Chen *et al. EURASIP Journal on Wireless Communications and Networking* (2017) 2017:178
DOI 10.1186/s13638-017-0969-1

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Artificial noise-assisted physical layer security in D2D-enabled cellular networks

Yajun Chen[1*], Xinsheng Ji[1,2,3], Kaizhi Huang[1], Jing Yang[1], Xin Hu[1] and Yunjia Xu[1]

Abstract

Device-to-device (D2D) communication has been deemed as a promising technology in the next generation 5G wireless communication. Due to the openness nature of the transmission medium, secure transmission is also a critical issue in the D2D-enabled cellular network as well as other wireless systems. In this paper, we investigate secure communication for the cellular downlink in this hybrid network. We consider a case in which each base station has no channel state information (CSI) from D2D transmitters which are generally deployed in the cell edge. To guarantee the secure communication of the cellular link, each base station employs the artificial noise assisted transmission strategy. Firstly, we derive the close-form expression and asymptotic expression of the secrecy outage probability of the cellular link in different scenarios: (I) eavesdroppers having no multi-user decedability; (II) eavesdroppers having the multi-user decedability. Then, we comprehensively discuss the impacts of some main system parameters on the performance to provide some system design guidances. To characterize the reliable communication of the typical D2D link, the close-form expression and asymptotic expression of the connection outage probability are, respectively, derived and some comprehensive analysis are presented. Finally, simulation results are provided to validate the effectiveness of theoretical analysis.

Keywords: Device-to-device (D2D) communication, Physical layer security, Artificial noise, Secrecy outage probability, Connection outage probability

1 Introduction

To meet the explosive demand of proximity services, device-to-device (D2D) communication has been regarded as an ideal candidate technology for the next generation 5G wireless communication. D2D communication allows proximity user equipments to deliver their own messages over the direct link established between them without the base station relaying messages, which has the promise of many types of advantages: superior spectrum efficiency, increasing quality of service (QoS) of edge users and network capacity. Accordingly, D2D communication underlaying a cellular network has attracted remarkable attention both in the world of academia [1–3] and industry [4, 5] in recent years.

Due to the openness nature of the transmission medium, secure transmission is identified as a critical challenge facing the D2D-enabled cellular network as well as other wireless systems. As a remedy of the traditional security mechanism, the concept of physical layer security (PHY-security) has been proposed recently to achieve secure communication for wireless systems by exploiting the characteristics of wireless channels.

1.1 Related works

Recently, PHY-security in the D2D-enabled cellular network has sparked of wide interests and achieved fruitful research works in many different scenarios. To the best of our knowledge, most of works designed different resource-scheduling schemes to guarantee secure communication for the cellular uplink, such as [6–11]. More specifically, the literature above employed the hybrid interference to improve secure performance for the cellular uplink.

For the cellular downlink, Liu et al. proposed a power transfer model and an information signal model to enable wireless energy harvesting and secure information transmission in larger-scale cognitive cellular networks and

*Correspondence: chenyajun_cool@126.com
[1]National Digital Switching System Engineering and Technological R&D Center, No.7, Jianxue Road, 450002 Zhengzhou, China
Full list of author information is available at the end of the article

comprehensively discussed wireless power transfer policies and secrecy performance in [12]. More particularly, the authors in [13] designed two optimal D2D link-scheduling schemes under different criteria when each base station has a single antenna. When a base station is equipped with multi-antenna, the space redundancy could be exploited to enhance secure communication for the cellular link through some designed schemes, such as the secure beamforming and artificial noise assisted scheme. Specifically, Chu et al. investigated robust secrecy rate optimization problems for a multiple-input single-output (MISO) secrecy channel with multiple D2D communications, which was equivalently converted into the power minimization problem and the secrecy rate maximization problem to design the robust secure beamforming in [14]. The authors in [15] investigated a secure wireless powered D2D communication, in which a base station charged for D2D transmitters in wireless energy transfer phase and introduced the jamming service to interfere with the multiple eavesdroppers.

On the other hand, artificial noise-assisted scheme in the field of PHY-security is the most representative one among different schemes assuring the security of the wireless communication in MISO or multi-input multi-output (MIMO) scenario [16, 17]. The design idea of the artificial noise assisted scheme is that legitimate transmitters inject artificial noise into their transmission signals to confuse malicious eavesdroppers. Meanwhile, in order to guarantee the reliable communication of the legitimate user as much as possible, the artificial noise should be injected into the null space of the main channel (from source to destination). The authors in [18, 19] have expended the artificial noise-assisted scheme to the MISO D2D-enabled cellular network. More particularly, they designed the corresponding artificial noise-assisted beamforming vector matrix under the assumption that the channel state information (CSI) from each D2D transmitter is perfectly known at each base station.

