Social Trust Aided D2D Communications: Performance Bound and Implementation Mechanism

Xinlei Chen, Yulei Zhao, Yong Li, *Senior Member, IEEE*, Xu Chen, *Member, IEEE*, Ning Ge, *Member, IEEE*, and Sheng Chen, *Fellow, IEEE*

***Abstract*— In a device-to-device (D2D) communications underlaying cellular network, any user is a potential eavesdropper for the transmissions of others that occupy the same spectrum. The physical-layer security mechanism of theoretical secure capacity, which maximizes the rate of reliable communication from the source user to the legitimate receiver and ensure unauthorized users learn as little as information as possible, is typically employed to guarantee secure communications. As hand-held devices are carried by human beings, we may leverage their social trust to decrease the number of potential eavesdroppers. Aiming to establish a new paradigm for solving the challenging problem of security and efficiency tradeoff, we propose a social trust-aware D2D communication architecture that exploits the social-domain trust for securing the physical-domain communication. In order to understand the impact of social trust on the security of transmissions, we analyze the system ergodic rate of social trust aided communications via stochastic geometry, and our result based on a real data set shows that the proposed social trust aided D2D communication increases the system secrecy rate by about 63% compared with the scheme without considering social trust relation. Furthermore, in order to provide implementation mechanism, we utilize matching theory to implement efficient resource allocation among multiple users. Numerical results show that our proposed mechanism increases the system secrecy rate by 28% with fast convergence over the social oblivious approach.**

***Index Terms*— Social trust, stochastic geometry, D2D communications, matching theory.**

Manuscript received September 15, 2017; revised February 1, 2018; accepted February 15, 2018. Date of publication April 11, 2018; date of current version October 18, 2018. This work was supported in part by the National Key Research and Development Program of China under Grant 2017YFB1001703, in part by the National Nature Science Foundation of China under Grant 61132002 and Grant 61301080, in part by the Creative Research Group Program from NSFC under Grant 61321061, in part by the Program for Guangdong Introducing Innovative and Enterpreneurial Teams under Grant 2017ZT07X355, and in part by the Fundamental Research Funds for the Central Universities under Grant 17lgjc40. *(Corresponding author: Xinlei Chen.)*

X. Chen is with the Department of Electric and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: xinlei.chen@sv.cmu.edu).

Y. Zhao, Y. Li, and N. Ge are with the Tsinghua National Laboratory for Information Science and Technology, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China (e-mail: liyong07@tsinghua.edu.cn).

X. Chen is with the School of Data and Computer Science, Sun Yat-sen University, Guangzhou 510275, China.

S. Chen is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K.

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/JSAC.2018.2825658

I. Introduction

To MEET the increasing demands for local area services, D2D communication is proposed as a key component for next-generation cellular networks [1], where the user equipment (UE) communicates with nearby devices over direct links, instead of through a base station (BS) [2]. Licensed spectrum sharing in D2D communication can be categorized into two modes: overlay and underlay. Overlay assumes that the cellular and D2D users use orthogonal spectrum resources without mutual interferences at the cost of low efficiency. Underlay, as a more efficient way of spectrum sharing, enables users to share the same spectrum [3]. Due to this spectrum sharing, however, users have the potential to intercept the transmission of others that share the same spectrum resource. Since the security of communication is a critical issue for user privacy and mobile applications [4], mobile users may be reluctant to select D2D communication mode, despite the considerable benefits it brings. Therefore, academia and industry have put increasing efforts into the security problems [4], and the standardization of D2D security communication has been considered [5].

Due to the spectrum-sharing characteristic, confidentiality is a key problem in D2D transmission. To protect transmitted data from attacks, confidentiality in the physical layer prevents the data from being accessed by unauthorized users [6]. To achieve security against different passive and active attacks, different physical-layer security mechanisms are adopted, including theoretical secure capacity, channel, coding, power, and signal detection approaches [7]. Even with encryption, it is still challenging to prevent unauthorized user from eavesdropping due to the broadcast nature of the wireless medium. The communication still suffers from the risk of key loss, thus losing the data. In addition, encryption, decryption and key management are all computationally expensive. The physical layer security mechanism of theoretical secure capacity has been proved to be a valid method, which maximizes the rate of reliable communication from the source user to the legitimate receivers, while ensuring unauthorized users learn as little as information as possible [8]. However, to ensure secure transmission in the physical layer, this method has to pay the great cost of decreasing system transmission rate [9]. Therefore, it is a challenging problem to ensure secret

D2D communications while sustaining the benefits of high spectrum efficiency.

Hand-held devices are carried by human beings who form stable social structures, and social trust is a common attribute adopted among family members, friends and colleagues to form social groupings [10]. A natural question is 'can we leverage the social trust to improve the security of D2D transmissions without scarifying the efficiency?'. Intuitively, social trust relations can help to reduce the number of potential eavesdroppers and therefore to enhance the security of communications. For example, by only sharing the spectrum among social trusted users, the security of transmissions can be enhanced without having to rely on physical-layer security measure. Aiming to open up a new avenue for solving the challenging problem of security and efficiency tradeoff, we propose a social trust aided D2D communications architecture that exploits social trust for secure communication. There are two key challenges in meeting our goal. The first one is to understand the gains of social trust-aware D2D communications, i.e., how social trust can enhance social trust rate, and the second one is to provide implementation mechanism to efficiently utilize social trust relations in system design, i.e., how to efficiently utilize social trust to implement resource allocation among cellular and D2D users.

Therefore, we investigate these two fundamental problems. Our goal is to obtain theoretical bound and establish implementation mechanism as the first step to understand and utilize the framework of social trust aided D2D communications. The theoretical bound provides the potential performance gains of exploiting social trust among mobile users for efficient secure transmission. We utilize stochastic geometry to quantitatively analyze the social trust rate for D2D communications. Furthermore, we formulate the resource allocation as an optimization problem to maximize the system social trust rate and establish efficient implementation mechanism based on matching theory. The social trust mechanism presented here can also be applied to other wireless networks and has great potential to increase system secrecy rate significantly.

Our contributions are summarized as follows:

- *Social trust aided D2D communications*: We propose this novel architecture by jointly considering social trust and secure communication to solve the security problem with ensured transmission rate. Specifically, the proposed scheme implements efficient spectrum sharing among mobile users by utilizing social trust in the social domain to achieve secure communications in the physical domain. To the best of our knowledge, this is the first study applying social trust to enhance the security of communications.
- *Performance bound*: We obtain the ergodic rate of the proposed social trust aided D2D communication architecture by utilizing stochastic geometry. Theoretical and numerical analysis based on a real dataset shows that the system secrecy rate increases about 63% by considering social trust relation. Our results also reveal how the D2D user density impacts on the intercepted rate of cellular and D2D users, which indicates that efficient resource allocation is beneficial in order to maximize the system secrecy rate.
- *Efficient resource allocation*: In order to provide a practical mechanism in utilizing the social trust, we employ matching theory to implement efficient resource allocation by jointly considering social trust and mutual interference among cellular and D2D users. Our results show that the proposed matching algorithm significantly increases the system secrecy rate, and it outperforms the coalition game method without considering social trust by about 28% in the scenario involving 20 D2D users.

II. Related Work

Andreev *et al.* [11] discussed the vision and open challenges of D2D communication, many of which are related to security. To achieve security against different passive and active attacks, different physical-layer security mechanisms are adopted, including theoretical secure capacity, channel, coding, power, and signal detection approaches [7]. Security has attracted increasing attention from academia and industry [4], especially for D2D underlaying cellular networks due to spectrum sharing [12]. Yue *et al.* [13] introduced D2D communication as the interference against eavesdropping. The physical layer security mechanism of theoretical secure capacity has been proved to be a valid method, which maximizes the rate of reliable communication from the source user to the legitimate receivers, while ensuring unauthorized users learn as little as information as possible [8], [9]. This mechanism guarantees the secrecy of transmission from an information-theoretic viewpoint [6], which is conceived as a promise solution in 5G networks [14]. For example, a scheduling algorithm is proposed to maximize the physical-layer security transmission rate for future cellular networks [15]. Such a physical-layer security method typically assumes that all users are not trustworthy, and it ensures the secrecy of transmissions at the cost of reducing the system transmission rate significantly. However, the assumption that all D2D users are not trustworthy is not appropriate, as users in same social grouping are often have high social trust [10], [16]–[18].

Social network features, such as social ties, community and centrality, have been exploited to design efficient resource allocation and mode selection for D2D communication systems [16]. Social trust and reciprocity have been utilized to design efficient cooperative strategies for D2D communications [10], [17], [19]–[22]. For example, Chen *et al.* [19] proposed a framework to maximize social group utility, and Zhang *et al.* [22] designed social-aware peer-discovery approach. Ometov *et al.* [23] enable the communication devices to automatically decide entities with a novel layer of social awareness. These existing works however do not consider explicitly the security problem. To the best of our knowledge, we are the first to consider the utilization of social trust to enhance the security of D2D communications. In particular, we propose a social security aided D2D communication mechanism to protect user privacy and to ensure spectrum sharing efficiency.

Stochastic geometry is an efficient tool to analyze spectrum sharing relationships for large-scale wireless networks [24]. In recent years, many researches have utilized stochastic geometry to analyze interference and coverage probability for D2D communication networks [3], [25]–[27]. Lin *et al.* [3] proposed a general analytical approach with stochastic geometry to evaluate the performance of D2D communication through overlay and underlay spectrum sharing schemes. Lee *et al.* [25] utilized stochastic geometric to analyze power control for D2D communication underlaying cellular network. Liu *et al.* [26] analyzed the ergodic rate for D2D overlaying multi-channel downlink cellular network based on stochastic geometry. Furthermore, Ma *et al.* [27] used stochastic geometry to model the D2D-enabled cellular network with eavesdroppers and exploited the interferences through a secrecy perspective.

Matching theory has been regarded as an efficient resource allocation method for future wireless networks [28]. Xu and Li [29] utilized a stable matching framework to solve network problems. Gu *et al.* [30] introduced matching theory to implement the efficient resource allocation for D2D communication underlaying cellular networks. However, this work only considered the scenario of one-to-one matching. Saad *et al.* [31] used many-to-one matching to implement uplink user association in small cell networks. In this paper, we first utilize stochastic geometry to analyze the critical parameters that influence the social trust rate. Then, matching theory is used to determine the spectrum sharing relationships for secrecy transmissions.

The rest of this paper is organized as follows. Section III presents the system overview and problem statement. Section IV analyzes the theoretical physical-layer secrecy rate of the proposed social trust aided D2D communication scheme, while an efficient resource allocation is developed in Section V. Performance evaluations are given in Section VI, and Section VIII concludes this work.

III. System Overview and Problem Statement

A. System Overview

Fig. 1 illustrates the social trust aided D2D communications underlaying cellular network from both the physical domain and social domain. The social domain indicates the social trust relationship among mobile users, while the wireless links are determined by the spectrum sharing relations among cellular users and D2D user pairs in the physical domain. Let C and D denote the numbers of cellular users and D2D pairs working under full-duplex mode [10], respectively. Cellular and D2D users that share the same spectrum resource will incur severe interference among them [32].

