assistance of the relay pairs selected based on social ties relationship achieves substantially higher SKGR than the direct SKG scheme without relay assistance. In our future work, we will combine authentication of higher layer and information confidentiality via PLS technique for securing data transmission to overcome the problem of impersonation attack.

Appendix

A. Proof of Equation (8)

Proof: Since $h_{1,d_i} \sim \mathcal{N}\left(0, \sigma_d^2 + \frac{2\sigma_n^2}{pT_c}\right)$ for $i = 1, 2$, the entropies

$$H\big(h_{1,d_i}\big) = \log_2\left(2\pi e\left(\sigma_d^2 + \frac{2\sigma_n^2}{pT_c}\right)\right), \quad i = 1, 2. \tag{18}$$

On the other hand, the correlation coefficient between h_{1,d_1} and h_{1,d_2} is given by

$$E\left[\left(g_d + \frac{X_{d_2}^*}{\|X_{d_2}\|^2} n_{d_1}\right)\left(g_d + \frac{X_{d_1}^*}{\|X_{d_1}\|^2} n_{d_2}\right)\right] = E\big[g_d^2\big] = \sigma_d^2. \tag{19}$$

Therefore the covariance matrix of the joint Gaussian variables $\big[h_{1,d_1}\ h_{1,d_2}\big]^{\mathrm{T}}$ is

$$\mathbf{\Sigma} = \begin{bmatrix} \sigma_d^2 + \frac{2\sigma_n^2}{pT_c} & \sigma_d^2 \\ \sigma_d^2 & \sigma_d^2 + \frac{2\sigma_n^2}{pT_c} \end{bmatrix}, \tag{20}$$

and the entropy i.e., $H\big(h_{1,d_1}, h_{1,d_2}\big)$

$$= \log_2\Big((2\pi e)^2 \det\left(\mathbf{\Sigma}\right)\Big) = \log_2\left((2\pi e)^2 \frac{4\big(\sigma_n^4 + \sigma_d^2\sigma_n^2 pT_c\big)}{p^2 T_c^2}\right). \tag{21}$$

The MI can be computed by the entropy method [21], [45], [46] as

$$I\big(h_{1,d_1}; h_{1,d_2}\big) = H\big(h_{1,d_1}\big) + H\big(h_{1,d_2}\big) - H\big(h_{1,d_1}, h_{1,d_2}\big). \tag{22}$$

Substituting (18) and (21) into (22) leads to

$$I\big(h_{1,d_1}; h_{1,d_2}\big) = \log_2\left(1 + \frac{\sigma_d^4 p^2 T_c^2}{4\big(\sigma_n^4 + \sigma_n^2\sigma_d^2 pT_c\big)}\right). \tag{23}$$

■

B. Proof of Equation (11)

Proof: Denote $K_2 = X$, $K_4 \oplus K_5 = Y$, and $K_2 \oplus K_4 = Z$. Then we have

$$I\big((K_2, K_4 \oplus K_5); K_2 \oplus K_4\big) = I\big(X, Y; Z\big) = I(X; Z) + I(X; Y|Z), \tag{24}$$

where the last equality is according to the chain rule of MI [46]. Since X and Y are independent and, therefore, they are conditional independent given Z. Thus we have $I(X;Y|Z) = 0$. Clearly, K_2 and K_4 are independent. Since $X = K_2$ is completely unpredictable from $Z = K_2 \oplus K_4$ and vice versu, we conclude that X and Z are independent [47]. Thus, $I(X;Z) = 0$. This completes the proof. ■

REFERENCES

[1] "Cisco visual networking index: Global mobile data traffic forecast update, 2016–2021," White Paper, Feb. 2017.

[2] A. Asadi, Q. Wang, and V. Mancuso, "A survey on device-to-device communication in cellular networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 4, pp. 1801–1819, 4th Quart., 2014.

[3] L. Lei, Z. Zhong, C. Lin, and X. Shen, "Operator controlled device-to-device communications in LTE-advanced networks," *IEEE Wireless Commun.*, vol. 19, no. 3, pp. 96–104, Jun. 2012.

[4] K. Doppler, C.-H. Yu, C. B. Ribeiro, and P. Janis, "Mode selection for device-to-device communication underlaying an LTE-advanced network," in *Proc. WCNC*, Sydney, NSW, Australia, Apr. 2010, pp. 1–6.

[5] A. T. Gamage, H. Liang, R. Zhang, and X. Shen, "Device-to-device communication underlaying converged heterogeneous networks," *IEEE Wireless Commun.*, vol. 21, no. 6, pp. 98–107, Dec. 2014.

[6] M. Waqas, M. Zeng, and Y. Li, "Mobility-assisted device to device communications for content transmission," in *Proc. IWCMC*, Valencia, Spain, Jun. 2017, pp. 206–211.