Nevertheless, they only considered one cellular user and one D2D pair within a cell, which only focused on the point-to-point link and ignored the interference from other neighbor cells [18, 19]. On the other hand, due to the original purpose of the D2D communication, the D2D transmitter is generally deployed in the cell edge. Hence, in practical cases, CSI between each base station and each D2D transmitter is difficult to be perfectly known at each base station due to the channel estimation and quantization errors.

1.2 Motivation and contributions

Motivated by the abovementioned observations, in this paper, we consider a case in which each base station only knows CSI from the served cellular user, but does not know CSI from each D2D transmitter. Firstly, the spatial locations of base stations, cellular users, D2D pairs and eavesdroppers within a cell are modeled as independent homogeneous Poisson Point Processes (HPPP). In order to guarantee secure transmission for the cellular link, each multi-antenna base station employs the artificial noise assisted transmission strategy. Then, we derive the secrecy outage probability of the cellular link and provide some comprehensive analysis. Then, we, respectively, derive the connection outage probability of the typical D2D link to characterize its reliable communication. Specially, our main contributions can be summarized as follows:

- In this hybrid network, we consider a case in which each base station has no CSI from each D2D transmitter generally deployed in the cell edge. To guarantee the secure communication for the cellular link, it is assumed that each base station employs the artificial noise-assisted transmission scheme. The close-form expression and asymptotic expression of secrecy outage probability of the typical cellular link are derived in the scenario in which eavesdroppers do not have the multi-user decodability. Based on the derived result of secrecy outage probability, we provide some comprehensive analysis on the secrecy performance of the cellular link.
- Then, when eavesdroppers have the multi-user decodability, the close-form expression and asymptotic expression of secrecy outage probability of the typical cellular link are also, respectively, derived. Based on derived results of the secrecy outage probability in this case, some comprehensive analysis are also provided to guide the system design.
- Finally, according to the design of the artificial noise assisted transmission scheme, the artificial noise is just injected into the null space of the cellular channel because each base station does not know CSI from each D2D transmitter. Hence, the artificial noise and the information-bearing signal could all degrade the reliable communication of the typical D2D link. In order to characterize the reliable performance, we analytically derive the close-form expression and the asymptotic expression of connection outage probability, and provide some comprehensive analysis.

1.3 Organization and notations

The reminder of this paper is organized as follows. In Section 2, we present the system model. In Section 3, the secrecy outage probability of the typical cellular link, the connection outage probability of the typical D2D link are respectively derived and some corresponding analysis are provided. Simulation results are presented in Section 4. Finally, we conclude this paper in Section 5.

Notations: Bold letters mean matrices (column vectors). We use $\mathcal{CN}(\mu, N_0)$ to denote the circularly symmetric complex Gaussian with mean μ and covariance N_0. $\mathbb{P}\{\bullet\}$ represents the probability of an input event and the notation $\mathbb{E}\{\bullet\}$ denotes the statistical expectation. exp (1) denotes the exponential distribution with unit mean. Gamma (N, λ) is Gamma distribution with parameters N and λ . In addition, $\|\bullet\|$ denotes euclidean norm and $(\bullet)^T$ means the transpose of the input matrix. $\kappa_n \triangleq \Gamma(n-1+\rho)\Gamma(1-\rho)/\Gamma(n-1)$ and $\Gamma(x)$ is gamma function.

2 System model

2.1 Network model

As illustrated in Fig. 1, we consider the cellular downlink between the base station and the cellular user in which a set of malicious eavesdroppers attempt to intercept the confidential message of the cellular link in a passive way without modifying it. Each D2D pair DD_n consists of a transmitter T_n and its associated receiver D_n. The spatial locations of base stations, cellular users, D2D transmitters, eavesdroppers, denoted as Φ_b, Φ_c, Φ_d, Φ_e, are modeled as HPPP with the intensities λ_b, λ_c, λ_d, λ_e over the two-dimensional space, respectively. The associated receiver with its corresponding D2D transmitter is located at a fixed distance away with the isotropic direction. It is assumed that each legitimate user (including cellular users and D2D pairs) and eavesdropper is equipped with a single antenna, respectively. Each base station has M antennas where $M \geq 2$.

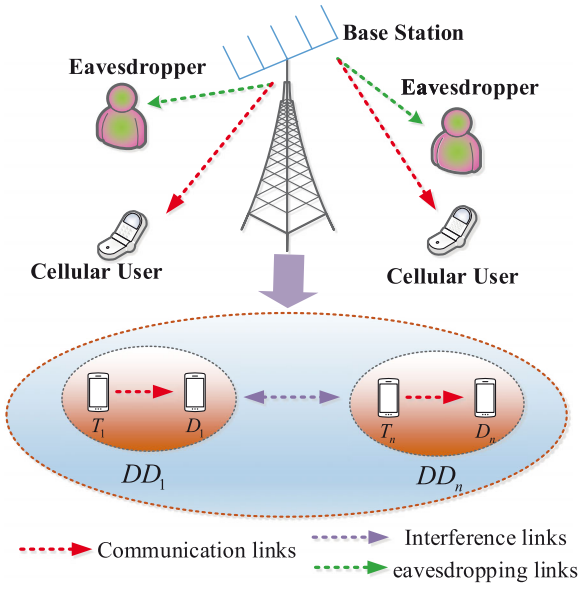

Fig. 1 System model. Figure 1 depicts the cellular downlink between the base station and the cellular user in which a set of malicious eavesdroppers attempt to intercept the confidential message of the cellular link in a passive way