In the social domain, social relation graph among mobile users is denoted by $G = (V, \mathcal{W})$, where V is the collection of all the cellular users and D2D pairs with $|V| = N = C + D$, while $\mathcal{W} = \{\omega_{i,j}, i, j = 1, 2, \cdots, N\}$ with binary $\omega_{i,j}$ denoting the social trust between users i and j. Specifically, $\omega_{i,j} = 1$ indicates that user i trusts user j; otherwise, $\omega_{i,j} = 0$. In our work, it is supposed that social trust relationships are undirected, i.e., $\omega_{i,j} = \omega_{j,i}$. In Fig. 1, *Alice* is friend of *Smith-Susan* and *Brown-Ben*, which means $\omega_{c_1,d_1} = 1$ and $\omega_{c_1,d_2} = 1$. They can enthusiastically share the same spectrum resource without worrying the secrecy problem. Especially, *Smith* and *Susan* represent the D2D users of D2D pair *Smith-Susan*. On the other hand, *Smith-Susan* and *Brown-Ben* have no trust of each other with $\omega_{d_1,d_2} = 0$, and both will worry the other's eavesdropping. Also *Bob* has no social ties with *Mike-Mary* and *David-Davis* with $\omega_{c_2,d_3} = 0$ and $\omega_{c_2,d_4} = 0$. Thus, *Bob* is a potential eavesdropper to *Mike-Mary* and *David-Davis*. We adopt clustering coefficient in graph theory to define social-link probability, denoted by $p_s \in [0,\ 1]$, to indicate the social trust among cellular and D2D users, which is the proportion between social trust edges and total edges of the complete graph in the social domain, i.e., $p_s = \sum_{i,j} \omega_{i,j} \big/ N(N-1)$.

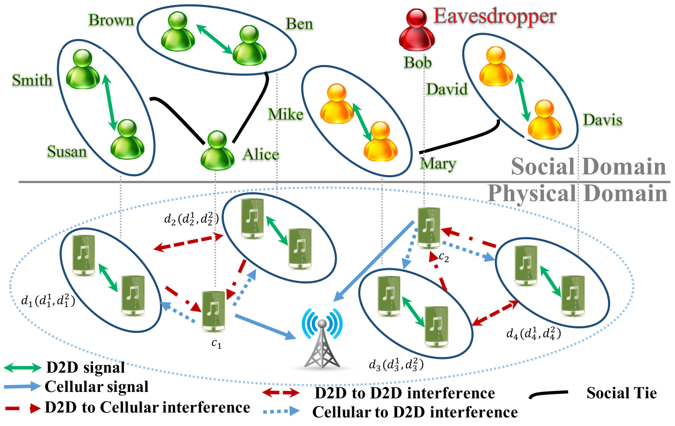


Fig. 1. A social trust aided D2D communication underlaying cellular network, with 2 cellular users, c_1 and c_2, and 4 D2D user pairs, d_1 to d_4. In the physical domain, wireless links are subject to physical interference constraints, while in the social domain, social trusts among mobile users are indicated.

In the physical domain, proximity D2D users communicating with each other can occupy the same spectrum resource of cellular users to increase the system capacity, and we need to match D2D users to cellular users to decrease the mutual interferences. As shown in Fig. 1, there are two cellular users, c_1 and c_2, as well as four D2D pairs, $d_i(d_i^1, d_i^2)$, $1 \leq i \leq 4$. Here we use d_i to denote the ith D2D pair, with d_i^1 representing transmitter and d_i^2 receiver. D2D pair d_1 and d_2 occupy the same spectrum resource with c_1, while D2D pair d_3 and d_4 share the spectrum resource with c_2.

B. System Assumptions

Since this paper focuses on investigating tradeoff between efficiency and security for D2D communication by integrating social trust information, to simplicity but without loss of generality, we make the following assumptions.

- The social trust relationships between cellular users and D2D users are stable. One user, either cellular or D2D user, does not change its trust relationship with another user very frequently. This is valid since social trust relationship transmission frequency is usually slower than daily change. As a result, the system has enough time to reallocate resources based on new social trust relationship.

- The transmit power P_c for every cellular user is the same. We also assume same transmit power P_d for every D2D user. In the following subsection, it is shown that transmit powers P_c and P_d are two constant values in the equations. Whether same or different transmit powers are assumed for different cellular or D2D users do not change the form of the problem and solution. We assume the same transmit power only for the simplified form of the all related equations, which does not affect the way we solve the problem and final solution.
- The receiver noise of cellular user and D2D user is negligible. According to [25], for uplink cellular user transmission, the dominant interferer is the nearest several D2D transmissions. Inference from these D2D transmissions are usually much stronger than the receiver noise of the cellular user with a high probability. As a result, the receiver noise is negligible. This is also true for D2D users.

C. Problems and Challenges

From the above system overview, it is observed that social trust relations can be exploited to decrease the number of potential eavesdroppers and hence to improve the system secrecy rate. This motivates us to propose the social trust aided D2D communication to solve the challenging problem of security and efficiency tradeoff. There are two key issues requiring investigation in order to realize social trust aided D2D communications systems, namely, determining the potential gains of utilizing social trust to assist D2D communications and providing practical implementation mechanism.

A major challenge in the derivation of performance bound is how to consider social trust relations to obtain the system secrecy rate. In D2D communications, mutual interference determines the maximum system rate. On the other hand, social trust relations of users have significant impact on the maximum system secrecy rate. When one additional D2D user shares the same spectrum, it changes both the interference and social relationships among users.

The challenge in implementation is how to efficiently allocate the spectrum resources of cellular users to D2D users by jointly considering social trust and mutual interferences. Traditional resource allocation in D2D communications only considers interference to divide mobile users into multiple groups with small mutual interferences. However, in social trust aided D2D communications, the users who are trustworthy with each other may occupy the same spectrum resource, even though this may cause large mutual interferences.

IV. Coverage Probability and Ergodic Rate

We now tackle the first challenge of deriving the performance bound. Our analysis model is depicted in Fig. 2. D2D pairs are spatially distributed according to a Poisson point process (PPP) Φ_d with density λ_d in the plane with radius R [25], [26]. D2D receivers distribute randomly at fixed distances away from their corresponding D2D transmitters. We first study the mutual interferences among a cellular user and the D2D users that share the same spectrum resource. As illustrated in Fig. 2, D2D pairs d_1, d_2, d_3 and d_4 occupy the same spectrum resource of cellular user c. The uplink transmission of c is interfered by D2D transmitters d_1^1, d_2^1, d_3^1 and d_4^1. D2D transmissions also interfere with each other as well as suffer the interference from the cellular user's transmission. Consider for example D2D pair d_3. d_3^2 receives the interference from d_1^1, d_2^1, d_4^1 and c. From the eavesdropper's perspective, d_3^2 has the probability $p_e = 1 - p_s$ to intercept the transmissions of these other users.

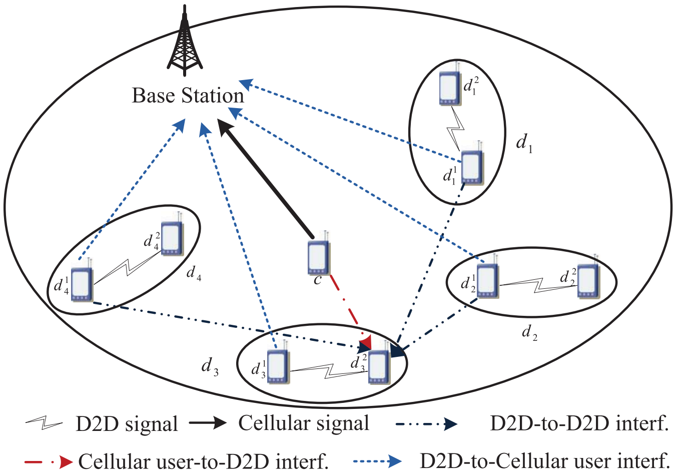


Fig. 2. Illustration of interference relationship for D2D communication underlaying cellular network in single cell.

The transmission link from node i to node j is modeled as a Rayleigh fading channel with channel impulse response $h_{i,j}$. The received power of node j from the transmission of node i is given by $P_{i,j} = P_i \cdot |h_{i,j}|^2 = P_i \cdot \rho_{i,j}^{-\alpha} \cdot |h_0|^2$, where P_i is the transmit power of node i, $\rho_{i,j}$ is the distance between the two nodes, α is the path-loss exponent, and h_0 is the complex Gaussian channel coefficient. According to [8] and [9], the complex Gaussian channel coefficient h_0 represents distance-independent fading, which does not depend on i and j. However, it is true that the channel characteristic depends on the distance between i and j, which is denoted by $\rho_{i,j}^{-\alpha}$. Based on the interference analysis, we need to consider the signal to interference plus noise ratio (SINR) in each time slot. The SINR at terminal j receiving the desired signal from transmitter i can be expressed as

$$\gamma_j = \frac{P_i \rho_{i,j}^{-\alpha} |h_0|^2}{P_{\mathrm{int},j} + N_0},$$

where $P_{\mathrm{int},j}$ is the interference power received by terminal j and N_0 is the noise power at the receiver.

A. Social Trust Rate of Cellular User

The coverage probability of cellular user c is defined by $\overline{P}_{cov}^{c}(T_c) = \mathbb{P}(\gamma_c \geq T_c)$, where γ_c denotes the SINR of cellular user c and T_c is the SINR threshold required for data detection. γ_c can be expressed as

$$\gamma_c = \frac{P_c \rho_{c,b}^{-\alpha} \left|h_0\right|^2}{\sum\limits_{d\in\mathcal{D}} P_d \rho_{d,b}^{-\alpha} \left|h_0\right|^2 + N_0}, \tag{1}$$

where $\mathcal{D}$ denotes the set of D2D users that share the spectrum resource with c, $\rho_{c,b}$ is the distance between c and BS and $\rho_{d,b}$ is the distance between D2D user d and BS, while P_c is the transmit power of c and P_d is the transmit power of d. The ergodic rate of cellular user c is obtained by $\log_2(1+\gamma_c)$ when γ_c is a constant value. Since γ_c is a random variable in our scenario, the ergodic rate of cellular user c can be obtained by the expected value $E[\log_2(1+\gamma_c)]$ as [25]

$$\begin{aligned} R_c &= \int_0^\infty \log_2(1+x)\mathbb{P}(\gamma_c = x)dx \\ &= \int_0^\infty \frac{\mathbb{P}(\gamma_c \geq x)}{(1+x)\ln 2}dx. \end{aligned} \tag{2}$$

Each D2D user that does not build a trusted connect with cellular user c may act as eavesdropper to intercept the cellular user's transmission. Let T_s denote the minimum SINR requirement for eavesdropper to intercept the signal correctly. The uplink information transmission of c is safe when the largest SINR at potential eavesdroppers is less than this minimum SINR requirement T_s. Therefore, we have the following definition for social trust coverage probability of cellular user.