[7] M. Waqas, M. Zeng, Y. Li, D. Jin, and Z. Han, "Mobility assisted content transmission for device-to-device communication underlaying cellular networks," *IEEE Trans. Veh. Technol.*, to be published.

[8] P. Jänis *et al.*, "Device-to-device communication underlaying cellular communications systems," *Int. J. Commun., Netw. Syst. Sci.*, vol. 2, no. 3, pp. 169–178, 2009.

[9] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (D2D) communication: A review," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1054–1079, 2nd Quart., 2017.

[10] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[11] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[12] I. Csiszár and J. Kerner,"Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[13] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[14] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[15] V. Kumar, J.-M. J. Park, and K. Bian, "PHY-layer authentication using duobinary signaling for spectrum enforcement," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1027–1038, May 2016.

[16] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, 1st Quart., 2017.

[17] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[18] M. Wang and Z. Yan, "Security in D2D communications: A review," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Helsinki, Finland, Aug. 2015, pp. 1199–1204.

[19] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[20] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 5, pp. 1484–1497, Oct. 2012.

[21] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 8, pp. 1578–1588, Sep. 2012.

[22] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Social trust and social reciprocity based cooperative D2D communications," in *Proc. MobiHoc*, Bangalore, India, Jul./Aug. 2013, pp. 187–196.

[23] Y. Li, T. Wu, P. Hui, D. Jin, and S. Chen, "Social-aware D2D communications: Qualitative insights and quantitative analysis," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 150–158, Jun. 2014.

[24] H. Gintis, "Strong reciprocity and human sociality," *J. Theor. Biol.*, vol. 206, no. 2, pp. 169–179, 2000.

[25] K.-C. Chen, M. Chiang, and H. V. Poor, "From technological networks to social networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 548–572, Sep. 2013.

[26] X. Chen, J. Huang, and H. Li, "Adaptive channel recommendation for opportunistic spectrum access," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1788–1800, Sep. 2013.

[27] X. Chen and J. Huang, "Imitation-based social spectrum sharing," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1189–1202, Jun. 2015.

[28] Y. Cao, X. Chen, T. Jiang, and J. Zhang, "SoCast: Social ties based cooperative video multicast," in *Proc. IEEE INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 415–423.

[29] Y. Zhang, E. Pan, L. Song, W. Saad, Z. Dawy, and Z. Han, "Social network aware device-to-device communication in wireless networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 1, pp. 177–190, Jan. 2015.

[30] Y. Sun, T. Wang, L. Song, and Z. Han, "Efficient resource allocation for mobile social networks in D2D communication underlaying cellular networks," in *Proc. ICC*, Sydney, NSW, Australia, 2014, pp. 2466–2471.

[31] K. Chen, B. B. Natarajan, and S. Shattil, "Secret key generation rate with power allocation in relay-based LTE-A networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2424–2434, Nov. 2015.

[32] S. Gopinath, R. Guillaume, P. Duplys, and A. Czylwik, "Reciprocity enhancement and decorrelation schemes for PHY-based key generation," in *Proc. Globecom Workshops*, Austin, TX, USA, Dec. 2014, pp. 1367–1372.

[33] A. Sadeghi, M. Zorzi, and F. Lahouti, "Analysis of key generation rate from wireless channel in in-band full-duplex communications," in *Proc. ICC Workshops*, Kuala Lumpur, Malaysia, May 2016, pp. 1–6.

[34] C. Thai, J. Lee, and T. Q. S. Quek, "Physical-layer secret key generation with colluding untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1517–1530, Feb. 2016.

[35] J. Sun, X. Chen, J. Zhang, Y. Zhang, and J. Zhang, "SYNERGY: A game-theoretical approach for cooperative key generation in wireless networks," in *Proc. INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 997–1005.

[36] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. CCS*, Alexandria, VA, USA, Oct./Nov. 2007, pp. 401–410.

[37] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. MobiCom*, Beijing, China, Sep. 2009, pp. 321–332.

[38] R. Ahlswede and I. Csiszàr, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[39] L. Lai, Y. Liang, and W. Du, "PHY-based cooperative key generation in wireless networks," in *Proc. 49th Annu. Allerton Conf.*, Monticello, IL, USA, Sep. 2011, pp. 662–669.

[40] P. Xu, Z. Ding, X. Dai, and G. K. Karagiannidis, "Simultaneously generating secret and private keys in a cooperative pairwise-independent network," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1139–1150, Jun. 2016.

[41] W. Saad, Z. Han, M. Debbah, A. Hjørungnes, and T. Basar, "Coalitional game theory for communication networks," *IEEE Signal Process. Mag.*, vol. 26, no. 5, pp. 77–97, May 2009.

[42] Y. Li, D. Jin, J. Yuan, and Z. Han, "Coalitional games for resource allocation in the device-to-device uplink underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 3965–3977, Jul. 2014.