Both the large-scale fading and small-scale fading of wireless channels are considered in this paper. The standard path loss model is taken into account for the large-scale fading, i.e., $l(r_{ij}) = r_{ij}^{-\alpha}$, where r_{ij} is the distance between the node i and the node j, and $\alpha > 2$ represents the fading coefficient. In addition, the small-scale fading imposes the independent quasi-static Rayleigh fading model, whose coefficient is constant for each transmission block.

2.2 Artificial noise-assisted transmission scheme and wiretap code

To guarantee secure transmission of the cellular link, every multi-antenna base station employs the artificial noise-assisted transmission scheme to confuse malicious eavesdroppers. Consequently, the transmitted signal $\mathbf{u}_i$ of the base station located at x_i can be expressed as:

$$\mathbf{u}_i = \sqrt{p_I}\mathbf{w}_i s_i + \sqrt{p_A}\mathbf{W}_i\mathbf{v}_i, \tag{1}$$

where s_i is the information-bearing signal with $\mathbb{E}\left[|s_i|^2\right] = 1$, $\mathbf{v}_i \in \mathbb{C}^{(M-1)\times 1}$ is an artificial noise vector with independent identically distributed (i.i.d.) entries $v_{i,n} \sim \mathcal{CN}\left(0, \frac{1}{M-1}\right)$. $p_I = \phi p$ is the allocated transmission power to the information-bearing signal and $p_A = (1-\phi)p$ represents the allocated transmission power to generate the artificial noise at each base station to confuse malicious eavesdroppers, where p is the total transmission power. Thus, $\phi \in [0,1]$ represents the ratio of the total transmission power p allocated to transmit the information-bearing signal s_i. In addition, $\mathbf{h}_i$ means the wireless channel between each base station and the served cellular user. We consider a case in which it is assumed that CSI between each base station and D2D users is unknown at each base station because D2D users are generally deployed in the cell edge in practical cases. According to the design of the artificial noise-assisted transmission scheme, the beamforming vector $\mathbf{w}_i$ for the served cellular user should satisfy $\mathbf{w}_i = \mathbf{h}_i^+ / \|\mathbf{h}_i\|$. $\mathbf{W}_i \in \mathbb{C}^{M\times(M-1)}$ is a weight matrix for the artificial noise, and the columns of $\mathbf{W} \triangleq [\mathbf{w}_i \mathbf{W}_i]$ constitute an orthogonal basis.

To improve the secrecy performance of this hybrid network, all transmitters adopt the wiretap code scheme to encode the data before transmission. More specifically, it is assumed that the rate of the transmitted codeword and the rate of the confidential message are, respectively, denoted by R_b and R_s. The codeword rate R_b is the actual transmission rate of the codewords, while the secrecy rate R_s is the rate of the embedded message. The rate redundancy $R_e = R_b - R_s$ is intentionally

added in order to provide secrecy against malicious eavesdroppers. More discussions on code construction can be found in [20].

2.3 Performance metrics

In this paper, we mainly focus on two performance metrics: secrecy outage probability and connection outage probability to respectively characterize the performance of the cellular link and D2D link in this hybrid network. Based on the analysis above, we next will give their definitions.

When the capacity of the channel from the legitimate transmitter to the corresponding receiver falls below the predefined target codeword rate R_b, the receiver will not decode the transmission message correctly. We define the probability of this event as connection outage probability [21].

In addition, when the capacity of the most detrimental one among multiple eavesdroppers (i.e., the eavesdropper having the maximal capacity of the channel from the legitimate transmitter to multiple eavesdroppers) is above the predefined target rate redundancy R_e, confidential messages for legitimate receivers will be decoded correctly and obtained by malicious eavesdroppers. We define the probability of this event as secrecy outage probability [21][1].

In practical cases, the capacity of the channel is determined by signal-to-interference-plus-noise ratio (SINR) according to Shannon Theorem. Hence, the two outage probabilities above can be redefined in terms of SINR. To be specific, connection outage will happen if the instantaneous SINR falls below the target SINR threshold for the main channel. What is more, secrecy outage will occur if the instantaneous SINR is above the target SINR threshold for the most detrimental eavesdropper. Thus, the definition of connection outage probability and secrecy outage probability can be rewritten as:

$$p_{cop} = \mathbb{P}\left(\mathrm{SINR} \leq \alpha\right), \tag{2}$$

$$p_{sop} = \mathbb{P}\left(\mathrm{SINR}_e \geq \beta\right), \tag{3}$$

where SINR and SINR_e respectively, denote the received SINR at the legitimate receiver and the most detrimental eavesdropper. α and β are the target SINR thresholds for reliable and secure communication, respectively.

