SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

April 2018, Vol. 61 042304:1–042304:12
doi: 10.1007/s11432-017-9160-y

Opportunistic access control for enhancing security in D2D-enabled cellular networks

Yajun CHEN[1*], Xinsheng JI[1,2,3], Kaizhi HUANG[1], Bin LI[4] & Xiaolei KANG[1]

[1]*National Digital Switching System Engineering & Technological R&D Center, Zhengzhou* 450002*, China;*
[2]*National Mobile Communications Research Laboratory, Southeast University, Nanjing* 211189*, China;*
[3]*National Engineering Lab for Mobile Networking Security, Beijing* 100876*, China;*
[4]*School of Information and Electronics, Beijing Institute of Technology, Beijing* 100081*, China*

Received 28 March 2017/Accepted 26 June 2017/Published online 11 October 2017

Abstract In this paper, we investigate secure communication over cellular uplinks in device-to-device (D2D)-enabled cellular networks. We consider a more general scenario, in which multiple D2D pairs could simultaneously share the same resource block with a specific cellular user. First, an opportunistic access control scheme based on wireless channel gains is proposed, by which the candidate selected set of D2D pairs sharing the same resource block is determined. The proposed scheme could guarantee reliable communications for both cellular users and D2D pairs, and further could combat eavesdroppers while keeping the legitimate cellular user as non-intrusive as possible, regarding D2D pairs as friendly jammers in a non-collaborative way. Then, we derive theoretical results to characterize the security and reliability of the typical cellular and D2D links, respectively. To further support the performance of this hybrid network, we next present an interference threshold optimization model. Our aim is to minimize the connection outage probability (COP) of D2D pairs subject to the secrecy requirement of the cellular user. Finally, simulation results are presented to validate the effectiveness of our proposed scheme.

Keywords device-to-device (D2D) communication, opportunistic access control, physical layer security (PHY-security), secrecy outage probability (SOP), connection outage probability (COP)

Citation Chen Y J, Ji X S, Huang K Z, et al. Opportunistic access control for enhancing security in D2D-enabled cellular networks. Sci China Inf Sci, 2018, 61(4): 042304, doi: 10.1007/s11432-017-9160-y

1 Introduction

To meet the emerging proximity traffic demands, device-to-device (D2D) communication underlying cellular networks has attracted a great deal of attention, and has been regarded as a promising technique for next-generation communication (5G) [1–3]. The proximity users, called D2D pairs, can exchange information directly over D2D links, by passing the base station, which can bring the benefits of improving spectrum efficiency, offloading cellular traffic, and enhancing the quality of service (QoS) of edge users [4, 5].

On the other hand, since the inherent openness of the transmission medium makes wireless information more vulnerable to being eavesdropped, secure communication is identified as a critical challenge facing wireless systems. To overcome this issue, physical layer security (PHY-security), as a remedy of traditional encryption techniques, has been recognized as a prominent component to realize secure communication by exploiting the physical characteristics of wireless channels. This research topic has attracted significant

* Corresponding author (email: chenyajun_cool@126.com)

attention and yielded fruitful research in various scenarios [6–12]. Further advances were achieved by the authors in [13, 14], who respectively investigated PHY-key generation and PHY-authentication by exploiting intrinsic characteristics of wireless channels.

To guarantee secure communication in a D2D-enabled cellular network, the concept of PHY-security has been further expanded to this hybrid network, on which there have been many researches. To be specific, Alam et al. [15] presented a comprehensive analysis of the security threats in this hybrid cellular network. Zhu et al. [16] theoretically proved that secure performance over straight D2D links was better than that over traditional cellular links via a base station. Kang et al. [17, 18] employed a traditional artificial noise scheme in a D2D-enabled cellular network to guarantee secure communication for the cellular downlink. The excessive interference induced by these hybrid links is regarded as an obstacle to cellular communications from the traditional perspective. However, in the presence of eavesdroppers (Eves), it will also degrade their reliable communications. Hence, gains in security could be obtained by appropriate scheduling if the interference from D2D links to eavesdropping links is more severe than that to cellular links from the PHY-security perspective. The security of the cellular uplink is always the bottleneck due to its inherent limitations (e.g., small number of antennas, lower transmission power). In response to this, a wealth of studies exploit the interference between these hybrid links to improve the security performance of cellular uplinks [19–25]. However, they only consider the simple scenario in which at most one D2D pair shares the specific cellular resource block. To further support the performance of these hybrid networks, Zhang and Ma considered a general scenario in the D2D-enabled cellular network [25, 26], in which multiple D2D pairs could share the same cellular resource simultaneously. Undoubtedly, this will cause deleterious internal interference between different D2D pairs, degrading their reliable communications. In order to guarantee reliable communications, the interference to cellular links and other D2D links must be constrained. Unfortunately, the previous studies did not take this into account and only considered the impact of the interference on the security. Moreover, since Eves often work passively, it will be impossible to know their locations. It is no wonder that most of the existing studies [19–25] only consider the impact of the small-scale fading of wireless channels while ignoring the large-scale fading. As an efficient mathematical tool to further accurately characterize the impact of the wireless channel, including both the small and large-scale fading, on the system performance, stochastic geometry has been widely employed in the field of wireless networks in recent years [26–33].

Motivated by the above mentioned observations, in this paper, we consider a more general scenario, in which multiple D2D pairs could simultaneously share the same resource block with the specific cellular user. Assuming the cellular users, D2D pairs, and Eves follow the independent homogeneous Poisson Point Process (PPP), an opportunistic access control scheme based on wireless channel gains is proposed. Then, we utilize the secrecy outage probability (SOP) and connection outage probability (COP) to characterize the security and reliability of the communication over cellular links and D2D links, respectively. To further support the system performance, we propose an interference threshold optimization model. For the sake of clarify, the main contributions of this paper are summarized as follows.

(1) Considering a general scenario, an opportunistic access control scheme is proposed. In this proposed scheme, the D2D pairs sharing the same resource should satisfy the following two criteria: (a) the channel gains from the D2D transmitters to the base station should be less than the predefined threshold, such that the interference limitation for the cellular user could be guaranteed; (b) the channel gains between the different D2D pairs should also be below a fixed threshold, such that the interference limitation between different D2D pairs could be guaranteed. Based on the above two criteria, the proposed scheme could combat Eves while keeping the legitimate cellular user as non-intrusive as possible, regarding D2D pairs as friendly jammers in a non-collaborative way, which could guarantee the reliable communications of both cellular users and D2D pairs.

