Social Security Aided D2D Communications: Performance Bound and Implementation Mechanism

Yulei Zhao, Yong Li, *Member, IEEE,* Lin Chen, *Member, IEEE,* Yang Cao, *Member, IEEE,* Sheng Chen, *Fellow, IEEE,* and Ning Ge, *Member, 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. Physical-layer security mechanism is typically employed to guarantee secure communications, at the cost of reducing the system's throughput. 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 security aware D2D communication architecture that exploits social-domain trust for securing 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 security aided communications via stochastic geometry, and our result based on a real dataset shows that the proposed social security aided D2D communication increases the system secrecy rate by about 63% compared to 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 security, stochastic geometry, device-to-device communications, matching theory

1 Introduction

To meet the increasing demands for local area services, device-to-device (D2D) communication is proposed as a key component for next generation cellular networks [1], where user equipments (UEs) communicate 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].

To provide confidential data transmissions, physical-layer security mechanism, which exploits the imperfections of wireless channel [6], is typically employed to ensure that the transmitter can communicate with the receiver, while the potential eavesdroppers cannot intercept the information at physical layer. Confidential D2D communications can be maintained by adopting such a physical-layer security scheme at the great cost of decreasing system transmission rate. 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 [7]. 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 security 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 security aware D2D communications, i.e., how social

- *Y. Zhao, Y. Li, and N. Ge are with Tsinghua National Laboratory for Information Science and Technology (TNLIST), Department of Electronic Engineering, Tsinghua University, Beijing 100084, China. (E-mails: zhao-yl12@mails.tsinghua.edu.cn, liyong07@tsinghua.edu.cn, gening@tsinghua.edu.cn)*
- *L. Chen is with University of Paris-Sud. (E-mail: chen@lri.fr)*
- *Y. Cao is with Huazhong University of Science and Technology. (E-mail: ycao@hust.edu.cn)*
- *S. Chen is with Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, UK (E-mail: sqc@ecs.soton.ac.uk), and also with King Abdulaziz University, Jeddah 21589, Saudi Arabia.*

This work was supported by the National Basic Research Program of China (973 Program) under Grant 2013CB329001, by the National Nature Science Foundation of China under Grant 61132002 and Grant 61301080, and by the Creative Research Group Program from NSFC (61321061).

trust can enhance social security 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 security 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 security rate for D2D communications. Furthermore, we formulate the resource allocation as an optimization problem to maximize the system social security rate and establish efficient implementation mechanism based on matching theory. The social security mechanism presented here can also be applied to other wireless networks and has great potential to increase system secrecy rate significantly.

1.1 Summary of Main Contributions

Our contributions are summarized as follows:

- *Social security 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 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 security 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 practical mechanism in utilizing 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.

1.2 Related Work

Security has attracted increasing attention from academia and industry [4], especially for D2D underlaying cellular networks due to spectrum sharing [8]. Physical-layer security guarantees the secrecy of transmission from an information-theoretic viewpoint [6], which is conceived as a promise solution in 5G networks [9]. For example, a scheduling algorithm is proposed to maximize the physical-layer security transmission rate for future cellular networks [10]. 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 [7], [11], [12], [13].

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 [11]. Social trust and reciprocity have been utilized to design efficient cooperative strategies for D2D communications [7], [12], [14], [15], [16], [17]. For example, Chen *et al*. [14] proposed a framework to maximize social group utility, and Zhang *et al*. [17] designed social-aware peer-discovery approach. 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 [18]. In recent years, many researches have utilized stochastic geometry to analyze interference and coverage probability for D2D communication networks [3], [19], [20], [21]. 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*. [19] utilized stochastic geometric to analyze power control for D2D communication underlaying cellular network. Liu *et al*. [20] analyzed the ergodic rate for D2D overlaying multi-channel downlink cellular network based on stochastic geometry. Furthermore, Ma *et al*. [21] 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 [22]. Xu *et al*. [23] utilized a stable matching framework to solve network problems. Gu *et al*. [24] 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*. [25] used many-to-one matching to implement uplink user association in small cell networks. By contrast, in this paper, we first utilize stochastic geometry to analyze the critical parameters that influence the social security 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 2 presents the system overview and problem statement. Section 3 analyzes the theoretical physical-layer secrecy rate of the proposed social security aided D2D communication scheme, while an efficient resource allocation is developed

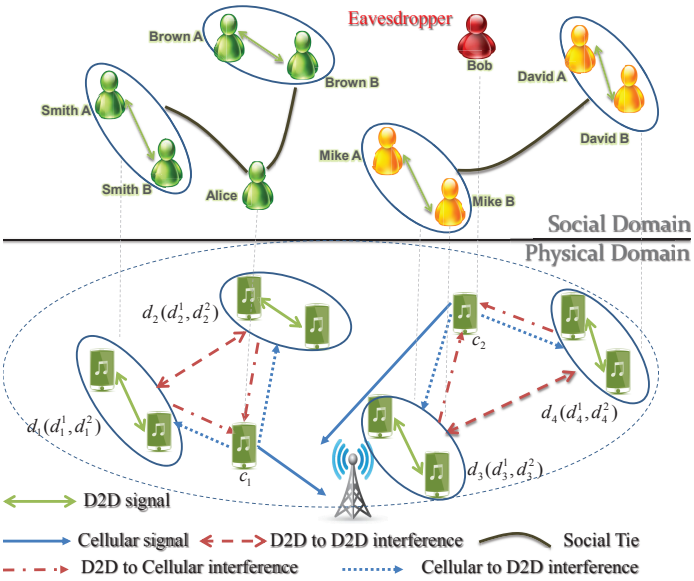


Fig. 1. A social security aided D2D communication underlaying cellular network, with 2 cellular users, c_1 and c_2, and 4 D2D user pairs, d_1 to d_4. In physical domain, wireless links are subject to physical interference constraints, while in social domain, social trusts among mobile users are indicated.

in Section 4. Performance evaluations are given in Section 5, and Section 6 concludes this work.