2.4 Cellular user association

In this paper, we consider that each user is served by the nearest base station. In this hybrid network, the cellular user should be assigned the orthogonal resource before D2D being allowed to share the cellular resource block. However, some base stations may not serve any cellular user [22], which do not transmit any signal and are called inactive base stations. Just as in [22] and [23], we denote the probability that a base station being active as p_a, which can be given by:

$$p_a = 1 - \left(1 + \frac{\delta}{\varsigma}\right)^{-\varsigma}, \tag{4}$$

where $\varsigma = 3.5$ for the nearest base station association scheme and $\delta = \lambda_c / \lambda_b$ represents the cell load. Note that when there are more than one cellular users to be served by a base station, the base station just chooses one cellular user to serve at each time slot through the time-division multiple access (TDMA) scheme[2].

3 Outage probabilities analysis

In the section, we will conduct the performance analysis about the security of the typical cellular link and the reliability of the typical D2D link, respectively. Firstly, considering whether eavesdroppers have the multi-user decedability or not, we derive the close-form expression and asymptotic expression of the secrecy outage probability of the cellular link in two different scenarios in the non-colluding way. Then, for the typical D2D link, we consider its reliable communication and derive the close-form expression and asymptotic expression of the connection outage probability.

3.1 Secrecy outage probability of cellular links

In this subsection, we will conduct the secrecy performance analysis for the cellular link and derive the secrecy outage probability of the cellular link in two different scenarios depending on whether eavesdroppers have the multi-user decedability or not. Due to the property of PPP that its distribution will not be changed by shifting the coordinates, we firstly shift the coordinates to put the typical base station located at the origin.

In the system model, eavesdroppers work in a non-colluding way, the most detrimental eavesdropper is the one who has the largest SINR. According to the definition of the secrecy outage probability, secrecy outage will occur when the instantaneous SINR of the most detrimental eavesdropper is above the given target threshold SINR. Consequently, if the given target SINR threshold is set as $\hat{\gamma}_e$, the secrecy outage probability of the typical cellular link for the eavesdropper located at x_z can be calculated as:

$$
\begin{aligned}
P_{c,sop} &= \mathbb{P}\left(\max_{x_z\in\Phi_e} \mathrm{SINR}_e\left(x_z\right) \geq \hat{\gamma}_e\right) \\
&= 1-\mathbb{P}\left(\max_{x_z\in\Phi_e} \mathrm{SINR}_e\left(x_z\right) \leq \hat{\gamma}_e\right) \\
&= 1-\mathbb{P}\left(\bigcap_{x_z\in\Phi_e} \mathrm{SINR}_e\left(x_z\right) \leq \hat{\gamma}_e\right) \\
&= 1-\mathbb{E}_{\Phi_e,\Phi_b^a}\left(\left(\bigcap_{x_z\in\Phi_e} \mathrm{SINR}_e\left(x_z\right) \leq \hat{\gamma}_e \middle| \Phi_e, \Phi_b^a\right)\right) \\
&\overset{(a)}{=} 1-\mathbb{E}_{\Phi_b^a}\left\{\mathbb{E}_{\Phi_e}\left\{\prod_{x_z\in\Phi_e}\left(\mathrm{SINR}_e\left(x_z\right) < \hat{\gamma}_e \middle| \Phi_e, \Phi_b^a\right)\right\}\right\} \\
&\overset{(b)}{=} 1-\mathbb{E}_{\Phi_b^a}\left\{\exp\left(-\lambda_e \int_{R^2}\prod_{x_z\in\Phi_e}\mathbb{P}\left(\mathrm{SINR}_e\left(x_z\right) \geq \hat{\gamma}_e \middle| \Phi_e, \Phi_b^a\right) dx_z\right)\right\}.
\end{aligned}
\tag{5}
$$

Note that the rate redundancy is R_e and $\hat{\gamma}_e = 2^{R_e} - 1$. (a) follows from the independent of different channel gains. (b) follows from the probability generating functional (PGFL) of PPP [24]: $\left[\prod_{x\in\Phi} f\left(x\right)\right] = \exp\left(-\lambda \int_{R^2} \left(1-f\left(x\right)\right) dx\right)$. Φ_b^a represents the active base station set.

On the other hand, since eavesdroppers generally work in a passive way, it is difficult for legitimate transmitters to know their abilities to overhear the confidential message of the cellular link. Hence, according to the different abilities of eavesdroppers to decode the transmission message, we consider the secrecy performance of the cellular link and derive the respective expressions of the secrecy outage probability in two different scenarios in the following subsection. Firstly, we will discuss the performance of the cellular link in the case in which eavesdroppers have no multi-user decedability.