Definition 1: Social trust coverage probability of cellular user: The social coverage probability of secrecy transmission for cellular user c, denoted by $\overline{P}^c_{cov,s}(T_s)$, is defined as

$$\overline{P}^c_{cov,s}(T_s) = \mathbb{P}\Big(\max_{d'\in\mathcal{D}_{c,e}} \gamma_{c,d'} \leq T_s\Big), \tag{3}$$

where $\mathcal{D}_{c,e} = \{d|\omega_{c,d} = 0, d \in \mathcal{D}\}$, and $\gamma_{c,d'}$ is the SINR at D2D receiver d' for the transmission of c, which is given by

$$\gamma_{c,d'} = \frac{P_c \rho_{c,d'}^{-\alpha} \left|h_0\right|^2}{\sum_{d\in\mathcal{D}\setminus\{d'\}} P_d \rho_{d,d'}^{-\alpha} \left|h_0\right|^2 + N_0}, \quad \forall d' \in \mathcal{D}. \tag{4}$$

Let R_c^e denote the intercepted transmission rate by D2D users. Since $\gamma_{c,d'}$ is a random variable, the intercepted transmission rate is defined by the expected value $E[\log_2(1+\gamma_{c,d'})]$, which can be obtained as follows:

$$\begin{aligned} R_c^e &= \int_0^\infty \log_2(1+x)\mathbb{P}\Big(\max_{d'\in\mathcal{D}_{c,e}} \gamma_{c,d'} = x\Big)dx \\ &= \int_0^\infty \frac{\mathbb{P}\Big(\max\limits_{d'\in\mathcal{D}_{c,e}} \gamma_{c,d'} \geq x\Big)}{(1+x)\ln 2}dx \\ &= \int_0^\infty \frac{1-\mathbb{P}\Big(\max\limits_{d'\in\mathcal{D}_{c,e}} \gamma_{c,d'} \leq x\Big)}{(1+x)\ln 2}dx. \end{aligned} \tag{5}$$

As the information transmission of cellular user is independent from the interception process of D2D users, the social secrecy rate of c can be defined as the difference between its ergodic rate and the intercepted transmission rate by D2D users. The social secrecy rate of c will be set to zero if the difference is negative. Larger difference means higher security for c transmission.

Definition 2: Social trust ergodic rate of cellular user: The social trust rate for cellular user c is $R_c^s = \max\{R_c - R_c^e, 0\}$. From (5), R_c^e is determined by both mutual interference relationship and social trust information. Therefore, Definition 1 can capture this feature and reflect the impact of social trust on secrecy rate.

Assuming the same transmit power P_c for every cellular user and the same transmit power P_d for every D2D user, the coverage probability of cellular user is obtained as [25]:

$$\overline{P}^c_{cov}(T_c) = \frac{1-\exp\Big(-\frac{\pi\lambda_d R^2}{\mathrm{sinc}(\delta)}\Big(\frac{P_d}{P_c}\Big)^\delta T_c^\delta\Big)}{\frac{\pi\lambda_d R^2}{\mathrm{sinc}(\delta)}\Big(\frac{P_d}{P_c}\Big)^\delta T_c^\delta}, \tag{6}$$

where $\delta = \frac{2}{\alpha}$, and the noise is neglected. The expression shows that the coverage probability of cellular user is jointly affected by three factors: 1) the transmit power ratio between D2D user and cellular user $\frac{P_d}{P_c}$, 2) the average number of D2D transmitters $\pi\lambda_d R^2$, 3) the SINR threshold required for data detection of cellular user c T_c. Then the transmission rate of cellular user is:

$$R_c = \int_0^\infty \frac{\overline{P}^c_{cov}(x)}{(1+x)\ln 2}dx, \tag{7}$$

which cannot guarantee the secrecy of data transmissions.

Theorem 1: If the receiver noise is negligible, the social secrecy coverage probability of cellular user is

$$\begin{aligned} &\overline{P}^c_{cov,s}(T_s) \\ &= \exp\Big(-2\pi p_e \lambda_d \int_0^R \exp\Big(-\frac{\pi\lambda_d\Big(\frac{P_d T_s}{P_c}\Big)^\delta \rho_{c,z}^2}{\mathrm{sinc}(\delta)}\Big)\rho_{c,z} d\rho_{c,z}\Big). \end{aligned} \tag{8}$$

This equation shows that the social secrecy coverage probability of cellular user is determined by the following factors: 1) the transmit power ratio between D2D user and cellular user $\frac{P_d}{P_c}$, 2) the minimum SINR requirement for eavesdropper to intercept T_s, 3) the probability to intercept p_e, 4) D2D pair density λ_d.

Proof: See Appendix A

From (5) and (8), we have the secrecy rate of c given by

$$R_c^e = \int_0^\infty \frac{1-\overline{P}^c_{cov,s}(x)}{(1+x)\ln 2}dx. \tag{9}$$

Finally, we obtain the social trust rate of cellular user as $R_c^s = \max\{R_c - R_c^e, 0\}$.

B. Secrecy Rate of D2D Users

Similarly, for D2D user pair d_i, its ergodic rate R_{d_i} is:

$$\begin{cases} \gamma_{d_i} = \dfrac{P_d \rho_{d_i,d_i}^{-\alpha} \left|h_0\right|^2}{P_c \rho_{c,d_i}^{-\alpha} \left|h_0\right|^2 + \sum\limits_{d'\in\mathcal{D}\setminus\{d_i\}} P_d \rho_{d',d_i}^{-\alpha} \left|h_0\right|^2 + N_0}, \\ R_{d_i} = \displaystyle\int_0^\infty \log_2(1+x)\mathbb{P}(\gamma_{d_i} = x)dx, \end{cases} \tag{10}$$

where γ_{d_i} is the SINR at receiver of D2D pair d_i and we use ρ_{d_i,d_i} to denote the distance between the transmitter and receiver of D2D pair d_i.

For D2D user pair d_i, each D2D user that does not build a trusted connect with it may act as eavesdropper to intercept its transmission. Let Ts denote the minimum SINR requirement for eavesdropper to intercept the signal correctly. Transmission of d_i is safe when the largest SINR at potential eavesdroppers is less than this minimum SINR requirement T_s. Therefore, we have the following definition for social trust coverage probability of D2D user d_i.

Definition 3: Social trust coverage probability of D2D user: The coverage probability of secrecy transmission for D2D user d_i, denoted by $\overline{P}^{d_i}_{cov,s}(T_s)$, is

$$\overline{P}^{d_i}_{cov,s}(T_s) = \mathbb{P}\left(\max_{d'\in\mathcal{D}_{d_i,e}} \gamma_{d_i,d'} \le T_s\right), \tag{11}$$

where $\mathcal{D}_{d_i,e} = \{d|\omega_{d_i,d} = 0, d \in \mathcal{D} \setminus \{d_i\} \cup \{c\}\}$.

The intercepted rate of D2D user d_i, denoted by $R^e_{d_i}$, is:

$$\begin{cases} \gamma_{d_i,d'} = \dfrac{P_d \rho_{d_i,d'}^{-\alpha} |h_0|^2}{P_c \rho_{c,d'}^{-\alpha} |h_0|^2 + \sum\limits_{d^0\in\mathcal{D}\setminus\{d_i,d'\}} P_d \rho_{d^0,d'}^{-\alpha} |h_0|^2 + N_0}, \\ R^e_{d_i} = \displaystyle\int_0^\infty \log_2(1+x)\mathbb{P}\left(\max_{d'\in\mathcal{D}_{d_i,e}} \gamma_{d_i,d'} = x\right) dx, \end{cases} \tag{12}$$

where $\gamma_{d_i,d'}$ is the SINR at the receiver of eavesdropper d', and $R^e_{d_i}$ is the intercepted rate of regular transmission for d_i. With R_{d_i} and $R^e_{d_i}$, we have the secrecy rate of D2D user d_i.

Similar to cellular user, the social secrecy rate of d_i can be defined as the difference between its ergodic rate and the intercepted transmission rate. The social secrecy rate of d_i will be set to zero if the difference is negative. Larger difference means higher security for c transmission.

Definition 4: Social secrecy ergodic rate of D2D user: The social secrecy rate for D2D user d_i is $R^s_{d_i} = \max\left\{R_{d_i} - R^e_{d_i}, 0\right\}$.

The coverage probability of D2D user d_i is given by [25]:

$$\begin{aligned} &\overline{P}^{d_i}_{cov}(T_d) \\ &\quad = \exp\left(-\frac{\pi\lambda_d T_d^\delta}{\text{sinc}(\delta)}\rho^2_{d_i,d_i}\right) \frac{1}{1+\left(\frac{T_d P_c}{P_d}\right)^\delta \left(\rho_{d_i,d_i}\frac{45\pi}{128R}\right)^2}, \end{aligned} \tag{13}$$

where T_d is the SINR threshold for data detection required by D2D receiver, and the noise is neglected.

The expression shows that the coverage probability of D2D user d_i is meanly decided by following factors: 1) the transmit power ratio between cellular user and D2D user $\frac{P_c}{P_d}$, 2) the SINR threshold for data detection required by D2D receiver T_d, 3) D2D pair density λ_d, 4) ρ_{d_i,d_i} the distance of D2D pair d_i.

The transmission rate of D2D user is given by

$$R_{d_i} = \int_0^\infty \frac{\overline{P}^{d_i}_{cov}(x)}{(1+x)\ln 2} dx. \tag{14}$$

Theorem 2: If the receiver noise is negligible, the social trust coverage probability of D2D user d_i is given as

$$\begin{aligned} &\overline{P}^{d_i}_{cov,s}(T_s) \\ &= \exp\left(-2\pi p_e \lambda_d \int_0^R L_{d-d}(s_z) L_{d-c}(s_z) \rho_{d_i,z} d\rho_{d_i,z}\right) \\ &\quad \times \left(1 - \left(\int_0^{2R} \exp\left(-\frac{\pi\lambda_d T_s^\delta \rho^2_{d_i,c}}{\text{sinc}(\delta)}\right) f(\rho_{d_i,c}) d\rho_{d_i,c}\right)\right), \end{aligned} \tag{15}$$

where

$$L_{I_{d-d}}(s_z) = \exp\left(-\frac{\pi\lambda_d T_s^\delta \rho^2_{d_i,z}}{\text{sinc}(\delta)}\right), \tag{16}$$

$$L_{I_{d-c}}(s_z) = 1\Big/\left(1 + \left(\frac{P_c}{P_d}T_s\right)^\delta \frac{\rho^2_{d_i,z}}{\left(\frac{128R}{45\pi}\right)^2}\right), \tag{17}$$

and for $1 \le \rho_{d_i,c} \le 2R$,

$$f(\rho_{d_i,c}) = \frac{2\rho_{d_i,c}}{R^2}\left(\frac{2}{\pi}\cos^{-1}\left(\frac{\rho_{d_i,c}}{2R}\right) - \frac{\rho_{d_i,c}}{\pi R}\sqrt{1-\frac{\rho^2_{d_i,c}}{4R^2}}\right). \tag{18}$$

The expression shows that the social trust coverage probability of D2D user d_i is meanly affected by following factors: 1) the transmit power ratio between cellular user and D2D user $\frac{P_c}{P_d}$, 2) SINR requirement for eavesdropper to intercept the signal correctly T_s, 3) D2D pair density λ_d, 4) $\rho_{d_i,c}$ the distance between D2D pair d_i and cellular user c, 5) the probability to intercept p_e. Different from coverage probability of D2D user d_i, the social trust coverage probability of D2D user d_i is affected by the probability to intercept p_e, which is decided by social-link probability.

Proof: See Appendix B.

The intercepted rate of D2D user can then be obtained as

$$\begin{aligned} R^e_{d_i} &= \int_0^\infty \frac{\mathbb{P}\left[\max\limits_{d'\in\mathcal{D}_{d_i,e}} \gamma_{d_i,d'} \ge x\right]}{(1+x)\ln 2} dx \\ &= \int_0^\infty \frac{1}{(1+x)\ln 2}\left(1 - \overline{P}^{d}_{cov,s}\right) dx, \end{aligned} \tag{19}$$

and we have $R^s_{d_i} = \max\left\{R_{d_i} - R^e_{d_i}, 0\right\}, \forall d \in \mathcal{D}$.