(2) Based on the proposed scheme, just as was done in [20–26], we respectively consider the secure communication of the typical cellular link and the reliable communication the typical D2D link, which are characterized by their corresponding SOP and COP, respectively. Hence, the SOP of the typical cellular link and the COP of the typical D2D link are analytically derived.

(3) Finally, we propose an interference threshold optimization model to improve the performance of

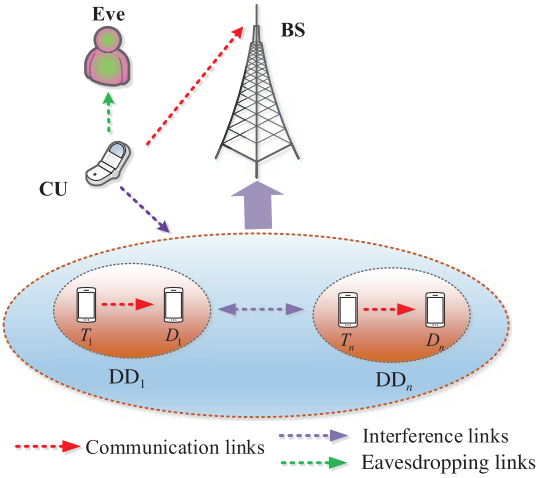

Figure 1 (Color online) System model.

this hybrid network. Since the cellular users have higher priorities and their performances should be guaranteed before D2D pairs are allowed to access the cellular network, our aim is to minimize the COP of the typical D2D link, subject to the cellular secrecy requirement, by which we can obtain the numerical results of the optimal interference thresholds.

The rest of this paper is organized as follows. The system model and problem description are given in Section 2. In Section 3, we provide a novel opportunistic access control scheme for this hybrid network. The performance of this hybrid network is analyzed in Section 4. Simulation results and analysis are presented in Section 5. Finally, we draw conclusion in Section 6.

Notations. We use $\mathcal{CN}(\mu, \sigma^2)$ to denote the noise following a circularly symmetric complex Gaussian with mean μ and covariance σ^2. exp(1) represents the exponential distribution with unit mean. $\Gamma(x)$ is the gamma function. In addition, the notation $\mathrm{E}\{\cdot\}$ denotes the mathematical expectation and $\mathbb{P}(\cdot)$ denotes the probability of an input event. Card$(\cdot)$ represents the number of the entries in the input set.

2 System model and problem description

2.1 System model

As demonstrated in Figure 1, we consider the cellular uplink communication scenario between the cellular user (CU) and the base station (BS), in which multiple D2D pairs could share the same resource block with the given CU. Meanwhile, just as in [20–26], there are multiple malicious Eves attempting to interpret the confidential message over the cellular uplink[1)]. Each D2D pair DD$_n$ consists of a transmitter T_n and the corresponding receiver D_n. It is assumed that the spatial positions of CUs, D2D transmitters and Eves all obey the homogeneous PPP with the density λ_c, λ_d and λ_e, denoted as Φ_c, Φ_d, and Φ_e, respectively. The associated receiver with each D2D transmitter is located at a fixed distance away with isotropic direction [26]. The difference from [26] is that we consider the case where D2D pairs share the same resource block employed by cellular uplinks. In this case, the resource blocks among different CUs assigned by the serving BS are orthogonal so that there is no interference among different cellular links. Note that the BS, all the legitimate users, and Eves are equipped with single antennas.

In this paper, the large-scale fading and small-scale fading are considered for all the wireless channel models. For the large-scale fading model, we consider the standard path loss model, i.e., $l(r_{ij}) = {r_{ij}}^{-\kappa}$, where r_{ij} represents the distance between the nodes i and j, and $\kappa > 2$ denotes the path loss coefficient.

1) The base station will determine that the transceiver pair is not allowed to transmit its confidential messages employing the D2D mode if it has some security requirements; thus, we do not consider the security requirement for D2D links in this system model, just as in [21–24, 26].

For the small-scale fading, we adopt the independent quasi-static Rayleigh fading model and their channel gains follow the exponential distribution with unit mean.

The received signal-to-interference-plus-noise ratio (SINR) at D_n and E_k can be given by

$$\mathrm{SINR}_{D_n} = \frac{P_D r_D^{-\kappa} |h_{T_n D_n}|^2}{I_{D_n} + \sigma^2}, \tag{1}$$

$$\mathrm{SINR}_{E_k} = \frac{P_C r_{CE_k}^{-\kappa} |h_{CE_k}|^2}{I_{E_k} + \sigma^2}, \tag{2}$$

where $I_{D_n} = P_C r_{CD_n}^{-\kappa} |h_{CD_n}|^2 + \sum_{j \in \Phi_d, j \neq n} P_D r_{T_j D_n}^{-\kappa} |h_{T_j D_n}|^2$, $I_{E_k} = \sum_{n \in \Phi_d} P_D r_{T_n E_k}^{-\kappa} |h_{T_n E_k}|^2$. $h_{T_n D_n}$, $h_{T_j D_n}$ $(j \neq n)$, h_{CD_n}, h_{CE_k}, and $h_{T_n E_k}$ denote the small-scale fading over the links $T_n \to D_n$, $T_j \to D_n$, $C \to D_n$, $C \to E_k$, and $T_n \to E_k$, respectively. P_C and P_D are the transmission power of the CU and each D2D transmitter, respectively. r_D is the fixed distance between every associated D2D pair. It is assumed that the additive Gaussian noise at the BS, n-th receiver D_n and k-th Eve E_k all both follow the distribution $\mathcal{CN}(0, \sigma^2)$. In practical cases, the interference is generally much stronger than the noise power, especially in an ultra dense network (UDN), which is an important potential technology in 5G. Considering a special case where the cellular network is interference-limited and letting $\sigma^2 = 0$ without loss of generality, in that case, SINR will be equivalent to the signal-to-interference ratio (SIR).