3.1.1 Scenario I

In what following, we firstly derive the close-form expression of the secrecy outage probability under the condition that eavesdroppers do not have the multi-user decedability. In other words, the information-bearing signal as well as the artificial noise from legitimate transmitters (including base stations and D2D transmitters) could confuse eavesdroppers. Based on the analysis above, the received SINR at the eavesdropper located at x_z could be expressed as:

$$
\mathrm{SINR}_e\left(x_z\right) = \frac{p_I\left|\mathbf{g}_{0e}^T\mathbf{w}_0\right|^2\|x_z\|^{-\alpha}}{\frac{p_A}{M-1}\left\|\mathbf{g}_{0e}^T\mathbf{W}_0\right\|^2\|x_z\|^{-\alpha} + I_{e\setminus\{0\}} + N_0}. \tag{6}
$$

where $\frac{p_A}{M-1}\left\|\mathbf{g}_{0e}^T\mathbf{W}_0\right\|^2$ represents the received interference induced by the injected artificial noise from the typical base station. $I_{e\setminus\{0\}} = \sum_{y_i\in\Phi_d} p_d|h_i|^2\left\|y_i - x_z\right\|^{-\alpha} + \sum_{x_i\in\Phi_b^a\setminus\{0\}}\left(p_I\left|\mathbf{g}_{ie}^T\mathbf{w}_i\right|^2 + \frac{p_A}{M-1}\left\|\mathbf{g}_{ie}^T\mathbf{W}_i\right\|^2\right)\|x_i - x_z\|^{-\alpha}$ represents the cumulative interference from legitimate transmitters (including both D2D transmitters located at y_i and base stations located at x_i, but except the typical base station located at the origin). For notational conciseness, we define $I_{e,c-e} = \sum_{x_i\in\Phi_b^a\setminus\{0\}}\left(p_I\left|\mathbf{g}_{ie}^T\mathbf{w}_i\right|^2 + \frac{p_A}{M-1}\left\|\mathbf{g}_{ie}^T\mathbf{W}_i\right\|^2\right)\|x_i - x_z\|^{-\alpha}$, which represents the cumulative interference from other base stations located at x_i (except the typical base station) induced by both the information-bearing signal and the artificial noise. $I_{e,d-e} = \sum_{y_i\in\Phi_d} p_d|h_i|^2\left\|y_i - x_z\right\|^{-\alpha}$ represents the cumulative interference from all the D2D transmitters. N_0 represents the covariance of the additive Gaussian noise at eavesdroppers. Based the analysis above, we can easily obtain $I_{e\setminus\{0\}} = I_{e,c-e} + I_{e,d-e}$.

Theorem 1 *Considering the case in which eavesdroppers have no multi-user decedability, the close-form expression of the secrecy outage probability of the cellular link can be given by:*

$$
P_{c,sop}^I = 1 - \exp\left(-\upsilon\int_0^\infty e^{-sN_0}\exp\left(-\mu\right) rdr\right), \tag{7}
$$

where $\rho = \frac{2}{\alpha}$ and $s = \frac{\hat{\gamma}_e r^\alpha}{p_I}$. For notational conciseness, we define $\upsilon = 2\pi\lambda_e\left(1+\hat{\gamma}_e\xi\right)^{1-M}$ and $\mu = \left(\pi\lambda_b p_a \omega p_I^\rho + \frac{\pi\lambda_d p_d^\rho}{\sin c\rho}\right)s^\rho$, where $\xi = \left(\phi^{-1}-1\right)/\left(M-1\right)$ and $\frac{1}{\sin c\rho} = \frac{\pi\rho}{\sin\pi\rho} = \Gamma\left(1+\rho\right)\Gamma\left(1-\rho\right)$. Note that ω is given by:

$$
\omega = \begin{cases} \kappa_{M+1}, & \text{if } \xi = 1, \\ \frac{\kappa_2}{(1-\xi)^{M-1}} - \sum_{m=0}^{M-2}\frac{\xi^{1+\rho}\kappa_{m+2}}{(1-\xi)^{M-m-1}}, & \text{otherwise.} \end{cases}
$$

Proof Please refer to Appendix 1. □

Remarks 1 *From* (7)*, it is easily observed that the close-form expression of the secrecy outage probability, $P_{c,sop}^I$, is negatively correlated with the base station density λ_b and the D2D transmitter density λ_d. In contrast, it is positively correlated with the eavesdropper density λ_e. This is due to the fact that the average received aggregate interference to confuse the most detrimental eavesdropper will be stronger with the increase of λ_b or λ_d. However, the average received SINR at the most detrimental eavesdropper will be higher as λ_e increases. Furthermore, the detailed reason why the secrecy outage probability decreases as λ_b increases is given by the following Corollary* 1.

In addition, from (7) we can easily know that λ_b only affects μ. Hence, we can obtain the following corollary.