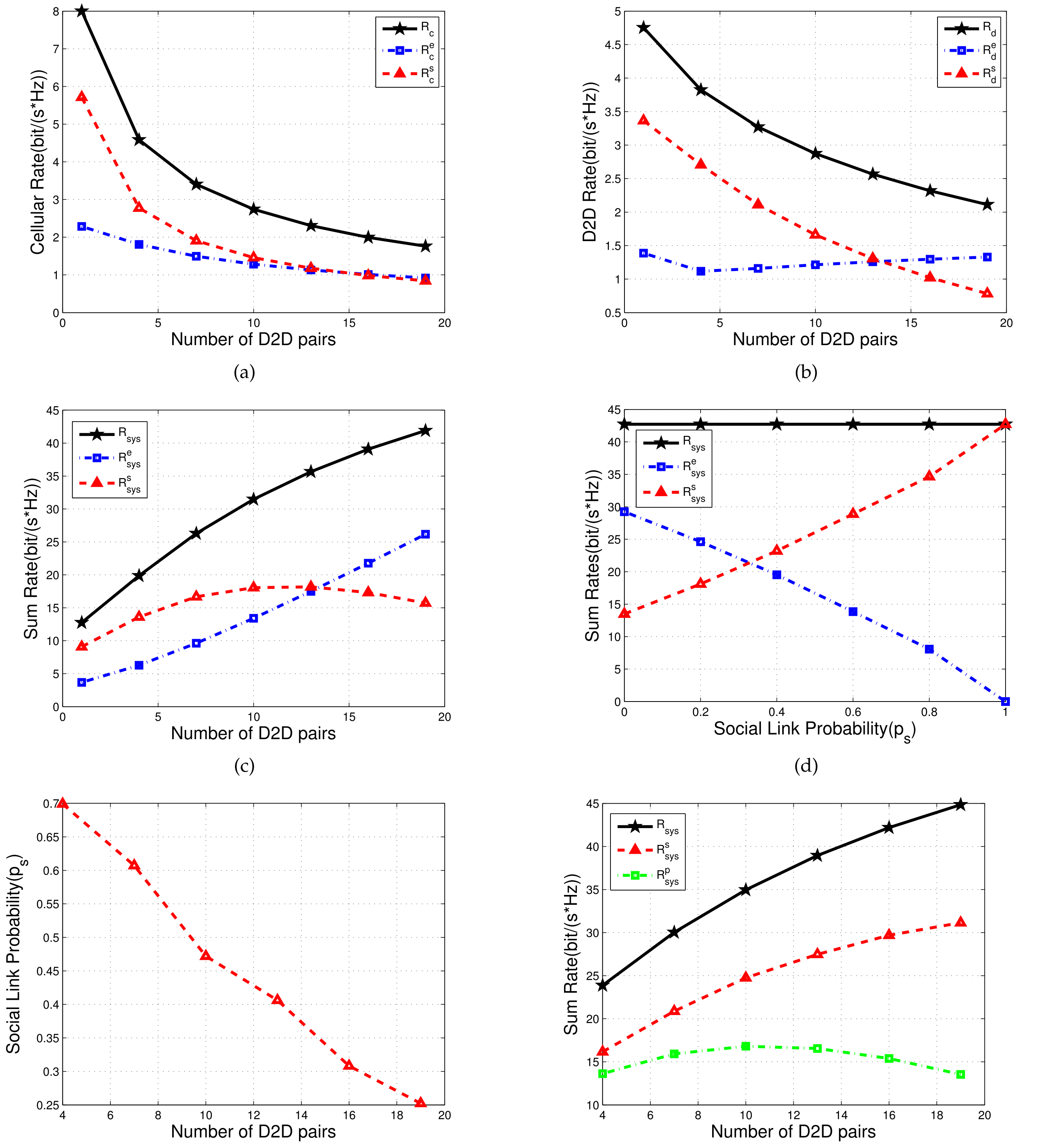
Given the average intercepted rate R^e_d, the average secrecy rate R^s_d and the average transmission rate R_d of typical D2D pair, we have the following theorem.

Theorem 3: The system secrecy rate $R^s_{\text{sys}} = R^s_c + \lambda_d \pi R^2 \cdot R^s_d$, the system intercepted rate $R^e_{\text{sys}} = R^e_c + \lambda_d \pi R^2 \cdot R^e_d$, and the system transmission rate $R_{\text{sys}} = R_c + \lambda_d \pi R^2 \cdot R_d$.

Proof: The system secrecy rate can be derived by adding the cellular user and D2D users as:

$$R^s_{\text{sys}} = R^s_c + \mathbb{E}_{\Phi_d}\left[\sum_{d_i\in\mathcal{D}} R^s_{d_i}\right] = R^s_c + \lambda_d \pi R^2 \cdot R^s_d \tag{20}$$

Similarly, we can obtain R^e_{sys} and R_{sys}. □



(a)

(b)

(c)

(d)

(e)

(f)

Fig. 3. Performance analysis via stochastic geometry: (a) secrecy rate of cellular user, (b) secrecy rate of D2D user, (c) sum secrecy rate of cellular user and all D2D users, (d) relationship between sum secrecy rate and social link probability, (e) social trust based on real dataset, and (f) social trust performance of real social trust.

C. Numerical Results

To evaluate the impact of D2D density and social link probability on secrecy rate, we set the simulation parameters as $P_c = 100\,\text{mW}$, $P_d = 0.4\,\text{mW}$, $R = 500\,\text{m}$, and $\alpha = 4$. The maximum transmission distance of D2D pair is 50 m. We first evaluate the performances of social oblivious mechanism by setting $p_s = 0$. It can be observed from Fig. 3 (a) and (b) that the secrecy rates R_c^s and R_d^s decrease quickly as λ_d increases, while the intercepted rates R_c^e and R_d^e are affected slightly by changing λ_d. For example, when the number of D2D pairs is 16, average secrecy rate of cellular user and D2D pair decreases about 80% and 70%, respectively. Also the transmission rates R_c and R_d decrease with the increase of λ_d. The reason is that larger number of D2D users introduces more interferences. At the same time, the number of potential eavesdroppers increases. Therefore, the intercepted rate changes slightly, and the secrecy rate drops sharply.

From Fig. 3 (c), it can be seen that the system or sum secrecy rate R^s_{sys} first increases with the increase of D2D users, and it starts to decrease when the number of D2D users is larger than 10. This is because the system intercepted rate R^e_{sys} is increasing faster than the sum transmission rate R_{sys}, when the number of D2D users is larger than 10. Although system transmission rate increases with the number of D2D pairs, sum secrecy rate decreases at some point, which is important for system design. Then we evaluate the impact of social link probability. With 20 D2D users, the relationship between the system secrecy rate and p_s is shown in Fig. 3(d). The system transmission rate does not change with different social link probability since it is irrelevant to social trust. With higher social link probability, system intercepted rate decreases while system secrecy rate increases. This is because high social trust contains more trusted relationships and fewer potential eavesdroppers in the network. It can be seen that the system secrecy rate increases about 200% when p_s increases from 0 to 1. This proves that considering social trust decreases the system intercepted rate and increases system secrecy rate significantly.

Furthermore, we utilize the social trust relations from the real dataset of Brightkite [33], which uses undirected edges to represent friendships. We obtain the average number of social edges of one user to represent the social link probability p_s, as depicted in Fig. 3 (e), which is used to obtain the system secrecy rate R^s_{sys} in Fig. 3 (f). In Fig. 3 (e), it is observed that social link probability decreases with increasement of the number of D2D pairs. In Fig. 3 (f), R^p_{sys} is the system secrecy rate without considering social trust. Clearly, our proposed social D2D communication security mechanism dramatically enhances the system secrecy rate, and R^s_{sys} outperforms R^p_{sys} by about 63% on average. Actually, this analysis method considering social trust can get a better result close to reality.

V. Matching Theory for Resource Allocation

We provide the solution to maximize the secrecy rate, which yields efficient resource allocation needed to utilize the social trust in order to attain the theoretical performance gains.

A. Problem Formulation

1) Secrecy Rate of Cellular User c: Let the set of cellular users be $\mathcal{C}$. To distinguish with the previous single cellular user scenario, we use R'_c, $R^{e'}_c$ and $R^{s'}_c$ to denote the uplink channel rate, intercepted rate and secrecy channel rate of cellular user $c \in \mathcal{C}$, respectively. Let binary $x_{c,d}$ denote the spectrum sharing relationship between cellular users and D2D users, namely, $x_{c,d} = 1$ indicates D2D user d occupies the spectrum resource of cellular user c; otherwise $x_{c,d} = 0$. The collection of eavesdroppers for $c \in \mathcal{C}$, denoted by $\mathcal{D}'_{c,e}$, is given by $\mathcal{D}'_{c,e} = \{d' | x_{c,d'} \cdot (1 - \omega_{c,d'}) = 1, \forall d' \in \mathcal{D}\}$, which indicates that the number of potential eavesdroppers is jointly determined by spectrum sharing and social trust relationships.

The interference at the cellular users c is incurred from the D2D pairs sharing the same spectrum resource with c and can be calculated as $\sum\limits_{d\in\mathcal{D}} x_{c,d}P_d\rho_{d,b}^{-\alpha}|h_0|^2$. The uplink channel rate of the cellular user c is

$$R'_c = \log_2\left(1 + \frac{P_c\rho_{c,b}^{-\alpha}|h_0|^2}{\sum\limits_{d\in\mathcal{D}} x_{c,d}P_d\rho_{d,b}^{-\alpha}|h_0|^2 + N_0}\right). \tag{21}$$

The potential eavesdropper of $d^0 \in \mathcal{D}'_{c,e}$ shares the same spectrum resource of c. Therefore, the interferences at d^0 can be calculated as $\sum\limits_{d\in\mathcal{D}\backslash\{d^0\}} x_{c,d}P_d\rho_{d,d^0}^{-\alpha}|h_0|^2$. The intercepted rate of c by the eavesdroppers is

$$R^{e'}_c = \max_{d^0\in\mathcal{D}'_{c,e}} \log_2\left(1 + \frac{P_c\rho_{c,d^0}^{-\alpha}|h_0|^2}{\sum\limits_{d\in\mathcal{D}\backslash\{d^0\}} x_{c,d}P_d\rho_{d,d^0}^{-\alpha}|h_0|^2 + N_0}\right). \tag{22}$$

The secrecy channel rate of the cellular user c is $R^{s'}_c = \max\left\{R'_c - R^{e'}_c, 0\right\}$.

2) Secrecy Rate of D2D Pair d: The collection of eavesdroppers for D2D user $d \in \mathcal{D}$, denoted by $\mathcal{D}'_{d,e}$, consisting of cellular users and D2D users, is given by $\mathcal{D}'_{d,e} = \{c | x_{c,d} \cdot (1 - \omega_{c,d}) = 1, \forall c \in \mathcal{C}\} \cup \{d' | y_{d',d} \cdot (1 - \omega_{d',d}) = 1, \forall d' \in \mathcal{D}\}$, where $y_{d,d'} = 1$ if and only if $\exists c \in \mathcal{C} : x_{c,d} = 1$, $x_{c,d'} = 1$; otherwise, $y_{d,d'} = 0$. To show the difference with the single cellular user scenario, we use R'_d, $R^{e'}_d$ and $R^{s'}_d$ to denote the channel rate, intercepted rate and secrecy channel rate of the D2D user d, respectively.