2 System Overview And Problem Statement

2.1 System Overview

Fig. 1 illustrates the social security aided D2D communications underlaying cellular network from both the physical and social domains, where the social trust relationships among mobile users are indicated in the social domain, 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 [7], respectively. Cellular and D2D users that share the same spectrum resource will incur severe interference among them [26].

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, social trust relationships are undirected, i.e., $\omega_{i,j} = \omega_{j,i}$. In Fig. 1, *Alice* is friend of *Smith* and *Brown*, 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 for *Smith A* and *Smith B* as well as for *Brown A* and *Brown B* which represent the D2D users of D2D pairs *Smith* and *Brown*, respectively. On the other hand, *Smith* and *Brown* 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* and *David* with $\omega_{c_2,d_3} = 0$ and $\omega_{c_2,d_4} = 0$. Thus, *Bob* is a potential eavesdropper to *Mike* and *David*. We introduce 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., $p_s = \sum_{i,j} \omega_{i,j} / N(N-1)$.

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, $d_i(d_i^1, d_i^2)$, $1 \le i \le 4$. Here we use d_i to denote the ith D2D pair, with d_i^1 representing transmitter and d_i^2 representing receiver. D2D pairs d_1 and d_2 occupy the same spectrum resource with c_1, while D2D pairs d_3 and d_4 share the spectrum resource with c_2.

2.2 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 security 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 security 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 security 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.

3 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 Poison point process (PPP) Φ_d with density λ_d in the plane with radius R [19], [20]. 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

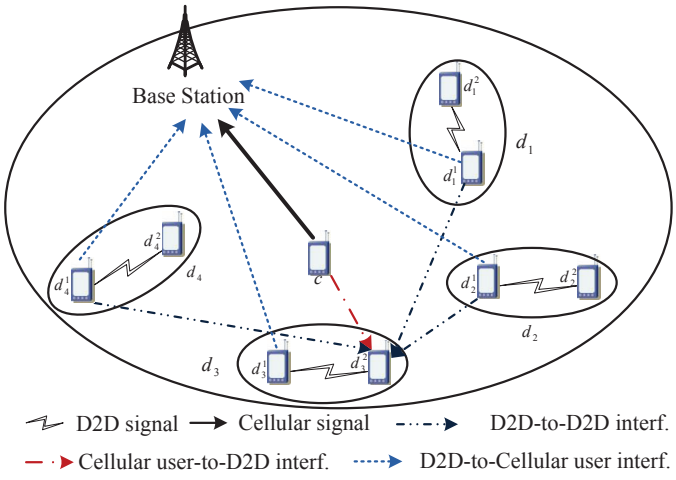


Fig. 2. Illustration of interference relationship for D2D communication underlaying cellular network in single cell.

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.

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. To complete the interference analysis, we need to consider the signal to interference plus noise ratio (SINR) at each node in each time slot. The SINR at terminal j receiving the desired signal from transmitter i can be expressed as

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

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

3.1 Social Security 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

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

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 can be obtained as [19]

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

Each D2D user 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. When the largest SINR at potential eavesdroppers is less than T_s, uplink information transmission of c is secret.

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

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

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

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

Let R_c^e denote the intercepted transmission rate by D2D users, 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 follows.

Definition 2 (Social security ergodic rate of cellular user)**.** *The social security 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 security 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 [19]:

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

where $\delta = \frac{2}{\alpha}$, and the noise is neglected. Then the transmission rate of cellular user is:

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

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*

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

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

$$\begin{aligned}
\overline{P}^{c}_{cov,s}(T_s) &= \mathbb{P}\Big(\max_{d'\in\mathcal{D}_{c,e}} \gamma_{c,d'} \le T_s\Big) \\
&= \mathbb{P}\left(\bigcap_{z\in\Phi_e} \gamma_{c,z} \le T_s\right) = \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(\gamma_{c,z} \le T_s\right)\right] \\
&\overset{(a)}{=} \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(1-\exp\left(-P_c^{-1}T_s\rho_{c,z}^{\alpha}\left(\sigma^2+I_d(z)\right)\right)\right)\right] \\
&= \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(1-\exp\left(-P_c^{-1}T_s\rho_{c,z}^{\alpha}\left(I_d(z)\right)\right)\right)\right] \\
&\overset{(b)}{=} \mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e} P\left(1-L_{I_d(z)}\left(-P_c^{-1}T_s\rho_{c,z}^{\alpha}\right)\right)\right] \\
&\overset{(c)}{=} \exp\left(-2\pi p_e\lambda_d\int_0^R L_{I_d(z)}\left(-P_c^{-1}T_s\rho_{0,z}^{\alpha}\right)\rho_{c,z}d\rho_{c,z}\right), \quad (9)
\end{aligned}$$

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 [21]. 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 [19]:

$$L_{I_d}(s)=\exp\left(-\frac{\pi\lambda_d P_d^{\delta}s^{\delta}}{\mathrm{sinc}(\delta)}\right), \quad (10)$$

where $s=P_c^{-1}T_s\rho_{c,z}^{\alpha}$. Substituting (10) into (9) leads to (8). □

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

$$R_c^e=\int_0^{\infty}\frac{1-\overline{P}^{c}_{cov,s}(x)}{(1+x)\ln 2}dx. \quad (11)$$

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

3.2 Security Rate of D2D Users

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

$$\begin{cases}
\gamma_{d_i}=\dfrac{P_d\rho_{d_i,d_i}^{-\alpha}|h_0|^2}{P_c\rho_{c,d_i}^{-\alpha}|h_0|^2+\sum\limits_{d'\in\mathcal{D}\setminus\{d_i\}}P_d\rho_{d',d_i}^{-\alpha}|h_0|^2+N_0}, \\
R_{d_i}=\int_0^{\infty}\log_2(1+x)\mathbb{P}(\gamma_{d_i}=x)dx,
\end{cases} \quad (12)$$

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.