2.2 Problem description

Just as in the open literature [20–26], we consider the security over cellular links and reliability over D2D links. In this paper, they are characterized by the SOP and COP, respectively. The SOP and COP are commonly used in the open literature. The COP is defined as the probability that the capacity of the legitimate channel is below the given target transmission rate [27], and the SOP is defined as the probability that the maximal capacity of the wiretap channels is above the given target secrecy rate [27, 28]. Furthermore, the received SINRs over different links determine their decoding capability, and thus reliable and secure transmission can be defined in terms of SINR. In the interference-limited networks considered in this paper, SIR is equivalent to SINR. Thus, the definition of COP and SOP can be rewritten as

$$p_{\mathrm{cop}} = \mathbb{P}\left(\mathrm{SIR} \leqslant \alpha\right), \tag{3}$$

$$p_{\mathrm{sop}} = \mathbb{P}\left(\mathrm{SIR}_e \geqslant \beta\right), \tag{4}$$

where SIR and SIR_e denote the received SIRs at the legitimate receiver and the reference Eve in the interference-limited network. α and β are the target SIR thresholds for reliable and secure communication, respectively.

In this paper, we first propose an opportunistic access control scheme based on wireless channel gains. The scheme not only could guarantee reliable communications under the interference constraint for legitimate users sharing the same resource, and further D2D transmitters can be regarded as friendly jammers to combat Eves overhearing confidential messages over the cellular links. Then, we respectively derive the expressions of the SOP of the CU and the COP of the D2D pair. To further support the system performance, we present an interference threshold optimization model to minimize the COP of D2D pairs subject to the secrecy requirement of the CU.

3 Opportunistic access control scheme based on wireless channel gains

In the proposed system model, multiple D2D pairs sharing the same cellular resource block will cause interference to both cellular links and other D2D links, influencing their performances. The communication reliability must be first guaranteed before D2D pairs are allowed to access this hybrid network. In practical communications, the performance of the hybrid network mainly depends on the strength of the interference, which is determined by wireless channel gains. To this end, we present an opportunistic

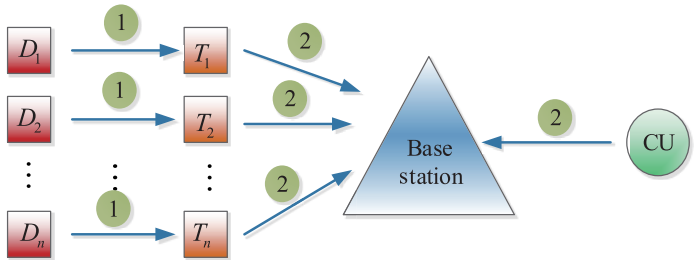

Figure 2 (Color online) Opportunistic access control scheme based on wireless channel gains.

access control scheme based on characteristics of wireless channels in this section. Distinguishing this work from [30], the transmission requirement over D2D links must be considered and we assume that cellular users also follow homogeneous PPP, which is more suitable to practical cases. Our proposed opportunistic access control scheme can be realized as follows, as shown in Figure 2.

(1) In the first slot, all the receivers of D2D pairs broadcast the reverse training sequences and all the transmitters can obtain the instantaneous channel statement information (CSI) from all the receivers of D2D pairs. According to the channel reciprocity in the time division duplex (TDD) system, the CSI from each transmitter of D2D pairs to all the receivers can also be obtained, which can characterize the interference among different D2D pairs sharing the same resource block. In order to satisfy the reliable communication of the n-th transmitter, the wireless channel gains from it to the receivers of the selected candidate D2D pairs (except for the n-th receiver) should lie in the set

$$\Re_{T_n} = \left\{ h_{T_n D_j} \left| \left| \hat{h}_{T_n D_j} \right|^2 \leqslant \delta_1 \ | n, j \in \Phi_d, \ j \neq n \right. \right\}, \tag{5}$$

where Φ_d^1 represents the candidate set of D2D pairs whose wireless gains satisfy the above criterion (5). $0 < \delta_1 < 1$ is the interference limitation threshold between different D2D pairs sharing the same cellular resource block. In a practical system, δ_1 should be limited to a certain range, neither too small nor too large. If it is too large, there are too many D2D pairs sharing the same cellular resource block, resulting in too much interference and degrading their reliable communications. If it is too small, this would result in a smaller number of available D2D pairs and lower spectrum efficiency.

(2) In the second slot, all the D2D transmitters will report the set of potential D2D pairs determined by the above criterion to the BS and broadcast their corresponding training sequences simultaneously. Hence, the BS can obtain the CSI from different D2D transmitters. Meanwhile, the CU broadcasts the training sequences, so the BS can obtain its CSI from the CU. In order to guarantee the communication reliability of the cellular link under the interference constraint induced by D2D links. The channel gains from the selected D2D transmitters to the BS should lie in the set

$$\Re_C = \left\{ h_{T_j B} \left| \left| \hat{h}_{T_j B} \right|^2 \leqslant \delta_2 \ | j \in \Phi_d \right. \right\}. \tag{6}$$

It is assumed that the selected candidate set of D2D pairs determined by the above criterion (6) is denoted as Φ_d^2. δ_2 should be set to a suitable value similar to the analysis of the value δ_1.

(3) Decision. The BS can easily obtain the set of D2D pairs that could simultaneously share the cellular resource block with the specific cellular resource block as determined by the two criteria above (5) and (6).

It is assumed that $|\hat{h}_{T_n D_j}|^2$ and $|\hat{h}_{T_n B}|^2$ follow the exponential distribution with unit mean, i.e., $|\hat{h}_{T_n D_j}|^2 \sim \exp(1)$ and $|\hat{h}_{T_n B}|^2 \sim \exp(1)$. Therefore, we can get the probability of $T_j \in \Phi_d^1$ as $\text{Prob}_1 = 1 - \exp(-\delta_1)$. Similarly, we can easily obtain the probability of $T_j \in \Phi_d^2$ as $\text{Prob}_2 = 1 - \exp(-\delta_2)$.