The interferences at D2D pair d are incurred by the cellular users and D2D users, which share the same spectrum resource with d. These interferences can be depicted as $I^c_d + \sum\limits_{d'\in\mathcal{D}\backslash\{d\}} y_{d,d'}P_{d'}\rho_{d',d}^{-\alpha}|h_0|^2$, where $I^c_d = \sum\limits_{c\in\mathcal{C}} x_{c,d}P_c\rho_{c,d}^{-\alpha}|h_0|^2$. The channel rate of D2D pair d is

$$R'_d = \log_2\left(1 + \frac{P_d\rho_{d,d}^{-\alpha}|h_0|^2}{I^c_d + \sum\limits_{d'\in\mathcal{D}\backslash\{d\}} y_{d,d'}P_{d'}\rho_{d',d}^{-\alpha}|h_0|^2 + N_0}\right). \tag{23}$$

When the eavesdropper $d^0 \in \mathcal{D}'_{d,e}$ is D2D pair, the interferences at d^0 can be calculated as $I^c_d + \sum\limits_{d'\in\mathcal{D}\backslash\{d,d^0\}} y_{d,d'}P_{d'}\rho_{d',d^0}^{-\alpha}|h_0|^2$. When d^0 represents cellular user, the interference from other cellular users equals to 0, i.e., $I^c_d = 0$. The intercepted rate of d by the eavesdroppers is

$$R^{e'}_d = \max_{d^0\in\mathcal{D}'_{d,e}} \log_2\left(1 + \frac{P_d\rho_{d,d^0}^{-\alpha}|h_0|^2}{I^c_d + \sum\limits_{d'\in\mathcal{D}\backslash\{d,d^0\}} y_{d,d'}P_{d'}\rho_{d',d^0}^{-\alpha}|h_0|^2 + N_0}\right). \tag{24}$$

The secrecy rate of D2D user d is $R^{s'}_d = \max\left\{R'_d - R^{e'}_d, 0\right\}$.

Combining the results of Subsections V-A.1 and V-A.2, we obtain the system social trust rate as

$$\Re(\mathbf{X})=\sum_{c\in\mathcal{C}}\left(R_c^{s'}+\sum_{d\in\mathcal{D}}x_{c,d}R_d^{s'}\right), \tag{25}$$

where $\mathbf{X}$ is the matrix of $x_{c,d}$, $\forall c \in \mathcal{C}, d \in \mathcal{D}$. Thus, we can formulate the optimal resource allocation for social trust communications as the following optimization problem:

$$\max_{x_{c,d},\ \forall c\in\mathcal{C},\ d\in\mathcal{D}} \Re(\mathbf{X}),$$
$$\text{s.t.} \begin{cases} x_{c,d}\in\{0,1\}, \quad \forall c\in\mathcal{C}, d\in\mathcal{D};\\ \sum\limits_{c\in\mathcal{C}} x_{c,d}\leq 1, \forall d\in\mathcal{D};\\ R_c^{s'}\geq \bar{R}_c, \forall c\in\mathcal{C}. \end{cases} \tag{26}$$

The second constraint is imposed since each D2D pair can only occupy one cellular user's resource, and the third constraint guarantees the minimum secrecy rate $\overline{R}_c$, required by each cellular user to guarantee its quality of service (QoS).

Lemma 1: The optimization problem (26) is NP-hard.

Proof: See Appendix C.

From Lemma 1, it is observed that the optimization problem (26) can not be solved by conventional algorithms. The secrecy rate of cellular user and D2D users are determined by both spectrum sharing relationships and social trust information. When one D2D user changes its spectrum sharing strategy, the secrecy rate of other D2D users and cellular users may be impacted significantly. Therefore, we need to adjust the spectrum sharing strategies of D2D users cooperatively to improve system secrecy rate. In the following section, matching game model is used to implement efficient resource allocation.

B. Matching Theory Model

Matching theory is an efficient method to implement resource allocation, which works in a decentralized and self-organizing approach for large-scale networks [29]. Our problem (26) can be regarded as a two-sided many-to-one matching game, where each cellular user $c \in \mathcal{C}$ shares its resource with multiple D2D pairs $d \in \mathcal{D}$. Thus our resource allocation problem can be reformulated as a many-to-one matching, denoted by the tuple $(\mathcal{C}, \mathcal{D}, \succ_{\mathcal{C}}, \succ_{\mathcal{D}})$, where $\succ_{\mathcal{C}}= \{\succ_c\}_{c\in\mathcal{C}}$ and $\succ_{\mathcal{D}}= \{\succ_d\}_{d\in\mathcal{D}}$ denote the sets of preference of cellular users and D2D pairs, respectively. The matching between cellular users and D2D pairs can be defined as follows.

Definition 5: Matching of social trust resource allocation: A many-to-one social trust matching M is defined as a function from the set $\mathcal{C}\cup\mathcal{D}$ onto the set of $\mathcal{C}\cup\mathcal{D}$ such that $c = M(d)$ if and only if $d \in M(c)$.

Each D2D user aims to improve its social trust rate, and the utility of D2D user d is defined as its social secrecy rate $U_d(M) = R_d^{s'}$. From the expression of $R_d^{s'}$, we observe that $U_d(M)$ depends on the matching of other players, which demonstrates peer effects for matching. The utility of cellular user c is defined as its social secrecy rate

$$U_c(M)=R_c^{s'}+\sum_{d\in M(c)}R_d^{s'},$$

which indicates that c aims to increase the sum secrecy rate of all users that occupy the same spectrum resource with it. From the utility definition, it is observed that each D2D user occupies the spectrum resource of cellular user without considering the other D2D users and cellular users. While the cellular user prefers to accept the D2D user, which maximizes the whole secrecy rate of all users sharing the same spectrum resource with this cellular user.

Definition 6: Preference of cellular user: Cellular user c prefers d to d', if $U_c(M) > U_c(M')$, denoted by $d \succ_c d'$, where $M' = M \setminus \{(c, d)\} \cup \{(c, d')\}$ for $c \in \mathcal{C}$, $d, d' \in \mathcal{D}$.

Definition 7: Preference of D2D pair: D2D pair d prefers c to c', if $U_d(M) > U_d(M')$, denoted by $c \succ_d c'$, where $M' = M \setminus \{(c, d)\} \cup \{(c', d)\}$, for $d \in \mathcal{D}$, $c, c' \in \mathcal{C}$.

Given the above defined matching model for social trust transmission, we aim to find a stable matching.

Definition 8: Stable matching: A matching M is stable if and only if there is no blocking pair. A pair $(c, d) \notin M$ is regarded as a blocking pair for the matching M, if there is another matching $M' = M \setminus \{(M(d), d)\} \cup \{(c, d)\}$, where $M' \succ_c M$, $M' \succ_{M(d)} M$ and $M' \succ_d M$.

For the established matching model for resource allocation, a stable matching indicates that no cellular user or D2D user would benefit from replacing their current association relation. From the utility definition, it can be seen that cellular users and D2D users may change their preferences as the game evolves. During the evolution of matching game, the utility of each player may change due to mutual interference and social trust. Therefore, the preference of each player is also varying, which incurs peer effects [28]. From the above analysis, we can see that the proposed social trust matching cannot be obtained based on the traditional deferred acceptance algorithm [28]. Therefore, we need to design an efficient mechanism to obtain a stable matching.

Now, we analyze the property of the stable matching qualitatively, which gives the intuition to design our proposed algorithm. If there is blocking pair (c, d) of matching M, the new matching $M' = M \setminus \{(M(d), d)\} \cup \{(c, d)\}$ is able to increase system secrecy rate under the stable condition in Definition 8. In other words, a stable matching achieves the local optimum of system sum secrecy rate $\Re(\mathbf{X})$, which can be utilized to obtain the stable matching. On the other hand, as the optimization problem (26) is the binary integer programming problem, an global optimum matching M^{opt} can be obtained by exhaustive search. From the above analysis, M^{opt} is the stable matching. Therefore, there is at least one stable matching for our proposed matching game model.

C. Algorithm and Solution

We propose a two-stage algorithm to achieve stable matching, as listed in Algorithm 1. In Stage I, we obtain the initial stable matching, which is then modified to increase system secrecy rate in Stage II.

1) Stage I (Initial Stable Matching): D2D users with their initialized preference list based on their utility are put into the matching queue. Then we randomly select D2D user d from the matching queue, who requests to occupy the resource of its most preferred cellular user c'. Whether to

Algorithm 1 Proposed Social Trust Matching

```
Input: D2D users' preference list $\mathcal{PL}^d$ and cellular
users' minimum secrecy rate $\overline{R}_c$;
Output: The stable matching $M_{fin}$;
Initialize:
    D2D user matching queue length: $n \leftarrow D$;
    $stop \leftarrow false$;
Stage I. Initial Stable Matching:
while $n \geq 1$ do
    for  k=1,...,C do
        $c' = \mathcal{PL}^d[k]$; $x_{c',d} = 1, d \in \mathcal{D}$;
        if $R^{s'}_{c'} < \overline{R_{c'}}$ or $\mathcal{D}_{c'}$ is not stable then
            $x_{c',d} = 0$; $x_{c_0,d} = 1$;
        else
            break;
    $n = n - 1$;
Obtain initial stable matching $M_{ini}$;
Stage II. Best Response Based Matching:
Set the current matching as $M_{cur} \leftarrow M_{ini}$;
while $stop == false$ do
    Uniformly randomly choose one D2D user $i$;
    Choose the local best response $x'_i$ according to (27),
    and update the $M$ with $M'$;
    if $\mathcal{R}(M') > \mathcal{R}(M)$ then
        Update $M_{cur} \leftarrow M'$;
    if Matching $M$ remains unchanged for two
    consecutive operations then
        $stop \leftarrow true$;
Return The stable matching $M_{fin} \leftarrow M_{cur}$.
```

accept this request is determined by two aspects. Firstly, c' needs to guarantee its secrecy rate $\overline{R}_{c'}$ and secondly, c' must guarantee the stable matching of the other D2D users $\mathcal{D}_{c'}$ that are already associated with it. If cellular user c' refuses to accept the application, d is mapped with empty resource c_0. Then, d would be removed from the matching queue. The above operations are repeated until the matching queue is empty.

2) Stage II (Best Response Based Iteration): Although the initial stable matching found in Stage I does not exist block pair, it may not be the optimally stable matching that maximizes the system social secrecy rate. Therefore, we need to adjust this initial stable matching to improve the system secrecy rate. From Definition 8, we have the following observation.

Lemma 2: All local optimum points of $\mathfrak{R}$ are stable matching.

Proof: See Appendix D.

In the light of Lemma 2, we need to adjust the initial matching into a local maximum. The strategy of D2D user i, denoted by x_i, represents the cellular user of which D2D user i occupies the same spectrum resource. The best response of D2D user i is defined as follows:

$$x_i^* = \arg\max_{c \in \mathcal{C}} U_c(M') + U_{M(i)}(M'), \tag{27}$$

TABLE I

MAIN SIMULATION PARAMETERS

Parameter	Value
Radius of cell	500 m
Noise spectral density	-174 dBm/Hz
Maximum distance of D2D	80 m
Transmission power of cellular user	200 mW
Transmission power of D2D user	1 mW

where $M' = M \setminus \{(c, M(c))\} \cup \{(c, i)\}$. We propose an iterative algorithm to obtain a local optimal stable matching, as listed in Stage II of Algorithm 1. The local best response of i is adopted to select its associated partner. When the current sum secrecy rate is larger than the initial matching, the new matching is maintained, and M is updated by M'. After a finite number of iterations, the matching converges to a local optimal stable matching M_{fin}.

D. Stability and Convergence

We now analyze the convergence and stability properties of Algorithm 1 in the following theorem.