Definition 3 (Social security 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*

$$\overline{P}^{d_i}_{cov,s}(T_s)=\mathbb{P}\left(\max_{d'\in\mathcal{D}_{d_i,e}}\gamma_{d_i,d'}\le T_s\right), \quad (13)$$

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 $R_{d_i}^e$, is:

$$\begin{cases}
\gamma_{d_i,d'}=\dfrac{P_d\rho_{d_i,d'}^{-\alpha}|h_0|^2}{P_c\rho_{c,d'}^{-\alpha}|h_0|^2+\sum\limits_{d^0\in\mathcal{D}\setminus\{d_i,d'\}}P_d\rho_{d^0,d'}^{-\alpha}|h_0|^2+N_0}, \\
R_{d_i}^e=\int_0^{\infty}\log_2(1+x)\mathbb{P}\left(\max\limits_{d'\in\mathcal{D}_{d_i,e}}\gamma_{d_i,d'}=x\right)dx,
\end{cases} \quad (14)$$

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

Definition 4 (Social security ergodic rate of D2D user)**.** *The social security rate for D2D user d_i is $R_{d_i}^s=\max\left\{R_{d_i}-R_{d_i}^e,0\right\}$.*

The coverage probability of D2D user d_i is given by [19]:

$$\overline{P}^{d_i}_{cov}(T_d)=\exp\left(-\frac{\pi\lambda_d T_d^{\delta}}{\mathrm{sinc}(\delta)}\rho_{d_i,d_i}^2\right)\frac{1}{1+\left(\frac{T_dP_c}{P_d}\right)^{\delta}\left(\rho_{d_i,d_i}\frac{45\pi}{128R}\right)^2}, \quad (15)$$

where T_d is the SINR threshold for data detection required by D2D receiver, and the noise is neglected. The transmission rate of D2D user is given by

$$R_{d_i}=\int_0^{\infty}\frac{\overline{P}^{d_i}_{cov}(x)}{(1+x)\ln 2}dx. \quad (16)$$

Theorem 2. *If the receiver noise is negligible, the social security coverage probability of D2D user d_i is given as*

$$\begin{aligned}
\overline{P}^{d_i}_{cov,s}(T_s) &= \exp\left(-2\pi p_e\lambda_d\int_0^R L_{d-d}(s_z)L_{d-c}(s_z)\rho_{d_i,z}d\rho_{d_i,z}\right) \\
&\times\left(1-\left(\int_0^{2R}\exp\left(-\frac{\pi\lambda_d T_s^{\delta}\rho_{d_i,c}^2}{\mathrm{sinc}(\delta)}\right)f(\rho_{d_i,c})d\rho_{d_i,c}\right)\right), \quad (17)
\end{aligned}$$

where

$$L_{I_{d-d}}(s_z)=\exp\left(-\frac{\pi\lambda_d T_s^{\delta}\rho_{d_i,z}^2}{\mathrm{sinc}(\delta)}\right), \quad (18)$$

$$L_{I_{d-c}}(s_z)=1\Big/\left(1+\left(\frac{P_c}{P_d}T_s\right)^{\delta}\frac{\rho_{d_i,z}^2}{\left(\frac{128R}{45\pi}\right)^2}\right), \quad (19)$$

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

$$f(\rho_{d_i,c})=\frac{2\rho_{d_i,c}}{R^2}\left(\frac{2}{\pi}\cos^{-1}\left(\frac{\rho_{d_i,c}}{2R}\right)-\frac{\rho_{d_i,c}}{\pi R}\sqrt{1-\frac{\rho_{d_i,c}^2}{4R^2}}\right). \quad (20)$$

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

$$\begin{aligned}
\overline{P}^{d_i}_{cov,s}(T_s) &= \mathbb{P}\left(\max_{z\in\Phi_e\cup\{c\}}\gamma_{d_i,z}^e<T_s\right) \\
&\overset{(a)}{=} \mathbb{P}\left(\max_{z\in\Phi_e}\gamma_{d_i,z}^e<T_s\right)\mathbb{P}\left(\gamma_{d_i,c}^e<T_s\right). \quad (21)
\end{aligned}$$

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

The first part of (21) can be expressed as

$$\begin{aligned}
&\mathbb{P}\left(\max_{z\in\Phi_e}\gamma^e_{d_i,z}<T_s\right)=\mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e}P(\gamma_{d_i,z}<T_s)\right]\\
&\overset{(a)}{=}\mathbb{E}_{\Phi_d}\left[\prod_{z\in\Phi_e}\left(1-L_{I_{d(z)}}\left(-P_d^{-1}T_s\rho^{\alpha}_{d_i,z}\right)\right)\right]\\
&=\exp\left(-2\pi p_e\lambda_d\int_0^R L_{I_d(z)}\left(-P_d^{-1}T_s\rho^{\alpha}_{d_i,z}\right)\rho_{d_i,z}d\rho_{d_i,z}\right)\\
&\overset{(b)}{=}\exp\left(-2\pi p_e\lambda_d\int_0^R L_{I_{d-d}(z)}\left(s_z\right)L_{I_{d-c}(z)}\left(s_z\right)\rho_{d_i,z}d\rho_{d_i,z}\right),
\end{aligned}\tag{22}$$

where $s_z=P_d^{-1}T_s\rho^{\alpha}_{d_i,z}$. 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:

$$\begin{aligned}
L_{I_d}(s_z)&=\mathbb{E}\left[\exp\left(-s_zI_d\right)\right]\\
&=E\left[\exp\left(-s_zI_{d-d}\right)\right]E\left[\exp\left(-s_zI_{d-c}\right)\right]\\
&=L_{I_{d-d}}(s_z)L_{I_{d-c}}(s_z).
\end{aligned}\tag{23}$$

From [19], we obtain the Laplace transformations, $L_{I_{d-d}}(s_z)$ and $L_{I_{d-c}}(s_z)$, as given in (18) and (19), respectively.