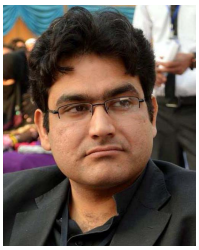
[43] G. Fodor *et al.*, "Design aspects of network assisted device-to-device communications," *IEEE Commun. Mag.*, vol. 50, no. 3, pp. 170–177, Mar. 2012.

[44] M. E. J. Newman, D. J. Watts, and S. H. Strogatz, "Random graph models of social networks," *Proc. Nat. Acad. Sci. USA*, vol. 99, no. 1, pp. 2566–2572, 2002.

[45] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.

[46] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.

[47] R. B. Davies. (Feb. 14, 2018). *Exclusive OR (XOR) and Hardware Random Number Generators*. [Online]. Available: http://www.robertnz.net/pdf/xor2.pdf



Muhammad Waqas received the B.Sc. and M.Sc. degrees from the Department of Electrical Engineering, University of Engineering and Technology, Peshawar, Pakistan, in 2009 and 2014, respectively. He is currently pursuing the Ph.D. degree at the Beijing National Research Center for Information Science and Technology, Department of Electronic Engineering, Tsinghua University, Beijing, China.

He has also served as an Assistant Professor and a Program Coordinator with the Sarhad University of Science and Information Technology, Peshawar, from 2011 to 2015. He has several research publications in IEEE journals and conferences. His current research interests are in the areas of networking and communications, including 5G networks, D2D communication resource allocation and physical layer security and information security, mobility investigation in D2D communication, Fog computing, and MEC.

Manzoor Ahmed received the B.E. from the Balochistan University of Engineering and Technology Khuzdar, Balochistan, Pakistan, in 1996, the M.Phil. degree from the Balochistan University of Information and Technology, Engineering and Management Sciences, Pakistan, in 2010, and the Ph.D. degree from the Beijing University of Posts and Telecommunications, Beijing, China, in 2015. He is currently a Post-Doctoral Researcher with the Beijing National Research Center for Information Science and Technology, Department of Electronic Engineering, Tsinghua University, Beijing, China. He served in the Telecomm Industry for 12 years. He has published several research publications in IEEE journals and conferences. His research interests include the non-cooperative and cooperative game theoretic-based resource management in hierarchical heterogeneous networks, interference management in small cell networks, and 5G networks, D2D communication resource allocation and physical layer security and information security, Fog-RAN, C-RAN and Fog computing, MEC, and computational offloading in vehicular networks. He was the recipient of the Best Paper Award at the 2014 GameNets Conference.

Yong Li (M'09–SM'16) received the B.S. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2007, and the Ph.D. degree in electronic engineering from Tsinghua University, Beijing, China, in 2012.

He is currently a Faculty Member of the Department of Electronic Engineering, Tsinghua University.

He has served as the General Chair, the TPC Chair, and a TPC Member for several international workshops and conferences, and he is on the editorial board of three international journals. His papers have been cited over 2300 times (six papers exceed 100 citations, Google Scholar). Among them, eight are ESI Highly Cited Papers in computer science, and four received conference Best Paper (run-up) Awards. He was the recipient of the IEEE 2016 ComSoc Asia-Pacific Outstanding Young Researchers and Young Talent Program of China Association for Science and Technology.

Depeng Jin (M'09) received the B.S., M.S., and Ph.D. degrees from Tsinghua University, Beijing, China, in 1995, 1997, and 2000, respectively.

From 2000 to 2003, he was an Assistant Professor. From 2004 to 2012, he was an Associate Professor. Since 2012, he has been a Professor with Department of Electronic Engineering, Tsinghua University. His research focuses on communication and networking. His current interests are in the topics of software-defined networks, wireless mobile network, and mobile big data.

Sheng Chen (M'90–SM'97–F'08) received the B.Eng. degree in control engineering from the East China Petroleum Institute, Dongying, China, in 1982, the Ph.D. degree in control engineering from City University, London, in 1986, and the D.Sc. degree from the University of Southampton, Southampton, U.K, in 2005.

From 1986 to 1999, he held research and academic appointments with the Universities of Sheffield, Edinburgh, and Portsmouth, all in the U.K. Since 1999, he has been with the School of Electronics and Computer Science, University of Southampton, where he is a Professor of intelligent systems and signal processing. He has authored or co-authored over 600 research papers. His research interests include adaptive signal processing, wireless communications, modeling and identification of nonlinear systems, neural network and machine learning, intelligent control system design, and evolutionary computation methods and optimization.

Prof. Chen is a Fellow of the United Kingdom Royal Academy of Engineering and IET, a Distinguished Adjunct Professor with King Abdulaziz University, Jeddah, Saudi Arabia, and an ISI highly cited Researcher in engineering in 2004.