Corollary 1 *The secrecy outage probability of the cellular link is monotonically non-increasing as λ_b increases and it is independent of λ_b when λ_b is large enough.*

This corollary implies that more base stations could improve the secrecy performance of the cellular link. This is because that the average received aggregate interference at each eavesdropper can be shown to scale with the base station density as $(\lambda_b p_a)^{\alpha/2}$. Since eavesdroppers follows HPPP on a two-dimensional plane, the received signal power at the most detrimental eavesdropper scales less than $(\lambda_b p_a)^{\alpha/2}$. Hence, the secrecy outage probability is negatively correlated with the base station density. However, from (4), we can know that $\lambda_b p_a$ will approach λ_u when the base station density is large enough. Therefore, in this case, the secrecy outage probability will be independent of λ_b.

Corollary 2 *In the interference-limited network, we can further derive the simple expression of the secrecy outage probability, i.e., $P_{c,sop}^{I,int}$, as follows:*

$$P_{c,sop}^{I,int}=1-\exp\left(-\frac{\lambda_e}{\lambda_b p_a \omega \hat{\gamma}_e^{\rho}+\frac{\lambda_d \hat{\gamma}_e^{\rho}}{\sin c\rho}\left(\frac{p_d}{p_I}\right)^{\rho}}\left(1+\hat{\gamma}_e\xi\right)^{1-M}\right). \tag{8}$$

Proof Following from Theorem 1 by letting $N_0 \to 0$. □

From (8), we can see that there are close relationships between the secrecy outage probability of the cellular link and some main system parameters, such as the number of antennas M, the power allocation ratio ϕ. To evaluate the effect of ϕ and M on the secrecy outage performance, next we will derive the asymptotic expression of $P_{c,sop}^{I}$ when the number of antennas at each base station approaches infinity. We firstly give the following lemma when the number of antennas approaches infinity[3].

Lemma 1 $\lim_{M\to\infty}\left\|\mathbf{g}_{0e}^T\mathbf{W}_0\right\|^2 = M-1$, $\lim_{M\to\infty}\left\|\mathbf{g}_{ie}^T\mathbf{W}_i\right\|^2 = M-1$.

Proof We can easily obtain Lemma 1 due to the fact that $\left\|\mathbf{g}_{0e}^T\mathbf{W}_0\right\|^2 \sim \text{Gamma}\,(M-1,1)$, $\left\|\mathbf{g}_{ie}^T\mathbf{W}_i\right\|^2 \sim \text{Gamma}\,(M-1,1)$. □

According to Lemma 1, when the number of antennas at each base station approaches infinity, the received asymptotic SINR at the eavesdropper located at x_z can be rewritten as:

$$\text{SINR}_e^{\infty}(x_z)=\frac{p_I\|x_z\|^{-\alpha}\left|\mathbf{g}_{0e}^T\mathbf{w}_0\right|^2}{p_A(M-1)\|x_z\|^{-\alpha}+I_{e\backslash\{0\}}^{\infty}+N_0}, \tag{9}$$

where $I_{e\backslash\{0\}}^{\infty}=\sum_{x_i\in\Phi_b^a\backslash\{0\}}\left(p_I\left|\mathbf{g}_{ie}^T\mathbf{w}_i\right|^2+p_A\right)\|x_i-x_z\|^{-\alpha}+\sum_{y_i\in\Phi_d}p_d|h_i|^2\left\|y_i-x_z\right\|^{-\alpha}$ denotes the cumulative interference from legitimate transmitters when the number of antennas at each base station approaches infinity. For notational conciseness, we define $I_{e,c-e}^{\infty}=\sum_{x_i\in\Phi_b^a\backslash\{0\}}\left(p_I\left\|\mathbf{g}_{ie}^T\mathbf{w}_i\right\|^2+p_A\right)\|x_i-x_z\|^{-\alpha}$, which similarly denotes the cumulative interference induced by both the information-bearing signal and the artificial noise from other base stations equipped with infinity antennas (except the typical base station). $I_{e,d-e}^{\infty}=\sum_{y_i\in\Phi_d}p_d|h_i|^2\left\|y_i-x_z\right\|^{-\alpha}$. Thus, we can obtain $I_{e\backslash\{0\}}^{\infty}=I_{e,c-e}^{\infty}+I_{e,d-e}^{\infty}$.

Then, we have the following proposition.

Proposition 1 *When the number of antennas at each base station approaches infinity, the asymptotic expression of the secrecy outage probability can be further given by:*

$$P_{c,sop}^{I,asy}=1-\exp\left(-\upsilon_1\int_0^{\infty}e^{-sN_0}\exp\left(-\mu_1\right)rdr\right), \tag{10}$$

where we define $\upsilon_1 = 2\pi\lambda_e e^{-\hat{\gamma}_e(M-1)\xi}$ and $\mu_1 = \left(\pi\lambda_b p_a\Gamma\left(1-\rho\right)\Psi p_I^{\rho}+\frac{\pi\lambda_d p_d^{\rho}}{\sin c\rho}\right)s^{\rho}$ for notational conciseness. Note that $\Psi=\Gamma\left(1+\rho,\left(\phi^{-1}-1\right)\right)e^{\left(\phi^{-1}-1\right)}$.