With the above proposed D2D pairs selection scheme, we define the resulting selected D2D pairs set sharing the same cellular resource block as Φ_d^s. Owing to the independence of channel gains between

different nodes, the probability of $T_j \in \Phi_d^s$, denoted as Prob_D, can be given by

$$\begin{aligned}\mathrm{Prob}_D &= \mathbb{P}\left(T_j \in \Phi_d^s\right)\\ &= \mathbb{P}\left(T_j \in \Phi_d^1 \cap T_j \in \Phi_d^2\right)\\ &= \left(1-\exp\left(-\delta_1\right)\right)\left(1-\exp\left(-\delta_2\right)\right), \quad j \neq n. \end{aligned} \tag{7}$$

According to the property of PPP [29], we can easily know that the resulting selected D2D pairs set sharing the same cellular resource block is a thinning of the homogeneous PPP of the intensity λ_d with the retention probability Prob_D. Hence the intensity λ_d^s of the resulting selected D2D pairs set can be obtained by

$$\lambda_d^s = \left(1-\exp\left(-\delta_1\right)\right)\left(1-\exp\left(-\delta_2\right)\right)\lambda_d. \tag{8}$$

In what follows, we will derive the SOP of the typical cellular link and COP of the typical D2D link to characterize their respectively different communication requirements according to the proposed scheme. Then we present an interference threshold optimization model to make this hybrid network to achieve its optimal performance.

4 Performance analysis and optimization

In this section, we respectively give the SOP of the typical cellular link and COP of the typical D2D link. Then, we discuss the impact of the interference thresholds (i.e., δ_1, δ_2) on their performances. To further support the performance of this hybrid network, we present an interference threshold optimization model to obtain the optimal interference thresholds by numerical solutions.

4.1 SOP of cellular links

Assuming that Eves are non-colluding, so their wireless channels could be regarded as a compound wiretap channel with the equivalent channel gain $\eta_e = \max_{E_k \in \Phi_E}(\mathrm{SIR}_{E_k})$. Consider the typical cellular link that comprises of the serving BS located at the origin and the typical CU located at x_c. For the k-th Eve located at z, its distance to the typical CU is denoted as $r_{CE} = \|x_c - z\|^2$. Then, for the given target SIR threshold β_e, setting $\rho = \frac{2}{\kappa}$, the SOP for the typical cellular link according to its definition in (4) can be derived as

$$\begin{aligned} p_c^{\mathrm{sop}} &= \mathbb{P}\left(\max_{k\in\Phi_e}\mathrm{SIR}_{E_k} \geqslant \beta_e\right)\\ &= 1-\mathbb{P}\left(\max_{k\in\Phi_e}\mathrm{SIR}_{E_k} < \beta_e\right)\\ &= 1-\mathrm{E}_{\Phi_e}\mathrm{E}_{\Phi_d^s}\left(\prod_{k\in\Phi_e}\Pr\left(\mathrm{SIR}_{E_k} < \beta_e\right)\right)\\ &= 1-\mathrm{E}_{\Phi_e}\left(\prod_{k\in\Phi_e}\Pr\left(\mathrm{E}_{\Phi_d^s}\left(\mathrm{SIR}_{E_k} < \beta_e\right)\right)\right)\\ &= 1-\mathrm{E}_{\Phi_e}\left(\prod_{k\in\Phi_e}\left(1-\exp\left(-\frac{\beta_e r_{CE}^{\kappa} I_E}{P_C}\right)\right)\right)\\ &= 1-\mathrm{E}_{\Phi_e}\left(\prod_{k\in\Phi_e}\left(1-\mathcal{L}_{I_E(z)}\left(P_C^{-1}\beta_e r_{CE}^{\kappa}\right)\right)\right)\\ &\overset{(a)}{=} 1-\exp\left(-2\pi\lambda_e\int_0^{\infty}\mathcal{L}_{I_E(z)}\left(P_C^{-1}\beta_e r_{CE}^{\kappa}\right)r_{CE}\mathrm{d}r_{CE}\right), \end{aligned} \tag{9}$$

where (a) follows from the probability generating functional (PGFL) of PPP [29]. According to the property of PPP, the coordinates translation will not change its distribution [29]. Now, we shift the

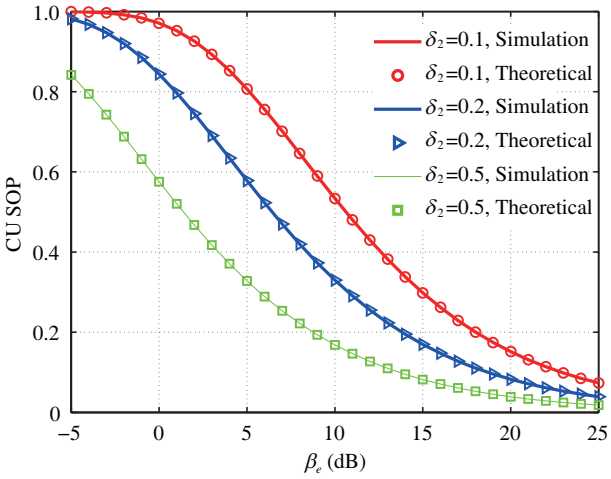

Figure 3 (Color online) CU SOP of the opportunistic access control scheme versus β_e.

coordinates such that the k-th Eve is located at the origin. Thus, $\mathcal{L}_{I_E}$ can replace $\mathcal{L}_{I_E(z)}$ which equals $\mathcal{L}_{I_E(z=0)}$. Then, employing [22, Eq. (7–10)], we obtain

$$\mathcal{L}_{I_E}\left(P_C^{-1}\beta_e r_{CE}^{\kappa}\right)=\exp\left(-\frac{\pi\lambda_d^s P_D^{\rho} s^{\rho}}{\sin c\delta}\right), \tag{10}$$

where $\frac{1}{\sin c\delta}=\frac{\pi\rho}{\sin\pi\rho}=\Gamma(1+\rho)\Gamma(1-\rho)$, $s=P_C^{-1}\beta_e r_{CE}^{\kappa}$, and $\Gamma(x)$ is the gamma function.

Setting $\Xi=\lambda_d^s(\frac{\beta_e P_D}{P_C})^{\rho}\Gamma(1+\rho)\Gamma(1-\rho)$ and substituting (10) into (9), the SOP of the typical cellular link can be given by

$$p_c^{\mathrm{sop}}=1-\exp\left(-\frac{\lambda_e}{\Xi}\right). \tag{11}$$

The theoretical results and the simulation results of the CU SOP in (11) are plotted in Figure 3. Intuitively, we can see that the theoretical curves are quite consistent with the simulations with respect to β_e under different interference thresholds, which validates the derived theoretical results.