The second part of (21) can be expressed as

$$\begin{aligned}
\mathbb{P}\left(\gamma_{d_i,c}<T_s\right)&=1-\mathbb{E}\Big[\exp\left(-P_d^{-1}T_s\rho^{\alpha}_{d_i,c}I_c(z)\right)\Big]\\
&=1-\mathbb{E}\left[L_{I_c}(s_c)\right],
\end{aligned}\tag{24}$$

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

$$L_{I_c}(s_c)=\exp\Big(-\frac{\pi\lambda_dT_s^{\frac{2}{\alpha}}\rho^2_{d_i,c}}{\mathrm{sinc}\delta}\Big).\tag{25}$$

Thus we have

$$\mathbb{P}\left(\gamma_{d_i,c}<T_s\right)=1-\int_0^{2R}\exp\left(-\frac{\pi\lambda_dT_s^{\delta}\rho^2_{d_i,c}}{\mathrm{sinc}}\right)f\left(\rho_{d_i,c}\right)d\rho_{d_i,c},\tag{26}$$

where $f\left(\rho_{d_i,c}\right)$ is the probability density function of $\rho_{d_i,c}$ given in (20). By substituting (22) and (26) into (21), we obtain $\overline{P}^{d_i}_{cov,s}$ of (17). □

The intercepted rate of D2D user can then be obtained as

$$\begin{aligned}
R^e_{d_i}&=\int_0^{\infty}\frac{\mathbb{P}\left(\max\limits_{d'\in\mathcal{D}_{d_i,e}}\gamma_{d_i,d'}\geq x\right)}{(1+x)\ln 2}dx\\
&=\int_0^{\infty}\frac{1}{(1+x)\ln 2}\left(1-\overline{P}^{d}_{cov,s}\right)dx,
\end{aligned}\tag{27}$$

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 $R^s_{\mathrm{sys}}=R^s_c+\lambda_d\pi R^2\cdot R^s_d$, the system intercepted rate $R^e_{\mathrm{sys}}=R^e_c+\lambda_d\pi R^2\cdot R^e_d$, and the system transmission rate $R_{\mathrm{sys}}=R_c+\lambda_d\pi R^2\cdot R_d$.*

Proof. The system secrecy rate can be derived as:

$$R^s_{\mathrm{sys}}=R^s_c+\mathbb{E}_{\Phi_d}\left[\sum_{d_i\in\mathcal{D}}R^s_{d_i}\right]=R^s_c+\lambda_d\pi R^2\cdot R^s_d\tag{28}$$

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

3.3 Numerical Results

To evaluate the impact of D2D density and social link probability on secrecy rate, we set the simulation parameters as $P_c=100\,\mathrm{mW}$, $P_d=0.4\,\mathrm{mW}$, $R=500\,\mathrm{m}$, 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^s_c and R^s_d decrease quickly as λ_d increases, while the intercepted rates R^e_c and R^e_d are affected slightly by changing λ_d. For example, when the number of D2D pairs increases from 1 to 16, the average secrecy rates of cellular user and D2D pair decrease by about 80% and 70%, respectively. The reason is that larger number of D2D users introduces more interferences, while the number of potential eavesdroppers also increases. Therefore, the intercepted rate changes slightly, and the secrecy rate drops sharply. Similarly, the transmission rates R_c and R_d decrease quickly with the increase of λ_d. 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 the system transmission rate increases with the number of D2D pairs, the sum secrecy rate decreases at some point, which has important implication 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). It can be seen that the system secrecy rate increases about 200% when p_s increases from 0 to 1. It is also obvious from Fig. 3(d) that social trust decreases the intercepted rate significantly.

Furthermore, we utilize the social trust relations from the real dataset of Brightkite [27], 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). From Fig. 3 (e), it is observed that social link probability decreases as the number of D2D pairs increases. In Fig. 3 (f), R^p_{sys} is the system secrecy rate without considering social trust, which shows the same trend as observed in Fig. 3 (c), while R^s_{sys} is the system secrecy rate obtained by considering social trust. Observe that 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. Moreover, unlike R^p_{sys}, R^s_{sys} keeps increasing as λ_b increases.

4 Matching Theory for Resource Allocation

We provide the solution to maximize the secrecy rate, which yields efficient resource allocation needed to utilize the