Theorem 4: Starting from any initial stable matching M_{ini}, Algorithm 1 always converges to a stable matching M_{fin}.

Proof: See appendix E.

VI. Performance Evaluation

We evaluate the performance of the proposed matching algorithm for social trust D2D communications based on a real dataset and a large-scale simulated network. The main parameters in our simulation are listed in Table I, which is based on the reference of [25]. We uniformly and randomly distribute the cellular users and D2D users within the coverage of the BS. In particular, the transmitter of D2D link is randomly distributed in the coverage of BS, and its corresponding receiver is randomly distributed in the circle of the transmitter with the maximum distance. According to the solution of proposed matching algorithm, we evaluate the following two performance metrics:

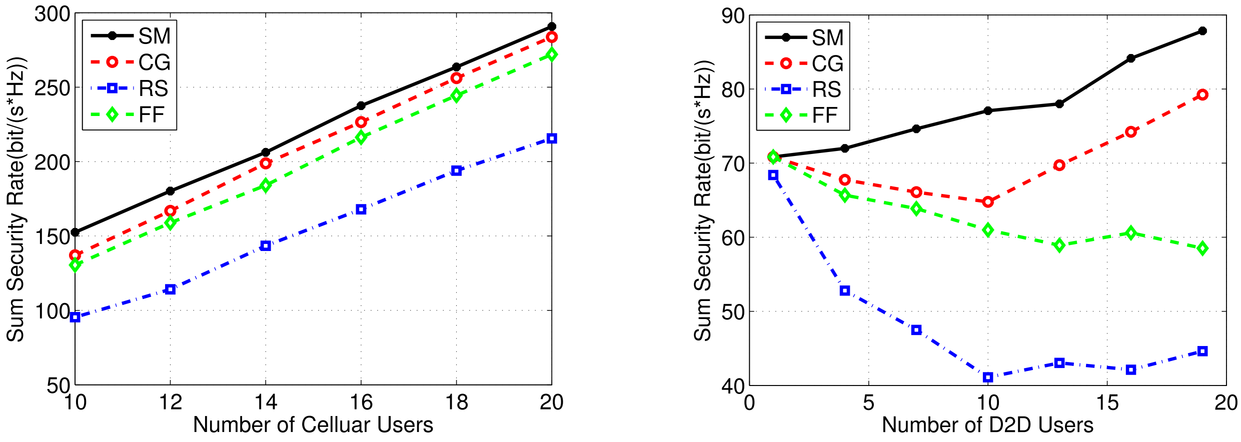
1) System sum secrecy rate, which is determined by all the D2D users, the cellular users and the social trust among them.
2) The Jain's fairness measure [35], which determines whether the receivers of D2D and cellular users are receiving the fair share of the system resources.

In order to demonstrate the effectiveness of our stable matching algorithm, we compare the performance of our scheme, denoted as Stable Matching (SM), with the following schemes.

a) Coalition Game (CG). It utilizes the coalition formation game to allocate the spectrum resources to D2D users [32]. This distributed algorithm achieves the near-optimal solution of the system secrecy rate without considering social trust information and is the current state-of-the-art solution.

b) Furthest First (FF). It allocates the D2D communication resources with the resources of the cellular users that are furthest away from the D2D users.

c) Random Selection (RS). It uniformly and randomly allocates the communication resources to the D2D users.



(a)

(b)

Fig. 4. Comparison of system performance in a real dataset. (a) Cellular users. (b) D2D users.

A. System Social Trust Rate

We first set up the simulation based on the social trust relations obtained from the real dataset of Brightkite [33]. The dataset Brightkite is the check-in data between Apr. 2008 to Oct. 2010, and the total number of check-ins is 4.5 million. Brightkite contains an explicit social network, which is utilized by our paper. We first estimate the social link probability, which is illustrated in Fig. 3 (e). Then, the social trust among cellular users and D2D users are generated in each simulation scenario randomly based on the social link probability.

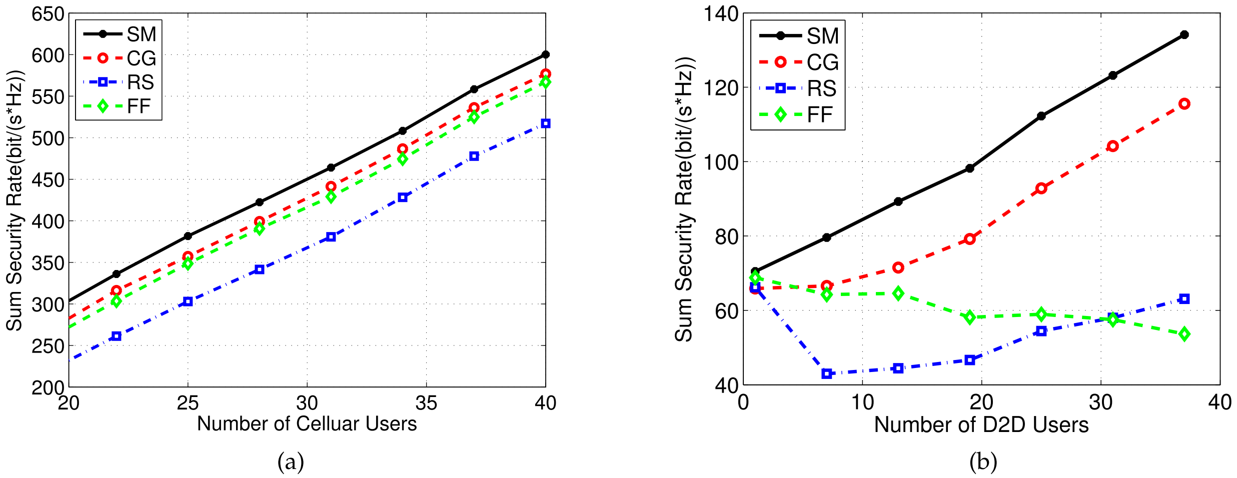
Fig. 4 compares the system secrecy rate attained by our proposed SM scheme with those of the three benchmark schemes. In Fig. 4 (a), the number of D2D pairs is set to be 10, and the number of cellular users varies from 10 to 20. Larger number of cellular users lead to better system performance since more cellular users offer more spectrum resources to share. It is observed that RS has the worst performances, as it does not consider the mutual inferences and utilize the social trust. Compared with RS, our SM increases sum secrecy rate about 50%. It also can be seen that our SM outperforms the CG considerably.

In Fig. 4 (b), the number of cellular user is set to be 5, and the number of D2D pairs varies from 1 to 20. It is observed that sum secrecy rate of CG, FF and RS decreases when the number of D2D pairs is less than 10. At this period, social trust plays important role in calculating sum secrecy rate due to small interference. And CG, FF and RS cannot utilize this information. When the number of D2D pairs is above 10, mutual interference plays important role for system secrecy rate. Therefore, sum secrecy rate of CG and RS increases with the number of D2D pairs. When the number of D2D pairs equals to 10, SM outperforms RS about 90%. From Fig. 4, SM not only considers mutual interferences but also utilizes social trust information. Therefore, SM perform best among these resource allocation algorithms. It is noticed that both FF and RS are fluctuant when the number of D2D pairs is larger than 10. Actually, the fluctuation happens to all the four methods in the figure. This is because the evaluation randomly distributes the cellular users and D2D users within the coverage of the base station. In particular, the transmitter of D2D link is randomly distributed in the coverage of BS, and its corresponding receiver is randomly distributed in the circle of the transmitter with the maximum distance. As a result, the system secrecy rate shows the fluctuant trend. Since SM and CG have obvious increasing trend, the large trend covers the fluctuation.

We also simulate a large-scale network with the social link probability $p_s = 0.8$. Fig. 5 compares the system secrecy rate of our SM scheme with those of the three benchmark schemes. In Fig. 5 (a), the number of D2D pairs is 10, and the number of cellular users varies from 20 to 40. This scenario represents the sufficient spectrum resources, where there may be no interference among D2D users. In Fig. 5 (b), the number of cellular users is 5, and the number of D2D pairs varies from 0 to 40. When the number of D2D users is less than 10, social trust plays important role in calculating sum secrecy rate due to small interference. As a result, sum secrecy rates of FF and RS decrease. Sum secrecy rates of CG does not change a lot. When the number of D2D users is above 10, both social trust and mutual interference need to be utilized to calculate sum secrecy rate. Sum secrecy rates of CG and RS increase with the number of D2D pairs. In addition, FF only considers interference of each D2D pair and performs worse than RS when the number of D2D pairs is above 30. Clearly, our SM attains the best performance among all the algorithms evaluated. For example, with 20 D2D pairs, our SM increases the sum secrecy rate by about 25%, compared with the current state-of-the-art CG, as can be seen from Fig. 5 (b). Similar to Fig. 4(b), both FF and RS are fluctuant when the number of D2D pairs is also larger than 10, which is caused by the same reason.

B. Impact of Social Link Probability

To observe the impact of the social link probability on the system secrecy rate, we set the numbers of cellular users and D2D pairs to be 5 and 20, respectively. Fig. 6 depicts the system secrecy rate as the functions of the social link probability for the three different approaches, where the Social Trust



(a)

(b)

Fig. 5. Comparison of system performance in a large-scale simulated network. (a) Cellular users. (b) D2D users.

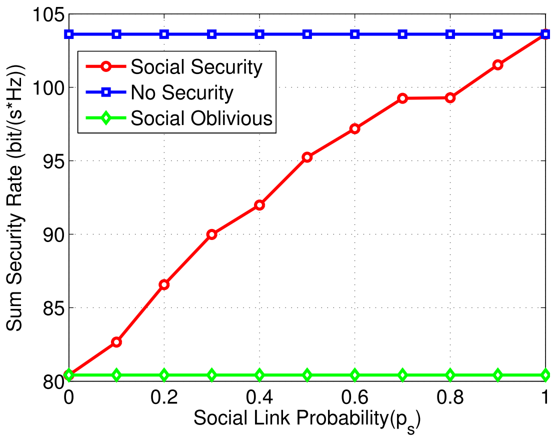


Fig. 6. Performance of system secrecy rate as the functions of social link probability obtained by various approaches.