4.2 COP of D2D links

In this subsection, we will give the expression of COP to characterize the performance of the typical D2D link under the interference constraint. According to the definition of COP in (3), the COP of D2D pairs that share the resource block with the specific CU can be expressed as

$$\begin{aligned}p_d^{\mathrm{cop}}&=\mathbb{P}\left\{\mathrm{SIR}_{D_n}\leqslant\beta_d\right\}\\&=\mathbb{P}\left\{|h_{D_n}|^2\leqslant P_D^{-1}r_D^{\kappa}\beta_d I_{D_n}\right\}\\&=1-\mathcal{L}_{I_{D_n}}(s_1),\end{aligned} \tag{12}$$

where $s_1=P_D^{-1}r_D^{\kappa}\beta_d$, $I_{D_n}=P_C r_{CD_n}^{-\kappa}|h_{CD_n}|^2+\sum_{j\in\Phi_d^s,j\neq n}P_D r_{T_jD_n}^{-\kappa}|h_{T_jD_n}|^2$, $\mathcal{L}_{I_{D_n}}(s)$ denotes the Laplace transform of I_{D_n}, i.e., $\mathcal{L}_{I_{D_n}}(s_1)=\mathrm{E}(-s_1 I_{D_n})$. Let $I_{D_n}=I_{I_{D_n}}^{c}+I_{I_{D_n}}^{d^o}$, where $I_{D_n}^{c}=P_C r_{CD_n}^{-\kappa}|h_{CD_n}|^2$ denotes the interference from the cellular link and $I_{D_n}^{d^o}=\sum_{j\in\Phi_d^s,j\neq n}P_D r_{T_jD_n}^{-\kappa}|h_{T_jD_n}|^2$ denotes the interference from other D2D transmitters (except for the typical D2D transmitter). According to the property of the Laplace transform, we can easily obtain $\mathcal{L}_{I_{D_n}}(s_1)=\mathcal{L}_{I_{D_n}^{c}}(s_1)\cdot\mathcal{L}_{I_{D_n}^{d^o}}(s_1)$. Owing to the Slivnyak-Mecke Theorem [32], we can get $\mathcal{L}_{I_{D_n}^{d^o}}(s_1)=\mathcal{L}_{I_{D_n}^{d}}(s_1)$, where $I_{D_n}^{d}=\sum_{j\in\Phi_d^s}P_D r_{T_jD_n}^{-\kappa}|h_{T_jD_n}|^2$. Similarly, employing [22, Eq. (7–10)], we can easily obtain

$$\mathcal{L}_{I_{D_n}^{d^o}}(s)=\exp\left(-\frac{\pi\lambda_d^s P_D^{\rho} s_1^{\rho}}{\sin c\rho}\right). \tag{13}$$

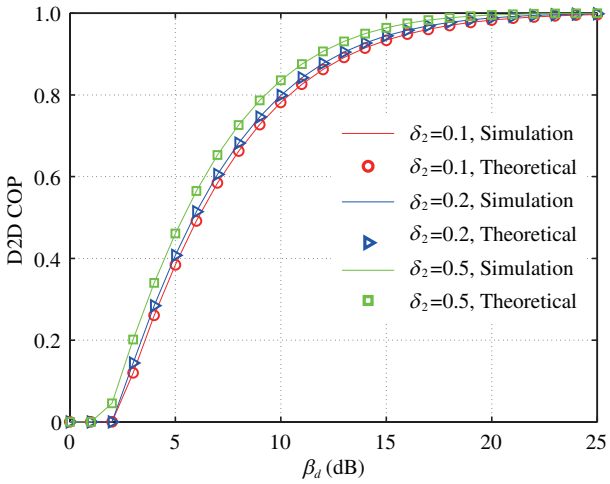

Figure 4 (Color online) D2D COP of the opportunistic access control scheme versus β_d.

Next we will give the expression of $\mathcal{L}_{I^c_{D_n}}(s_1)$. Let $\psi = \mathrm{E}[\exp(-s_1(P_C r_{CD_n}^{-\kappa}|h_{CD_n}|^2))]$. Assuming $r = r_{CD_n}$, which is Rayleigh distributed, its probability density function (PDF) can be given by $f_x(r) = 2\pi\lambda_c r\exp(-\pi\lambda_c r^2)$ [33]. Hence, ψ can be calculated by

$$\begin{aligned}\psi &= \mathrm{E}\left[\mathrm{E}_{|h_{CD_n}|^2}\left[\exp\left(-s_1\left(P_C r^{-\kappa}|h_{CD_n}|^2\right)\right)\right]\right]\\ &\overset{\text{(b)}}{=} \int_0^\infty 2\pi\lambda_c r\exp\left(-\pi\lambda_c r^2\right)\frac{1}{1+s_1P_C r^{-\kappa}}\mathrm{d}r\\ &= \int_0^\infty \frac{\exp(-x)}{1+bx^{-\rho}}\mathrm{d}x,\end{aligned} \tag{14}$$

where $x = \pi\lambda_c r^2$ and $b = s_1P_C(\pi\lambda_c)^\rho$. Assuming $h \sim \exp(1)$, we can easily get $\mathrm{E}_h[\exp(-hA)] = \frac{1}{A+1}$ for any constant A . In the Rayleigh fading channel, (b) can be obtained according to the above property of the exponential distribution. Then substituting (14) and (13) into (12), we can obtain

$$p_d^{\mathrm{cop}} = 1 - \int_0^\infty \frac{\exp(-x)}{1+bx^{-\rho}}\mathrm{d}x\cdot\exp\left(-\frac{\pi\lambda_d^s r_D^2\beta_d{}^\rho}{\sin c\rho}\right). \tag{15}$$

Figure 4 presents the simulation results and the theoretical results of D2D COP in (15), where we can see that the theoretical curves coincide very well with the simulations with respect to β_d under different interference thresholds, which validates the derived analytical results.