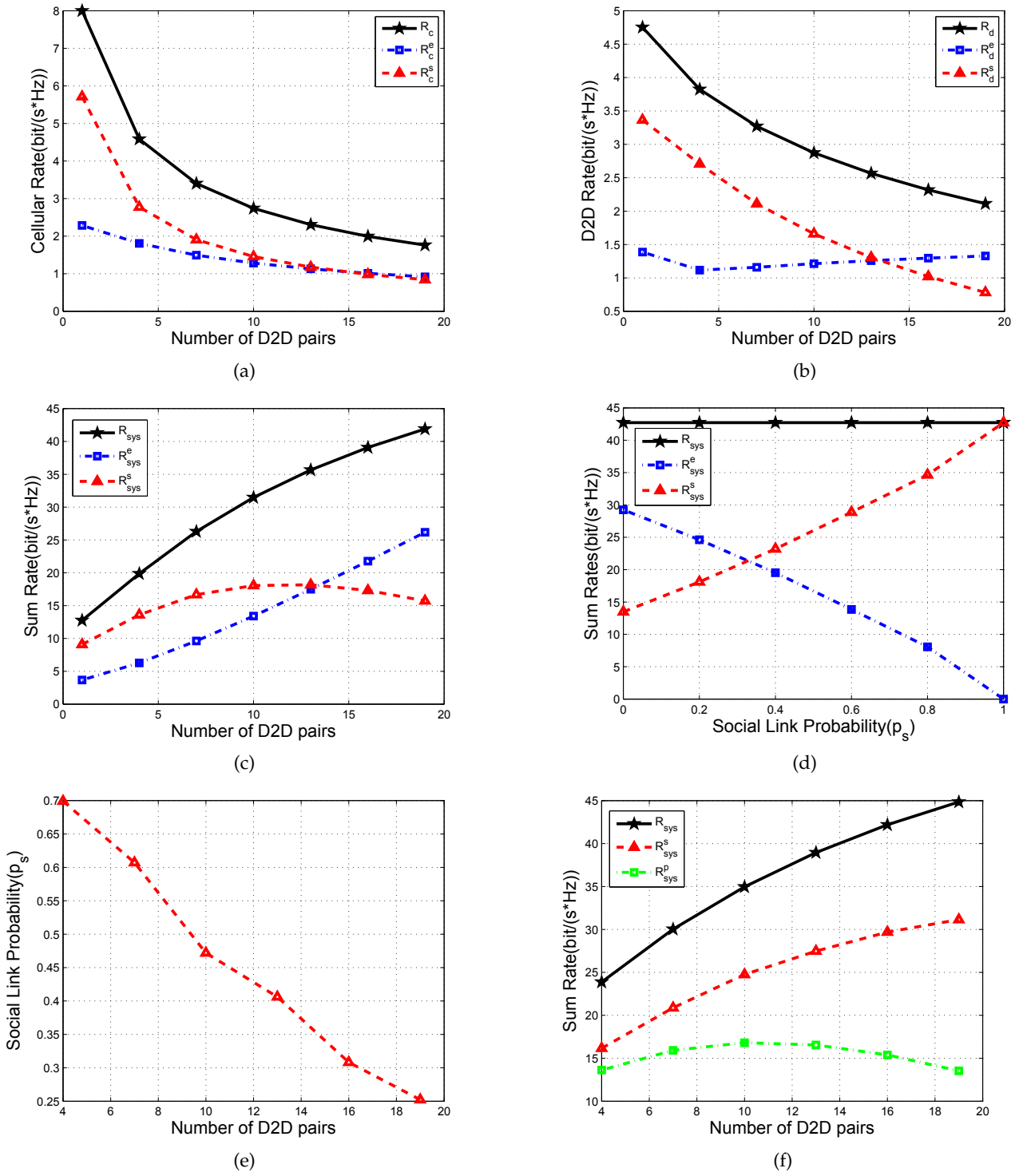


Fig. 3. Performance analysis via stochastic geometry: (a) secrecy rate of cellular user when $p_s = 0$, (b) secrecy rate of D2D user when $p_s = 0$, (c) sum secrecy rate of cellular user and all D2D users when $p_s = 0$,, (d) relationship between sum secrecy rate and social link probability given 20 D2D pairs, (e) social trust based on real dataset of Brightkite [27], and (f) social security performance of real social trust.

social trust in order to attain the theoretical performance gains.

4.1 Problem Formulation

4.1.1 *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, $R_c^{e'}$ and $R_c^{s'}$ 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 deter-

mined by spectrum sharing and social trust relationships.

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

$$R_c' = \log_2\left(1+\frac{P_c\rho_{c,b}^{-\alpha}|h_0|^2}{\sum_{d\in\mathcal{D}} x_{c,d}P_d\rho_{d,b}^{-\alpha}|h_0|^2+N_0}\right). \quad (29)$$

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

$$R_c^{e'} = \max_{d^0\in\mathcal{D}'_{c,e}} \log_2\left(1+\frac{P_c\rho_{c,d^0}^{-\alpha}|h_0|^2}{\sum_{d\in\mathcal{D}\setminus\{d^0\}} x_{c,d}P_d\rho_{d,d^0}^{-\alpha}|h_0|^2+N_0}\right). \quad (30)$$

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

4.1.2 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', $R_d^{e'}$ and $R_d^{s'}$ 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 expressed by $I_d^c + \sum_{d'\in\mathcal{D}\setminus\{d\}} y_{d,d'}P_{d'}\rho_{d',d}^{-\alpha}|h_0|^2$, where $I_d^c = \sum_{c\in\mathcal{C}} x_{c,d}P_c\rho_{c,d}^{-\alpha}|h_0|^2$. The channel rate of D2D pair d is thus given by

$$R_d' = \log_2\left(1+\frac{P_d\rho_{d,d}^{-\alpha}|h_0|^2}{I_d^c+\sum_{d'\in\mathcal{D}\setminus\{d\}} y_{d,d'}P_{d'}\rho_{d',d}^{-\alpha}|h_0|^2+N_0}\right). \quad (31)$$

If eavesdropper $d^0 \in \mathcal{D}'_{d,e}$ is a D2D pair, the interferences at d^0 can be calculated as $I_d^c + \sum_{d'\in\mathcal{D}\setminus\{d,d^0\}} y_{d,d'}P_{d'}\rho_{d',d^0}^{-\alpha}|h_0|^2$. If d^0 is a cellular user, the interference from other cellular users equals to 0, i.e., $I_d^c = 0$. The intercepted rate of d by the eavesdroppers is therefore given by

$$R_d^{e'} = \max_{d^0\in\mathcal{D}'_{d,e}} \log_2\left(1+\frac{P_d\rho_{d,d^0}^{-\alpha}|h_0|^2}{I_d^c+\sum_{d'\in\mathcal{D}\setminus\{d,d^0\}} y_{d,d'}P_{d'}\rho_{d',d^0}^{-\alpha}|h_0|^2+N_0}\right). \quad (32)$$

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

Combining the results of Subsections 4.1.1 and 4.1.2, we obtain the system social security rate as

$$\mathfrak{R}(\mathbf{X}) = \sum_{c\in\mathcal{C}}\left(R_c^{s'} + \sum_{d\in\mathcal{D}} x_{c,d}R_d^{s'}\right), \quad (33)$$

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 security communications as the following optimization problem:

$$\begin{aligned} &\max \mathfrak{R}(\mathbf{X}),\\ &\text{s.t.} \quad \begin{cases} x_{c,d}\in\{0,1\}, \forall c\in\mathcal{C}, d\in\mathcal{D};\\ \sum_{c\in\mathcal{C}} x_{c,d}\le 1, \forall d\in\mathcal{D};\\ R_c^{s'} \ge \overline{R}_c, \forall c\in\mathcal{C}. \end{cases} \end{aligned} \quad (34)$$

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 (34) is NP-hard.*

Proof. The optimization objective has no concave properties with $x_{c,d}$. Moreover, it is a binary integer non-linear programming problem. Therefore, it is NP-hard in general [28]. □

Lemma 1 indicates that the optimization problem (34) cannot be solved by conventional algorithms. Note that the security 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 security 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 security rate. In the following section, matching game model is used to implement efficient resource allocation.