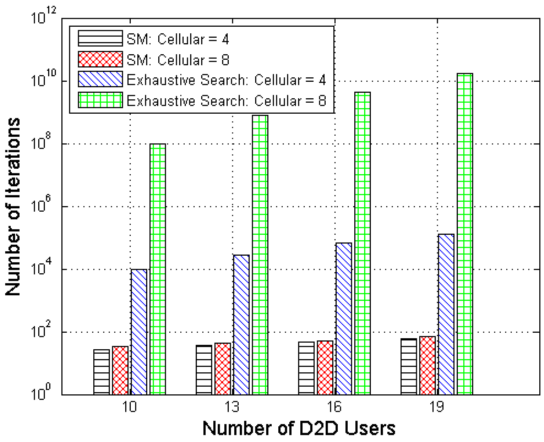


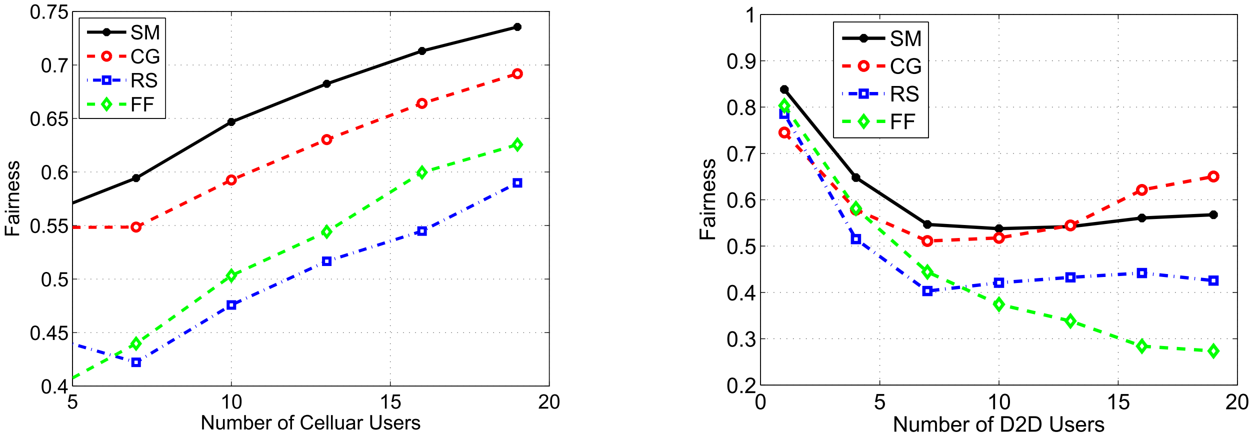
Fig. 7. Comparison of the convergence rates, in terms of the average number of iterations, required by our SM algorithm and the exhaustive search.

denotes our SM approach, while the No Security approach corresponds to the 'best' case that cellular users and D2D users all trust each other and there is no need to consider security transmissions, and the Social Oblivious approach represents the 'worst' case that cellular users and D2D users are social oblivious and they do not trust each other at all. In reality scenarios, social trust information exists among cellular user and D2D users. Therefore, Social Trust is utilized to exploit this basic relationships.

For each simulation scenario, we generate social trust relationship among cellular users and D2D users based on ps values randomly. With $p_s = 0$, the system secrecy rate of our SM approach have the smallest value equal to that of the Social Oblivious approach, as in this situation no trusted relationship exists between cellular users and D2D users. Thus, each user is the potential eavesdropper of the transmission of other users. With $p_s = 1$, the SM approach attains the maximum system secrecy rate, as all cellular users and D2D users trust each other. The system secrecy rate shows a near linear growth with social link probability increasing from 0 to 1. Compared to the Social Oblivious approach, our SM increases the system secrecy rate by about 28% at $p_s = 1$. This demonstrated that SM approach brings system secrecy rate gain by jointly considering social trust information and mutual interference in resource allocation.

C. Computation Complexity

To investigate the computation complexity and convergence rate of our proposed SM algorithm, we vary the number of D2D user D and check how iteration number changes. We set the number of cellular users to be 4 and 8, respectively, to check the influence of the cellular user number. Iteration number of the exhaustive search method is also calculated as a comparison. The average number of iterations required by the SM algorithm to converge to the final matching is shown in Fig. 7, in comparison to that required by the exhaustive search. The average number of iterations increases linearly by our algorithm to find the solution as D increases. By contrast, the exhaustive search needs 8^D iterations to find the optimal solution with 8 cellular users. Compared with the exhaustive search, our SM algorithm reduces the computation complexity dramatically.



(a)

(b)

Fig. 8. Illustration of system fairness by varying the number of cellular users and D2D users. (a) Cellular users. (b) D2D users.

D. System Fairness

To obtain some insights on how the secrecy data transmission is actually shared among the D2D users and cellular users, we depict the Jain's fairness index of in Fig. 8 with the variation of the number cellular users and D2D users, respectively. We observe that changing the number of D2D users has a non-obvious influence on the fairness of data transmission under these schemes. Among all these compared schemes, we can obtain that SM has the best fairness resource sharing among the the cellular users and D2D users.

VII. Discussion and Future Work

Several aspects of our social trust aided D2D communication architecture warrant further discussion and may lead to extensions.

We model the social trust in this paper with binary value, where 1 and 0 represent trust and non-trust relationship respectively. To define the social trust more exact, we need to model the social trust as a probability. Furthermore, this probability may change over time, since a friend might be transformed as a foe under some conditions. It will be interesting to investigate how the probability transformation affects the whole system performance. The new social trust model leads to several interesting questions to be investigated: 1) what probability distribution is suitable to describe social trust? 2) how does this probability distribution evolve over time? 3) how to decide the threshold to trust? 4) what is the suitable resource allocation scheme? We will investigate these questions in our future work.

To investigate the tradeoff between security and efficiency for D2D transmissions, this paper focuses on spectrum-sharing between cellular users and D2D users. Therefore, only social trust relationships between cellular users and D2D users are considered. The spectrum-sharing between cellular users can adopt different methods defined for 5G, including spectrum aggregation, radio aggregation, tiered sharing etc. It will be interesting that a more general scenario is considered, where cellular users also share the spectrum with each other. In this case, the social trust between cellular users should also be taken into consideration for resource allocations.

This paper considers both uplink and downlink cellular traffic. In 3GPP, uplink spectrum usage is relatively smaller than downlink spectrum usage. As a result, there exists more available uplink spectrum to share with D2D users. Therefore, we only consider sharing uplink spectrum with D2D users. In our future work, we will consider spectrum sharing on both downlink and uplink cellular traffic. The system secrecy rate will have a different form, which requires a new resource allocation scheme.

VIII. Conclusion

This paper has proposed the novel idea of social trust aided D2D communication underlaying cellular networks. We have quantitatively analyzed the impact of social trust on the social secrecy rate utilizing stochastic theory. It has been observed that the system secrecy rate increases by about 63% when considering social trust relations based on a real dataset. We have also used matching theory to allocate the resources of multiple cellular users to D2D users efficiently, which increases the system secrecy rate by about 28%, compared to the social oblivious approach. This study has opened a new paradigm for designing security D2D communications and has provided effective implementation mechanism for realizing social trust aided D2D communications.

Appendix A
Proof of Theorem 1

Proof: From Eq. (3), $\overline{P}^{c}_{cov,s}(T_s)$ can be derived as follows:

$$\begin{aligned}
&\overline{P}^{c}_{cov,s}(T_s)\\
&\quad = \mathbb{P}\Big(\max_{d'\in\mathcal{D}_{c,e}} \gamma_{c,d'} \le T_s\Big)\\
&\quad = \mathbb{P}\left(\bigcap_{z\in\Phi_e} \gamma_{c,z} \le T_s\right)\\
&\quad = \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(\gamma_{c,z} \le T_s\right)\right]
\end{aligned}$$

$$
\begin{aligned}
&\overset{(a)}{=} \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(1-\exp\left(-P_c^{-1}T_s\rho_{c,z}^{\alpha}\left(\sigma^2+I_d(z)\right)\right)\right)\right]\\
&= \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(1-\exp\left(-P_c^{-1}T_s\rho_{c,z}^{\alpha}\left(I_d(z)\right)\right)\right)\right]\\
&\overset{(b)}{=} \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(1-L_{I_d(z)}\left(-P_c^{-1}T_s\rho_{c,z}^{\alpha}\right)\right)\right]\\
&\overset{(c)}{=} \exp\left(-2\pi p_e\lambda_d\int_0^R L_{I_d(z)}\left(-P_c^{-1}T_s\rho_{0,z}^{\alpha}\right)\rho_{c,z}d\rho_{c,z}\right),
\end{aligned}
\tag{28}
$$

where $I_d(z)$ is the interferences at z incurred by the other D2D users following the PPP Φ_d, and $\mathbb{E}_{\Phi_d}[\,]$ denotes the expectation with respect to Φ_d. According to the thinning property of PPP, potential eavesdroppers follow a PPP, denoted by Φ_e, with density $p_e\lambda_d$. Equality (a) comes from the fact that $|h_0|^2$ is exponentially distributed, equality (b) uses the results that $L_X(s)=\mathbb{E}[\exp(-sX)]$ and the receiver noise variance σ^2 is 0, while equality (c) follows from the probability generating functional of PPP [27]. It should be noted that $I_d(z)$ can be replaced by I_d, because the distribution of PPP is unaffected by translation. $L_{I_d}(s)$ is given by [25]:

$$
L_{I_d}(s)=\exp\left(-\frac{\pi\lambda_d P_d^{\delta}s^{\delta}}{\mathrm{sinc}(\delta)}\right),
\tag{29}
$$

where $s=P_c^{-1}T_s\rho_{c,z}^{\alpha}$. Substituting (29) into (28) leads to (8). □

Appendix B
Proof of Theorem 2

Proof: The secrecy coverage probability of D2D user d_i can be expressed as

$$
\begin{aligned}
\overline{P}_{cov,s}^{d_i}(T_s) &= \mathbb{P}\left[\max_{z\in\Phi_e\cup\{c\}}\gamma_{d_i,z}^{e}<T_s\right]\\
&\overset{(a)}{=} \mathbb{P}\left(\max_{z\in\Phi_e}\gamma_{d_i,z}^{e}<T_s\right)\mathbb{P}\left(\gamma_{d_i,c}^{e}<T_s\right).
\end{aligned}
\tag{30}
$$

Equality (a) is because the secrecy probabilities for D2D receivers and cellular user are independent of each other.

The first part of (30) can be expressed as

$$
\begin{aligned}
&\mathbb{P}\left(\max_{z\in\Phi_e}\gamma_{d_i,z}^{e}<T_s\right)\\
&= \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P(\gamma_{d_i,z}<T_s)\right]\\
&\overset{(a)}{=} \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e}\left(1-L_{I_{d(z)}}\left(-P_d^{-1}T_s\rho_{d_i,z}^{\alpha}\right)\right)\right]\\
&= \exp\left(-2\pi p_e\lambda_d\int_0^R L_{I_d(z)}\left(-P_d^{-1}T_s\rho_{d_i,z}^{\alpha}\right)\rho_{d_i,z}d\rho_{d_i,z}\right)\\
&\overset{(b)}{=} \exp\left(-2\pi p_e\lambda_d\int_0^R L_{I_{d-d}(z)}(s_z)L_{I_{d-c}(z)}(s_z)\rho_{d_i,z}d\rho_{d_i,z}\right),
\end{aligned}
\tag{31}
$$

where $s_z=P_d^{-1}T_s\rho_{d_i,z}^{\alpha}$. Equality (a) follows from $\sigma^2=0$, and equality (b) comes from the fact that the interference at eavesdropper is from both other D2D users and cellular user so that the Laplace transformation $L_{I_{d(z)}}(s_z)$ can be divided into two parts:

$$
\begin{aligned}
L_{I_d}(s_z) &= \mathbb{E}\left[\exp\left(-s_zI_d\right)\right]\\
&= E\left[\exp\left(-s_zI_{d-d}\right)\right]E\left[\exp\left(-s_zI_{d-c}\right)\right]\\
&= L_{I_{d-d}}(s_z)L_{I_{d-c}}(s_z).
\end{aligned}
\tag{32}
$$

From [25], we obtain the Laplace transformations, $L_{I_{d-d}}(s_z)$ and $L_{I_{d-c}}(s_z)$, as given in (16) and (17), respectively.