4.3 Performance optimization

The performances of the typical cellular link and the typical D2D link are respectively derived for the fixed interference thresholds δ_1, δ_2 in the two previous subsections. To further support the performance of this hybrid network, we present an interference threshold optimization model in this subsection, which minimizes the COP of D2D pairs subject to the secrecy requirement of the cellular link.

For this hybrid network, cellular users have higher priorities and their performances should be guaranteed before D2D pairs are allowed to access the hybrid network. In other words, their secrecy requirements must first be fulfilled, as long as their SOP are no larger than a certain value, denoted by ϵ. To achieve the optimal performance for this hybrid network, the COP of D2D pairs sharing the same cellular resource block should be as small as possible, subject to their secrecy requirements of CUs. Hence, the D2D COP minimization problem under the constraint of secrecy requirements can be given as follows:

$$\begin{aligned}\min_{\delta_1,\delta_2}\ & p_d^{\mathrm{cop}}(\delta_1,\delta_2)\\ \text{s.t.}\ & \mathrm{C1}:\ p_{\mathrm{sop}}^c \leqslant \epsilon,\\ & \mathrm{C2}:\ \delta_1\in[0,\delta_1^{\mathrm{up}}],\ \delta_2\in[0,\delta_2^{\mathrm{up}}],\end{aligned} \tag{16}$$

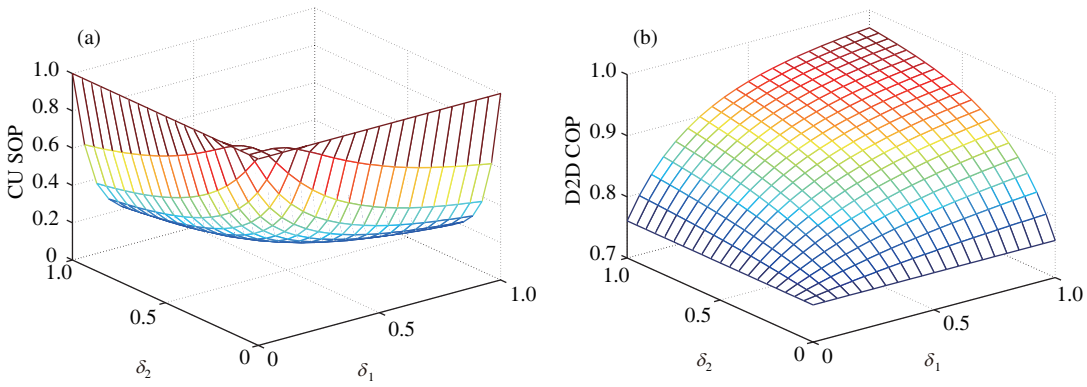

Figure 5 (Color online) Performance versus different interference thresholds. (a) CU SOP; (b) D2D COP.

where ϵ represents the minimum secrecy requirement of the typical CU. $\delta_1^{\rm up}$ and $\delta_2^{\rm up}$ denote the upper interference thresholds to satisfy the reliable communications for both CUs and D2D pairs.

On the other hand, from (11), we can easily observe that the SOP of the CU, i.e., $p_c^{\rm sop}$, decreases as the interference thresholds δ_1 and δ_2 increase, as illustrated in Figure 5(a). However, it is the opposite for the COP of D2D pairs versus δ_1, δ_2, as shown in Figure 5(b). That is, for D2D links, δ_1, δ_2 should be as small as possible to achieve their minimum COP. Unfortunately, we cannot obtain analytical solutions from (16). However, we can obtain numerical results of the optimal interference thresholds employing a two-dimensional search in the feasible solutions $(\tilde{\delta}_1, \tilde{\delta}_2)$ obtained by the constraint C1 in (16), which could satisfy the secrecy requirement of the CU. The optimal values of δ_1^*, δ_2^* should be those in the set $(\tilde{\delta}_1, \tilde{\delta}_2)$ to minimize the COP of D2D pairs. Based on the above analysis, we can get the optimal values, i.e., δ_1^*, δ_2^*, by

$$(\delta_1^*, \delta_2^*) = \min_{\delta_1, \delta_2} \; p_d^{\rm cop}\left(\tilde{\delta}_1, \tilde{\delta}_2\right). \tag{17}$$

Based on the above analysis, we present Algorithm 1 to numerically determine the optimal values δ_1^*, δ_2^* of the interference thresholds for cellular links and D2D links, respectively. In Algorithm 1, we respectively denote the step size of δ_1, δ_2 as $\Delta\delta_1$, $\Delta\delta_2$.

Algorithm 1 Search algorithm for obtaining optimal values δ_1^*, δ_2^*

Input: κ, λ_c, λ_d, λ_e, P_C, P_D, β_e, β_d, $\delta_1^{\rm up}$, $\delta_2^{\rm up}$, ϵ, $\Delta\delta_1$, $\Delta\delta_2$;
Output: δ_1^*, δ_2^*;
Initialization: $M{=}\frac{\delta_1^{\rm up}}{\Delta\delta_1}$, $N{=}\frac{\delta_2^{\rm up}}{\Delta\delta_2}$, and set $P_d^{\rm temp} = 1$;
for $m = 1 : M$ **do**
  for $n = 1 : N$ **do**
    Calculate $P_c^{\rm sop}(m, n)$ in (11);
    if $P_c^{\rm sop}(m, n) \leqslant \varepsilon$ **then**
      Update the set $(\tilde{\delta}_1, \tilde{\delta}_2)$ by putting $\Delta\delta_1 * m$, $\Delta\delta_2 * n$ into the set $(\tilde{\delta}_1, \tilde{\delta}_2)$;
    end if
  end for
end for
Set L as the number of entries in the determined set $\tilde{\delta}_1$ and $\tilde{\delta}_2$. That is, $L = {\rm Card}(\tilde{\delta}_1) = {\rm Card}(\tilde{\delta}_2)$.
for $l = 1 : L$ **do**
  Calculate $P_d^{\rm cop}$ by substituting the entries δ_{1l}, δ_{2l} into (15) that lie in the determined set $(\tilde{\delta}_1, \tilde{\delta}_2)$;
  if $P_d^{\rm cop} < P_d^{\rm temp}$ **then**
    $P_d^{\rm temp} = P_d^{\rm cop}$;
    Update δ_1^*, δ_2^* by $\delta_1^* = \delta_{1l}$, $\delta_2^* = \delta_{2l}$;
  end if
end for
Return δ_1^*, δ_2^*; (The optimal values are obtained.)