4.2 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 [23]. Our problem (34) 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 security resource allocation)**.** *A many-to-one social security 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 security rate, and the utility of D2D user d is defined as

$$U_d(M) = R_d^{s'}. \quad (35)$$

From the expression of $R_d^{s'}$, we can see that $U_d(M)$ depends on the matching of other players, which demonstrates peer effects for matching. The utility of cellular user c on the other hand is defined as

$$U_c(M) = R_c^{s'} + \sum_{d\in M(c)} R_d^{s'}, \quad (36)$$

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 definitions of $U_d(M)$ and $U_c(M)$, it is clear that each D2D user occupies the spectrum resource of a cellular user without considering the other D2D users and cellular users, while a cellular user prefers to accept the D2D user, which contributes to maximize the total security rate of all users sharing the same spectrum resource with it.

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 security 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 [22]. From the above analysis, we can see that the proposed social security matching cannot be obtained based on the traditional deferred acceptance algorithm [22]. Therefore, we need to design an efficient mechanism to obtain a stable matching.

We now analyze the property of the stable matching qualitatively, which will provide the intuition to design our proposed algorithm. If there exists blocking pair (c,d) of matching M, the new matching $M' = M \setminus \{(M(d),d)\} \cup \{(c,d)\}$ is able to increase the system security rate under the stable condition in Definition 8. In other words, a stable matching achieves a local optimum of the system sum security rate $\mathfrak{R}(\mathbf{X})$, which can be utilized to obtain a stable matching. On the other hand, as the optimization problem (34) is a binary integer programming problem, an global optimum matching M^{opt} can be obtained by exhaustive search. Obviously, M^{opt} is a stable matching. Therefore, there exists at least one stable matching for our proposed matching game model.

4.3 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.

4.3.1 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 accept this request is determined from two aspects. Firstly, c' needs to guarantee its security 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.

Algorithm 1: Proposed Social Security 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 (38), 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 $M_{fin} \leftarrow M_{cur}$.

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

$$\mathfrak{R}(M') - \mathfrak{R}(M) = U_c(M') + U_{M(d)}(M') - U_c(M) - U_{M(d)}(M). \quad (37)$$

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. □

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:

$$x_i^* = \arg\max_{c \in \mathcal{C}} U_c(M') + U_{M(i)}(M'), \tag{38}$$

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}.

4.4 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. 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 [26]. 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. □

5 Performance Evaluation

We evaluate the performance of the proposed matching algorithm for social security D2D communications based on a real dataset and a large-scale simulated network. The main parameters in our simulation are listed in Table 1. 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 transmitter with the maximum distance. According to the solution of the proposed matching algorithm, we evaluate the following two performance metrics.

TABLE 1
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

1) System sum secrecy rate, which is determined by all the D2D users and cellular users as well as the social trust among them.
2) The Jain's fairness measure [29], which determines whether the receivers of D2D users and the cellular users are receiving 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 [26]. 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 aways from the D2D users
c) Random Selection (RS). It uniformly and randomly allocates the communication resources to the D2D users.

5.1 System Social Security Rate

We first set up the simulation based on the social trust relations obtained from the real dataset of Brightkite [27]. The dataset Brightkite contains the check-in data between April 2008 to October 2010, and the total number of check-ins is 4.5 million. Brightkite contains an explicit social network, which is utilized in our simulation. We first estimate the social link probability, which is provided in Fig. 3 (e). Then, the social trust among cellular users and D2D users are generated in each simulation scenario randomly based on the obtained real 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 10, while the number of cellular users varies from 10 to 20. It can be seen that the RS scheme has the worst performance, as it does not consider the mutual interference and does not utilize the social trust. Compared with the RS, our SM scheme increases the sum security rate about 50% given 10 D2D pairs. It also can be seen that our SM clearly outperforms the existing state-of-the-art CG scheme.

In Fig. 4 (b), the number of cellular user is set to 5, and the number of D2D pairs varies from 1 to 20. When the number of D2D pairs is more than 5, multiple D2D pairs have to share the same spectrum resource of one cellular user. Observe from Fig. 4 (b) that the sum security rates of the CG, FF and RS schemes all decrease with the number of D2D pairs, when the number of D2D pairs is no more

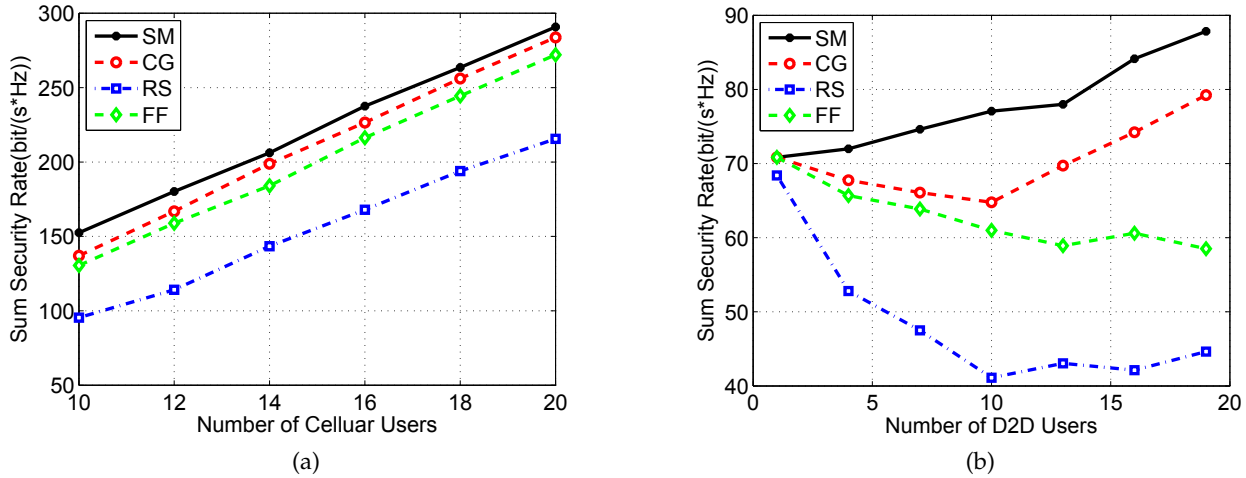


Fig. 4. Comparison of the system performance attained by the four schemes in a simulated network based on the real dataset [27]: (a) given 10 D2D pairs and varying the number of cellular users, and (b) given 5 cellular users and varying the number of D2D pairs.