The second part of (30) can be expressed as

$$
\begin{aligned}
\mathbb{P}\left(\gamma_{d_i,c}<T_s\right) &= 1-\mathbb{E}\Big[\exp\left(-P_d^{-1}T_s\rho_{d_i,c}^{\alpha}I_c(z)\right)\Big]\\
&= 1-\mathbb{E}\left[L_{I_c}(s_c)\right],
\end{aligned}
\tag{33}
$$

where $s_c=P_d^{-1}T_s\rho_{d_i,c}^{\alpha}$ and $I_c(z)$ denotes the interferences at c from other D2D users. Then we have the Laplace transformation of $I_c(z)$ as:

$$
L_{I_c}(s_c)=\exp\Big(-\frac{\pi\lambda_d T_s^{\frac{2}{\alpha}}\rho_{d_i,c}^{2}}{\mathrm{sinc}\delta}\Big).
\tag{34}
$$

Thus we have

$$
\begin{aligned}
\mathbb{P}\left(\gamma_{d_i,c}<T_s\right)=1-\int_0^{2R}\exp\left(-\frac{\pi\lambda_d T_s^{\delta}\rho_{d_i,c}^{2}}{\mathrm{sinc}}\right)&\\
\times\ f\big(\rho_{d_i,c}\big)d\rho_{d_i,c},&
\end{aligned}
\tag{35}
$$

where $f\big(\rho_{d_i,c}\big)$ is the probability density function of $\rho_{d_i,c}$ given in (18). By substituting (31) and (35) into (30), we obtain $\overline{P}_{cov,s}^{d_i}$ of (15). □

Appendix C
Proof of Lemma 1

Proof: The optimization objective has no concave properties with $x_{c,d}$. Moreover, it is a binary integer nonlinear programming problem. Therefore, it is NP-hard in general [34]. □

Appendix D
Proof of Lemma 2

Proof: Suppose that (c,d) is a blocking pair of matching M. We have

$$
\begin{aligned}
&\mathfrak{R}(M')-\mathfrak{R}(M)\\
&\quad= U_c(M')+U_{M(d)}(M')-U_c(M)-U_{M(d)}(M).
\end{aligned}
\tag{36}
$$

From Definition 8, we observe that $\mathfrak{R}(M')>\mathfrak{R}(M)$, which indicates that block pair can increase the sum secrecy rate.

Now, suppose that matching M^* is a local maximum point of $\mathfrak{R}$. If M^* is not a stable matching, there exists block pair. But from the above analysis, any block pair of M^* may increase $\mathfrak{R}$, which contradicts the fact that $\mathfrak{R}(M^*)$ is a local maximum value of the system secrecy rate. Therefore, all local optimum points of $\mathfrak{R}$ are stable matching. □

Appendix E
Proof of Theorem 4

Proof: Each iteration of Algorithm 1 yields a new matching by adopting the best response of D2D user, and the maximum number of strategies for each D2D user is finite since there are only finite cellular and D2D users in the system. Therefore, the number of strategies for the given D2D user set $\mathcal{D}$ is a Bell number [32]. Thus, the system converges to a stable matching M_{fin} after finite iterations with probability 1.

We now prove that the final matching M_{fin} must be stable by contradiction. Suppose that M_{fin} obtained is not stable. Then, there exists a D2D user $i \in \mathcal{D}$ whose strategy is denoted by $M_{fin}(i)$, and a new strategy $M'(i)$ such that $U(M') > U(M_{fin})$. According to Algorithm 1, D2D user i can perform a changing matching from M_{fin} to M', which contradicts the fact that M_{fin} is the final matching. □

References

[1] 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.

[2] K. Doppler, M. Rinne, C. Wijting, C. B. Ribeiro, and K. Hugl, "Device-to-device communication as an underlay to LTE-advanced networks," *IEEE Commun. Mag.*, vol. 47, no. 12, pp. 42–49, Dec. 2009.

[3] X. Lin, J. G. Andrews, and A. Ghosh, "Spectrum sharing for device-to-device communication in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6727–6740, Dec. 2014.

[4] P. A. Frangoudis and G. C. Polyzos, "Security and performance challenges for user-centric wireless networking," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 48–55, Dec. 2014.

[5] *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Architecture enhancements to support Proximity-Based Services (ProSe) Proximity Services (ProSe) (Release 13)*, document TR 33.833 V1.4.0, 3GPP, May 2015.

[6] 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 Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int Symp. Inf. Theory*, Jul. 2008, pp. 524–528.

[9] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. TIT-24, no. 4, pp. 451–456, Jul. 1978.

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

[11] S. Andreev, D. Moltchanov, O. Galinina, A. Pyattaev, A. Ometov, and Y. Koucheryavy, "Network-assisted device-to-device connectivity: Contemporary vision and open challenges," in *Proc. 21st Eur. Wireless Conf.*, May 2015, pp. 1–8.

[12] M. N. Tehrani, M. Uysal, and H. Yanikomeroglu, "Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions," *IEEE Commun. Mag.*, vol. 52, no. 5, pp. 86–92, May 2014.

[13] J. Yue, C. Ma, H. Yu, and W. Zhou, "Secrecy-based access control for device-to-device communication underlaying cellular networks," *IEEE Commun. Lett.*, vol. 17, no. 11, pp. 2068–2071, Nov. 2013.

[14] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[15] X. Wang, Y. Chen, L. Cai, and J. Pan, "Scheduling in a secure wireless network," in *Proc. INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 2184–2192.

[16] 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.

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

[18] 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.

[19] X. Chen, X. Gong, L. Yang, and J. Zhang, "A social group utility maximization framework with applications in database assisted spectrum access," in *Proc. INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 1959–1967.

[20] 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*, Jun. 2014, pp. 2466–2471.

[21] Z. Zheng, T. Wang, L. Song, Z. Han, and J. Wu, "Social-aware multi-file dissemination in device-to-device overlay networks," in *Proc. INFOCOM WKSHPS*, Apr./May 2014, pp. 219–220.

[22] B. Zhang, Y. Li, D. Jin, P. Hui, and Z. Han, "Social-aware peer discovery for D2D communications underlaying cellular networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2426–2439, May 2015.

[23] A. Ometov *et al.*, "Toward trusted, social-aware D2D connectivity: Bridging across the technology and sociality realms," *IEEE Wireless Commun.*, vol. 23, no. 4, pp. 103–111, Aug. 2016.

[24] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.

[25] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, Jr., "Power control for D2D underlaid cellular networks: Modeling, algorithms, and analysis," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 1, pp. 1–13, Jan. 2015.

[26] J. Liu, S. Zhang, H. Nishiyama, N. Kato, and J. Guo, "A stochastic geometry analysis of D2D overlaying multi-channel downlink cellular networks," in *Proc. INFOCOM*, Hong Kong, Apr./May 2015, pp. 1–9.

[27] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in D2D-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.

[28] Y. Gu, W. Saad, M. Bennis, M. Debbah, and Z. Han, "Matching theory for future wireless networks: Fundamentals and applications," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 52–59, May 2015.

[29] H. Xu and B. Li, "Seen as stable marriages," in *Proc. INFOCOM*, Shanghai, China, Apr. 2011, pp. 586–590.

[30] Y. Gu, Y. Zhang, M. Pan, and Z. Han, "Matching and cheating in device to device communications underlying cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2156–2166, Oct. 2015.

[31] W. Saad, Z. Han, R. Zheng, M. Debbah, and H. V. Poor, "A college admissions game for uplink user association in wireless small cell networks," in *Proc. INFOCOM*, Toronto, ON, Canada, Apr./May 2014, pp. 1096–1104.

[32] 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.

[33] *SNAP: Network Datasets: Brightkite*. Accessed: Jan. 15, 2018. [Online]. Available: http://snap.stanford.edu/data/loc-brightkite.html

[34] L. A. Wolsey, *Integer Programming*. Hoboken, NJ, USA: Wiley, 1998.

[35] R. Jain, D. W. Chiu, and W. R. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," Eastern Res. Lab., Digit. Equip. Corp., Hudson, MA, USA, Res. Rep. TR-301, Sep. 1984.

Xinlei Chen received the B.E. and M.S. degrees in electrical engineering from Tsinghua University, China, in 2009 and 2012, respectively. He is currently pursuing the Ph.D. degree with the Department of Electric and Computer Engineering, Carnegie Mellon University, USA. His research interests are in the areas of networking and communications, mobile embedded system, and big data.

Yulei Zhao received the B.S. and Ph.D. degrees from the Department of Communication Engineering, Zhengzhou Information Science and Technology Institute, Zhengzhou, Henan, China, in 2005 and 2008, respectively. He is currently pursuing the Ph.D. degree with the Department of Electronic Engineering, Tsinghua University, Beijing, China. His research interests include cooperative communications, device-to-device communications, and social networks.

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.

From 2012 to 2013, he was a Visiting Research Associate with Telekom Innovation Laboratories and the Hong Kong University of Science and Technology. From 2013 to 2014, he was a Visiting Scientist with the University of Miami, FL, USA. He is currently a Faculty Member of electronic engineering with Tsinghua University. He has published over 100 research papers, and has 10 granted and pending Chinese and International patents. His research interests are in the areas of networking and communications, including mobile opportunistic networks, device-to-device communication, software-defined networks, network virtualization, and future Internet.

He received the Outstanding Postdoctoral Researcher, the Outstanding Ph.D. Graduates, and the Outstanding Doctoral thesis from Tsinghua University. His research was supported by the Young Scientist Fund of Natural Science Foundation of China, the Postdoctoral Special Find of China, and industry companies of Hitachi and ZET. He has served as the Technical Program Committee (TPC) Chair for the WWW Workshop of Simplex 2013 and a TPC member of several international workshops and conferences. He is also a Guest-Editor for the *ACM/Springer Mobile Networks and Applications*, Special Issue on Software-Defined and Virtualized Future Wireless Networks. He is an Associate Editor of the *EURASIP Journal on Wireless Communications and Networking*.

Xu Chen (M'12) received the Ph.D. degree in information engineering from The Chinese University of Hong Kong in 2012. He was a Post-Doctoral Research Associate with Arizona State University, Tempe, USA, from 2012 to 2014. He was a Humboldt Scholar Fellow with the Institute of Computer Science, University of Göttingen, Germany, from 2014 to 2016. He is currently a Professor with the School of Data and Computer Science, Sun Yat-sen University, Guangzhou, China. He was a recipient of the Honorable Mention Award (first runner-up of best paper award) in the 2010 IEEE International Conference on Intelligence and Security Informatics, the Best Paper Runner-up Award of the 2014 IEEE International Conference on Computer Communications (INFOCOM), and the 2014 Hong Kong Young Scientist Award.

Ning Ge (M'97) received the B.S. and Ph.D. degrees from Tsinghua University, China, in 1993 and 1997, respectively. From 1998 to 2000, he was involved in the development of ATM switch fabric ASIC with ADC Telecommunications, Dallas. Since 2000, he has been with the Department of Electronics Engineering, Tsinghua University, where he is currently a Full Professor and also the Director of the Communication Institute. His research interests include ASIC design, short range wireless communication, and wireless communications. He is a senior member of CIC and CIE.

Sheng Chen (M'90–SM'97–F'08) received the B.E. degree in control engineering from the East China Petroleum Institute, Dongying, China, in 1982, the Ph.D. degree in control engineering from the City University of London, London, in 1986, and the D.Sc. degree (Hons.) 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, U.K., The Universities of Edinburgh, U.K., and the Universities of Portsmouth, U.K. Since 1999, he has been with the School of Electronics and Computer Science, University of Southampton, U.K., where he is currently a Professor in intelligent systems and signal processing. He has published 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, evolutionary computation methods, and optimization. He is a fellow of the United Kingdom Royal Academy of Engineering and IET, a Distinguished Adjunct Professor at King Abdulaziz University, Jeddah, Saudi Arabia, and an ISI Highly Cited Researcher in engineering (2004).