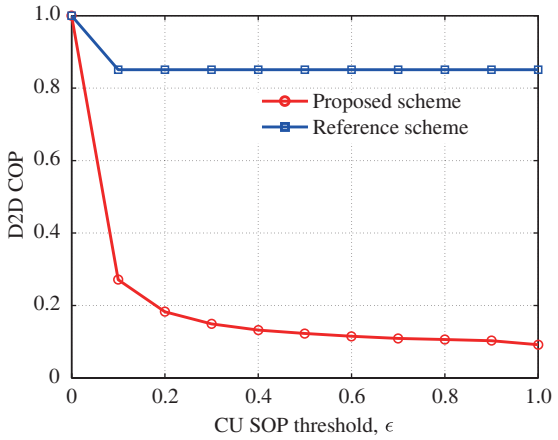

Figure 6 (Color online) D2D COP versus CU SOP threshold ϵ.

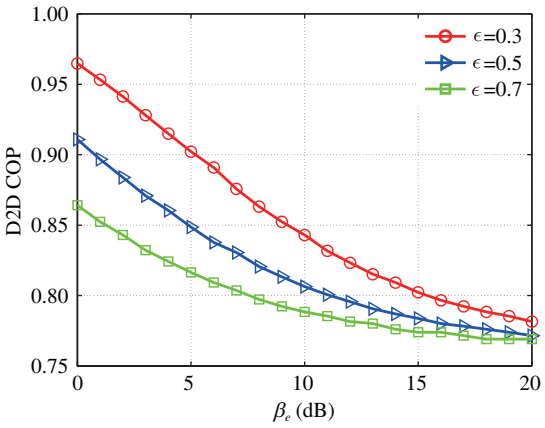

Figure 7 (Color online) D2D COP versus β_e under different threshold ϵ.

5 Simulation results

In this section, more detailed simulation and numerical results are provided to evaluate and analyze the performance of our proposed scheme. The path loss coefficient is set as $\kappa = 3$. The transmission power of the CU and each D2D transmitter are 20 and 10 dBm, respectively. The densities of cellular users, D2D pairs and Eves are set as $\lambda_c = 0.01/\mathrm{m}^2$, $\lambda_d = 0.1/\mathrm{m}^2$ and $\lambda_e = 0.01/\mathrm{m}^2$. For simplicity, the distance between D2D pairs is 1 m. δ_1^{up} and δ_2^{up} are set as $\delta_1^{\mathrm{up}} = \delta_2^{\mathrm{up}} = 1$. The step sizes of δ_1, δ_2 are set as $\Delta\delta_1 = 0.05$ and $\Delta\delta_2 = 0.05$. The following results are obtained with the optimal interference thresholds obtained from Algorithm 1 under different specific parameters.

In Figure 6, we plot the COP of the typical D2D link versus the SOP threshold of the CU, i.e., ϵ, which means its different secrecy requirements. The reference one in which all the D2D pairs share the same resource block in [26] without considering the interference constraint for CU and other D2D pairs, is presented for comparison. As expected, we can see that the D2D COP of our proposed scheme is lower than that of the reference scheme. This is because our proposed scheme considers the interference constraints for other D2D links. Furthermore, it is observed from Figure 6 that the COP of D2D pairs decreases as the cellular SOP threshold ϵ increases. The reason for this is that the secrecy requirement becomes lower with the increasing ϵ. In that case, the interference induced by the smaller number of D2D pairs sharing the same resource block with the CU would deteriorate the received performance of Eves to satisfy the secrecy requirement of the CU. Meanwhile, it will result in lower COP of D2D pairs, because the harmful interference among D2D pairs sharing the same resource block will be weaker.

We exploit the relationship of the COP of D2D pairs with β_e under different secrecy requirements, where β_d is set as 10 dB, as shown in Figure 7. It can be observed that the COP will decrease as β_e increases, and it is the same with ϵ increasing. The reason for this is that the secrecy requirement could be satisfied if only a smaller number of D2D pairs share the same resource block with higher β_e when ϵ is fixed, resulting in the lower COP. On the other hand, when the β_e is permanent, the requirement could be fulfilled if only a larger number of D2D pairs reuse the specific cellular resource under a lower ϵ, resulting in the higher COP.

Figure 8 demonstrates the performance of D2D pairs subject to different secrecy requirements of the CU, denoted as ϵ. As expected, we can see that the COP will increase as ϵ decreases. The smaller ϵ means the CU has a higher-level requirement. In practical cases, only if a larger number of D2D pair share the same resource block can the interference induced by D2D pairs fulfill its higher-secrecy requirement. However the stronger interference will result in a higher COP of D2D pairs.

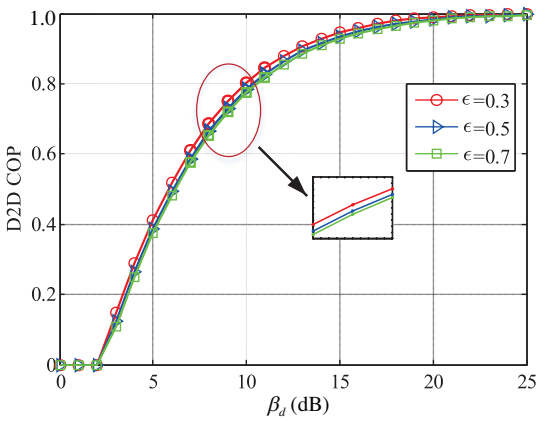

Figure 8 (Color online) D2D COP versus β_d under different threshold ϵ.

6 Conclusion

The secure communication of cellular links in D2D-enabled cellular networks was studied. An opportunistic access control scheme based on wireless channel gains has been proposed. Then, we analyzed the performance of the typical cellular and D2D links based on the proposed scheme. To further support the performance of this hybrid network, we presented an interference threshold optimization model for D2D pairs, which guaranteed the secrecy requirement of the CU owing to its higher priority. Simulation results have been provided to validate the effectiveness of our proposed scheme. Because in this paper we only considered single-input single-output (SISO) channels, the extension of the proposed scheme to the scenario of multiple-input multiple-output (MIMO) systems may be carried out in our future work.