Proof Please refer to Appendix 2. □

Since $\xi=\left(\phi^{-1}-1\right)/(M-1)$, we can easily obtain that the asymptotic secrecy outage probability is independent of the number of antennas from Proposition 1.

By letting $N_0 \to 0$, it is straightforward to obtain the following corollary for the interference-limited case when the number of antennas at each base station approaches infinity.

Corollary 3 *In the interference-limited network, the asymptotic expression of the secrecy outage probability can be further derived as:*

$$P_{c,sop}^{I,asy,int}=1-\exp\left(-\frac{\upsilon_1}{2\left(\pi\lambda_b p_a\Gamma\left(1-\rho\right)\Psi\hat{\gamma}_e^{\rho}+\frac{\pi\lambda_d\hat{\gamma}_e^{\rho}}{\sin c\rho}\left(\frac{p_d}{p_I}\right)^{\rho}\right)}\right). \tag{11}$$

Proof Following from Proposition 1 by letting $N_0 \to 0$. □

When eavesdroppers have no multi-user decedability, even if each base station has no transmission power to generate the artificial noise, the inter-cell interference induced by the cellular link and the intra-cell interference induced by the D2D link could also confuse eavesdroppers. Hence, the base station is unnecessary to inject the artificial noise at some specified conditions. Based on the analysis above, we can obtain the following corollary employing the asymptotic expression of $P_{c,sop}^{I,asy,int}$ in the interference-limited network when the number of antennas at each base station approaches infinity.

Corollary 4 *It is unnecessary to generate the artificial noise to confuse eavesdroppers under the following condition*

$$\frac{\lambda_e}{\left(\lambda_b p_a + \lambda_d \Gamma(1+\rho)\left(\frac{p_d}{p}\right)^{\rho}\right)\Gamma(1-\rho)\hat{\gamma}_e^{\rho}} \leq -\ln(1-\varepsilon), \tag{12}$$

where ε represents the minimum secrecy requirement for the cellular link.

Proof Since $P_{c,sop}^{I,asy,int}$ is a monotonic increasing function with respect to the power allocation ratio ϕ. The secrecy performance of the cellular link would be satisfied as long as the secrecy outage probability is no more than ε, which is determined by the value of ϕ. By substituting $\phi = 1$ into the above constraint, we can obtain Eq. (12) given by Corollary 4. This provides very useful insight for practical system designs. □

3.1.2 Scenario II

In this subsection, we consider a case, in which it is assumed that eavesdroppers are in a non-colluding way and have powerful multi-user decedability. In other words, eavesdroppers could distinguish every data stream sent for different legitimate users from legitimate transmitters. Thus, they could subtract the interference induced by the information-bearing signal from the base station and the D2D transmitter by employing multiuser detection techniques, just as done in [25, 26]. From the above analysis, considering the typical cellular downlink, the received SINR at the eavesdropper located at x_z can be expressed as:

$$\mathrm{SINR}_e^{worse}(x_z) = \frac{p_I\left|\mathbf{g}_{0e}^T\mathbf{w}_0\right|^2\|x_z\|^{-\alpha}}{\frac{p_A}{M-1}\left\|\mathbf{g}_{0e}^T\mathbf{W}_0\right\|^2\|x_z\|^{-\alpha} + I_{A\setminus\{0\}} + N_0}, \tag{13}$$

where $\frac{p_A}{M-1}\left\|\mathbf{g}_{0e}^T\mathbf{W}_0\right\|^2\|x_z\|^{-\alpha}$ means the received interference induced by the injected artificial noise from the typical base station. $I_{A\setminus\{0\}} = \sum_{x_i\in\Phi_b^a\setminus\{0\}} \frac{p_A}{M-1}\left\|\mathbf{g}_{ie}^T\mathbf{W}_i\right\|^2 \|x_i - x_z\|^{-\alpha}$ denotes the cumulative interference from other base stations (except the typical base station) induced by the artificial noise. Then, we will give the expression of the secrecy outage probability of the cellular link in this case in Theorem 2.

Theorem 2 *The close-form expression of the secrecy outage probability of the typical cellular link in the case where eavesdroppers have powerful multi-user decedability can be given by:*

$$P_{c,sop}^{II} = 1 - \exp\left(-\upsilon_2 \int_0^{\infty} e^{-sN_0}\exp(-\mu_2)\, rdr\right). \tag{14}$$

Note that $\upsilon_2 = 2\pi\lambda_e\left(1+\hat{\gamma}_e\xi\right)^{1-M}$ and $\mu_2 = \lambda_b p_a C_{\rho,M}\Theta^{\rho}r^2$ are defined for notational conciseness, where $\Theta = \frac{\hat{\gamma}_e(1-\phi)}{(M-1)\phi}$ and $C_{\rho,M} = \pi\frac{\Gamma(M-1+\rho)\Gamma(1-\rho)}{\Gamma(M-1)}$.