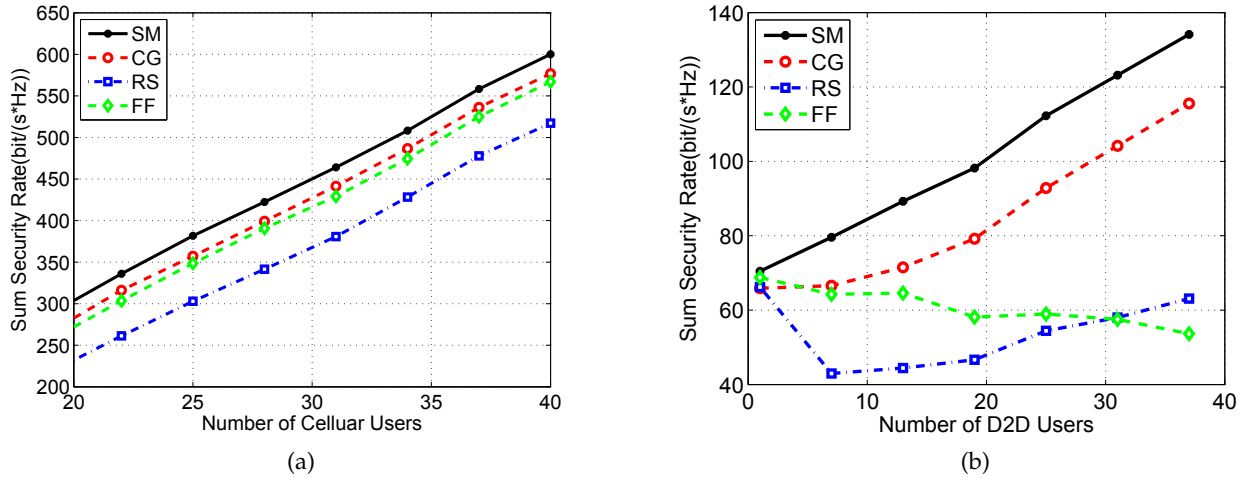


Fig. 5. Comparison of the system performance attained by the four schemes in a large-scale simulated network: (a) given 10 D2D pairs and varying the number of cellular users, and (b) given 5 cellular users and varying the number of D2D pairs..

than 10. This is because withing this range, the interference is relatively small, and social trust has dominant influence on the sum security rate but the CG, FF and RS schemes all cannot utilize this information. When the number of D2D pairs is more than 10, the mutual interference increases considerably and has serious influence on the achievable system security rate. Therefore, the sum security rate of the CG scheme becomes increasing with the number of D2D pairs, as the CG scheme can effectively take into account the mutual interference. By contrast, our SM scheme effectively not only considers the mutual interference but also utilizes the social trust information. Consequently, its achievable system security rate increases with the number of D2D pairs across the whole range of D2D pairs, and it significantly outperforms the existing state-of-the-art CG scheme, as can be clearly seen from Fig. 4 (b).

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 represents the scenario of sufficient spectrum resource, where D2D users do not need to share the resource of a same cellular user and, therefore, there may exist no interference among D2D users. It can be seen from Fig. 5 (a) that our SM scheme achieves the best performance, and it clearly outperforms the CG scheme. This is because our SM scheme can effectively consider the social trust information among D2D pairs and cellular users to achieve better resource allocation.

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 more than 20, both the social trust and mutual interference have serious influence on the sum security rate. For example, the FF scheme only considers the interference of each D2D pair and its performance is worse than that of the RS scheme when the number of D2D pairs is above 30. Clearly, our SM scheme attains the best performance among all the algorithms evaluated. For example, given 20 D2D pairs, our SM scheme 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).

5.2 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 5 and 20, respectively. Fig. 6 depicts the system

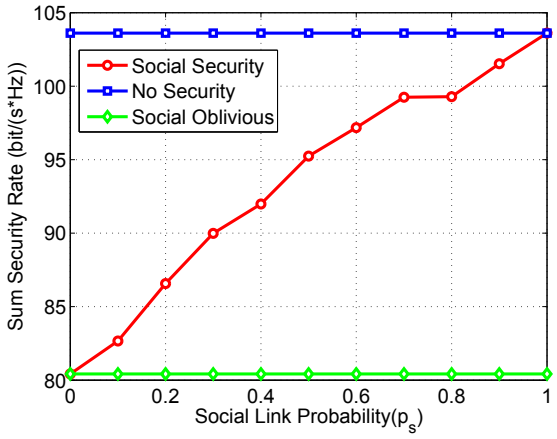


Fig. 6. System secrecy rate performance as the functions of social link probability obtained by three different approaches, given 5 cellular users and 20 D2D pairs.

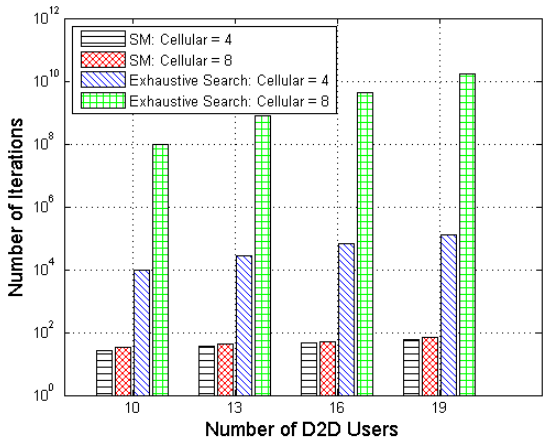
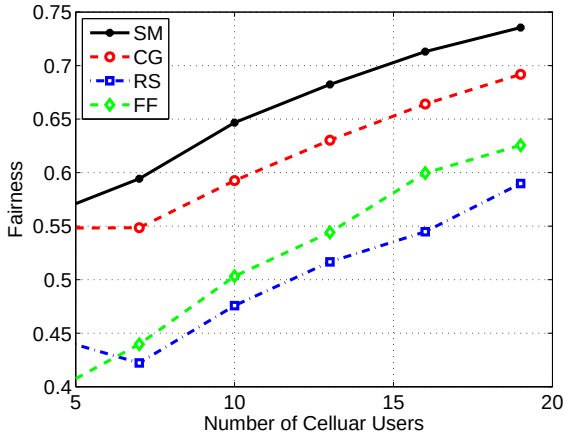
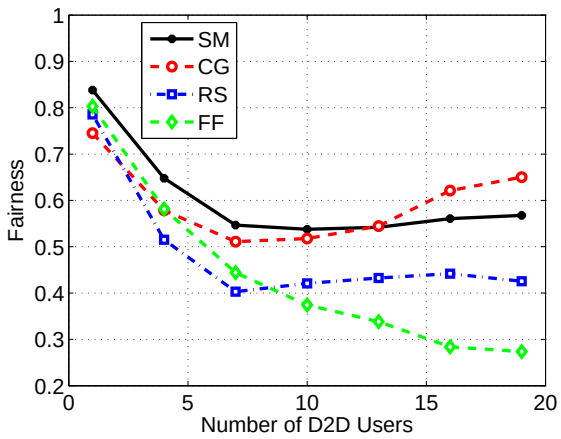