Acknowledgements This work was supported in part by National High Technology Research and Development Program of China (863) (Grant No. SS2015AA011306), Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (Grant No. 2013D09) and National Natural Science Foundation of China (Grant Nos. 61379006, 61521003, 61401510).

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Agiwal M, Roy A, Saxena N. Next generation 5G wireless networks: a comprehensive survey. IEEE Commun Surv Tut, 2016, 18: 1617–1655
2 Asadi A, Wang Q, Mancuso V. A survey on device-to-device communication in cellular networks. IEEE Commun Surv Tut, 2014, 16: 1801–1819
3 Phunchongharn P, Hossain E, Kim D I. Resource allocation for device-to-device communications underlaying LTE-advanced networks. IEEE Wirel Commun, 2013, 20: 91–100
4 Ding G R, Wang J L, Wu Q H, et al. Cellular-base-station-assisted device-to-device communications in TV white space. IEEE J Sel Areas Commun, 2016, 34: 107–121
5 Yu G D, Xu L K, Feng D Q. Joint mode selection and resource allocation for device-to-device communications. IEEE Trans Commun, 2014, 62: 3814–3824
6 Li B, Fei Z S, Chen H B. Robust artificial noise-aided secure beamforming in wireless-powered non-regenerative relay. IEEE Access, 2016, 4: 7921–7929
7 Li B, Fei Z S. Robust beamforming and cooperative jamming for secure transmission in DF relay systems. EURASIP J Wirel Commun, 2016, 1: 1–11
8 Zhang L J, Jin L, Luo W Y, et al. Robust secure transmission for multiuser MISO systems with probabilistic QoS constraints. Sci China Inf Sci, 2016, 59: 022309
9 Khisti A, Wornell G. Secure transmission with multiple antennas-part I: the MISOME wiretap channel. IEEE Trans Inf Theory, 2010, 56: 3088–3104
10 Bloch M, Barros J, Rodrigues M R D, et al. Wireless information theoretic security. IEEE Trans Inf Theory, 2011, 54: 2515–2534
11 Li B, Fei Z S, Chu Z, et al. Secure transmission for heterogeneous cellular networks with wireless information and power transfer. IEEE Syst J, 2017. doi: 10.1109/JSYST.2017.2713881

12 Xiong J, Cheng L W, Ma D T, et al. Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems. IEEE Trans Veh Tech, 2016, 65: 7274–7284
13 Cheng L W, Li W, Ma D T, et al. Moving window scheme for extracting secret keys in stationary environments. IET Commun, 2016, 10: 2206–2214
14 Ji X S, Yang Y, Huang K Z, et al. Physical layer authentication scheme based on hash method. J Electron Inf Technol, 2016, 38: 2900–2907
15 Alam M, Yang D, Rodriguez J, et al. Secure device-to-device communication in LTE-A. IEEE Commun Mag, 2014, 52: 66–73
16 Zhu D H, Swindlehurst A L, Fakoorian S A A, et al. Device-to-device communications: the physical layer security advantage. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Florence, 2014. 1606–1610
17 Kang X L, Ji X S, Huang K Z. Secure D2D underlaying cellular communication based on artificial noise assisted. J Commun, 2015, 36: 149–156
18 Kang X L, Ji X S, Huang K Z, et al. Secure D2D communication underlaying cellular networks: artificial noise assisted. In: Proceedings of IEEE International Conference on Vehicular Technology (VTC), Montreal, 2016
19 Chen Y J, Ji X S, Huang K Z, et al. Secrecy-outage-probability-based access strategy for device-to-device communications underlaying cellular networks. J Commun, 2016, 37: 86–94
20 Yue J T, Ma C, Yu H, et al. Secrecy-based channel assignment for device-to-device communication: an auction approach. In: Proceedings of IEEE International Conference on Wireless Communications and Signal Processing (WCSP), Hangzhou, 2013. 1–6
21 Chu Z, Cumanan K, Xu M, et al. Robust secrecy rate optimizations for multiuser multiple-input-single-output channel with device-to-device communications. IET Commun, 2015, 9: 396–403
22 Zhang H, Wang T Y, Song L Y, et al. Radio resource allocation for physical-layer security in D2D underlay communications. In: Proceedings of IEEE International Conference on Communications (ICC), Sydney, 2014. 2319–2324
23 Sun L, Du Q H, Ren P Y, et al. Two birds with one stone: towards secure and interference-free D2D transmissions via constellation rotation. IEEE Trans Veh Tech, 2016, 65: 8767–8774
24 Li W, Wu H Q, Song M, et al. Secrecy-oriented resource sharing for cellular device-to-device underlay. In: Proceedings of IEEE International Conference on Global Communications Conference (GLOBECOM), San Diego, 2015. 1–5
25 Zhang R Q, Cheng X, Yang L Q. Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks. IEEE Trans Wirel Commun, 2016, 15: 5651–5663
26 Ma C, Liu J Q, Tian X H, et al. Interference exploitation in D2D-enabled cellular networks: a secrecy perspective. IEEE Trans Commun, 2015, 63: 229–242
27 Xu X M, He B, Yang W W, et al. Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers. IEEE Trans Inf Foren Secur, 2016, 11: 373–387
28 Wang C, Wang H M, Xia X G. Uncoordinated jammer selection for securing SIMOME wiretap channels: a stochastic geometry approach. IEEE Trans Wirel Commun, 2015, 14: 2596–2612
29 Stoyan D, Kendall W S, Mecke J. Stochastic Geometry and Its Applications. 2nd ed. Hoboken: Wiley, 1996
30 Wang C, Wang H M. Opportunistic jamming for enhancing security: stochastic geometry modeling and analysis. IEEE Trans Veh Tech, 2016, 14: 2596–2612
31 Zhou X Y, Ganti R, Andrews J, et al. Physical layer security in cellular networks: a stochastic geometry approach. IEEE Trans Wirel Commun, 2013, 12: 2776–2787
32 Haenggi M, Ganti R K. Interference in large wireless networks. Found Trends Netw, 2008, 3: 127–248
33 Haenggi M. On distances in uniformly random networks. IEEE Trans Inf Theory, 2005, 51: 3584–3586