Fig. 7. Comparison of the convergence rates, in terms of the average number of iterations, required by our SM algorithm and the exhaustive search.



(a)



(b)

Fig. 8. Comparison of the system fairness for the four schemes in a simulated network based on the real dataset [27]: (a) given 10 D2D pairs and varying the number of cellular users, and (b) given 5 cellular users and varying the number of D2D users.

secrecy rates as the functions of the social link probability for the three different approaches, where the 'Social Security' denotes our SM approach, and 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 transmission, while 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, social trust information exists among cellular user and D2D users, and our Social Security approach can effectively exploit this inherent relationship.

For each simulation scenario, we generate the social trust information among the cellular users and D2D users based on p_s randomly. With $p_s = 0$, the system secrecy rate of our SM approach has the smallest value equal to that of the Social Oblivious approach, as in this situation cellular users and D2D users are social oblivious. Thus, each user is the potential eavesdropper of the transmissions of other users. With $p_s = 1$, the SM approach attains the maximum system secrecy rate, as cellular users and D2D users trust each other completely. It can be seen that with $p_s = 1$, our SM increases the system secrecy rate by about 28%, compared to the Social Oblivious approach. When p_s varies from 0 to 1, the sum security rate of our scheme increases from the smallest value to the largest value. The results of Fig. 6 again confirm that our SM approach jointly considers the social trust information and mutual interference in resource allocation effectively.

5.3 Computation Complexity

To investigate the convergence rate of our proposed SM algorithm, we set the numbers of cellular users to 4 and 8, respectively, and vary the number of D2D users D. 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.

5.4 System Fairness

To gain some insights on how the secrecy data transmission is actually shared among the D2D users and cellular users, in Fig. 8, we depict the Jain's fairness indexes obtained by

the four schemes under the same simulated network environment of Section 5.1. Among all the schemes evaluated, our proposed SM scheme achieves the best fairness resource sharing among the cellular users and D2D users. Fig. 8 (b) also indicates that varying the number of D2D users has a non-obvious influence on the fairness of data transmission for these four schemes.

6 Conclusion and Future Work

This paper has proposed the novel idea of social security 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, in the case involving 20 D2D user pairs. This study has opened a new paradigm for designing security D2D communications and has provided effective implementation mechanism for realizing social security aided D2D communications.

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. Polyzos, "Security and performance challenges for user-centric wireless networking," *IEEE Commun. Mag.*, vol. 52, no. 12, pp. 48-55, Dec. 2014.

[5] 3GPP TR 33.833 V1.4.0, "Study on security issues to support proximity services," Release 13, 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] X. Chen, B. Proulx, X. Gong, and J. Zhang, "Social trust and social reciprocity based cooperative D2D communications," in *Proc. MobiHoc 2013* (Bangalore, India) Jul. 29 - Aug. 1, 2013, pp. 187-196.

[8] 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.

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

[10] X. Wang, Y. Chen, L. Cai, and J. Pan, "Scheduling in a secure wireless network," in *Proc. INFOCOM 2014* (Toronto, Canada), Apr. 27 - May 2, 2014, pp. 2184-2192.

[11] 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.

[12] Y. Cao, X. Chen, T. Jiang, and J. Zhang, "SoCast: social ties based cooperative video multicast," in *Proc. INFOCOM 2014* (Toronto, Canada), Apr. 27 - May 2, 2014, pp. 415-423.

[13] 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.

[14] 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 2014* (Toronto, Canada), Apr. 27-May 2, 2014, pp. 1959–1967.

[15] 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 2014* (Sydney. Australia), Jun. 10-14, 2014, pp. 2466-2471.

[16] 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 2014 WKSHPS* (Toronto, Canada), Apr. 27-May 2, 2014, pp. 219-220.

[17] 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.

[18] 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.

[19] N. Lee, X. Lin, J. G. Andrews, and R. W. Heath, "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.

[20] 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 2015* (Hong Kong, China), Apr. 26 - May 1, 2015, pp. 1-9.

[21] 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. Wireless Commun.*, vol. 63, no. 1, pp. 229-242, Jan. 2015.

[22] 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.

[23] H. Xu and B. Li, "Seen as stable marriages," in *Proc. INFOCOM 2011* (Shanghai, China), Apr. 10-15, 2011, pp. 586-590.

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

[25] 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 2014* (Toronto, Canada), Apr. 27-May 2, 2014, pp. 1096-1094.

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

[27] "SNAP: Network datasets: Brightkite." [Online]. Available: *http://snap.stanford.edu/data/loc-brightkite.html*.

[28] L. A. Wolsey, *Integer Programming*. Wiley-Interscience, 1998.

[29] R. K. Jain, D. W. Chiu, and W. R. Hawe, "A quantitative measure of fairness and discrimination for resource allocation in shared computer systems," *DEC Research Report TR-301*, Eastern Research Lab, Digital Equipment Corporation, Hudson, MA, Sep. 1984.