Proof Please refer to Appendix 3. □

Theorem 2 implies that the secrecy outage probability is negatively correlated with the base station density λ_b. In contrast, it is positively correlated with the eavesdroppers density λ_e. This stated remark agrees well with the remark from Theorem 1. Nevertheless, it is independent of the D2D transmitters density λ_d. This is because that eavesdroppers have the multi-user decedebility to remove the interference induced by the D2D link and thus result in no impact on the eavesdropping link.

In addition, we can easily obtain that $p_{c,sop}^{II}$ increases as ϕ increases, which denotes the power allocation ratio of the total transmission power allocated to the information transmission power. This is because that only the artificial noise will confuse eavesdroppers in this worst case. While a higher ϕ represents a lower transmission power allocated to generate the artificial noise to confuse eavesdroppers at the base station. Therefore, this will result in a much higher secrecy outage probability with a higher ϕ.

Corollary 5 *In the interference-limited network, the secrecy outage probability of the typical cellular link when eavesdroppers have the multi-user decedability can be further derived as:*

$$P_{c,sop}^{II,int} = 1 - \exp\left(-\frac{\pi\lambda_e}{\lambda_b C_{\rho,M}\Theta^{\rho}}\left(1+\hat{\gamma}_e\xi\right)^{1-M}\right). \tag{15}$$

Proof By letting $N_0 \to 0$, we simplify the integral in (14) and yield the result in (15). □

To evaluate the effect of ϕ and M on the secrecy performance, similar to Proposition 1, next we will derive the asymptotic expression of the secrecy outage probability when eavesdroppers have the multi-user decedability and each base station has infinity antennas.

Proposition 2 *When the number of antennas at each base station approaches infinity, the asymptotic expression of the secrecy outage probability can be further given by:*

$$P_{c,sop}^{II,asy} = 1 - \exp\left(-\upsilon_2 \int_0^{\infty} e^{-sN_0} \exp\left(-\mu_3\right) rdr\right), \tag{16}$$

where $\upsilon_2 = 2\pi\lambda_e e^{-\hat{\gamma}_e(M-1)\xi}$ *and* $\mu_3 = \pi\lambda_b p_a \Gamma\left(1-\rho\right)(\phi ps)^{\rho}\left(\phi^{-1}-1\right)^{\rho}$ *are defined for notational conciseness.*

Proof When each base station has infinity antennas, from Lemma 1, the received SINR can be equivalently rewritten as:

$$\mathrm{SINR}_e^{\infty,w}(x_z) = \frac{p_I\left|\mathbf{g}_{0e}^T\mathbf{w}_0\right|^2\|x_z\|^{-\alpha}}{p_A\|x_z\|^{-\alpha} + I_{A\setminus\{0\}}^{\infty} + N_0}, \tag{17}$$

where $p_A\|x_z\|^{-\alpha}$ represents the received interference induced by the injected artificial noise from the typical base station equipped with infinity antennas. $I_{A\setminus\{0\}}^{\infty} = \sum_{x_i\in\Phi_b^a\setminus\{0\}} p_A\|x_i - x_z\|^{-\alpha}$ represents the cumulative interference from other base stations with infinity antennas (except the typical base station) induced by the artificial noise. □

Denote $\hat{\gamma}_{0,e}^{\infty} = \phi p\left(\left\|\mathbf{g}_{0e}^T\mathbf{w}_0\right\|^2 - \hat{\gamma}_e\xi\left(M-1\right)\right)$. According to the definition of the secrecy outage probability, we can obtain

$$\begin{aligned}
&\mathbb{P}\left(\mathrm{SINR}_e^{\infty,w}(x_z) \le \hat{\gamma}_e\right)\\
&= \mathbb{P}\left(\hat{\gamma}_{0,e}^{\infty} \le \hat{\gamma}_e\|x_z\|^{\alpha}\left(I_{A\setminus\{0\}}^{\infty} + N_0\right)\right)\\
&= 1 - e^{-\hat{\gamma}_e(M-1)\xi} e^{-sN_0}\mathcal{L}_{I_{A\setminus\{0\}}^{\infty}}(s).
\end{aligned} \tag{18}$$

When each base station has infinity antennas, employing ([27], Eq. (68)), we obtain:

$$\mathcal{L}_{I_{A\setminus\{0\}}^{\infty}}(s) = \exp\left(-\pi\lambda_b p_a\Gamma\left(1-\rho\right)(\phi ps)^{\rho}\left(\phi^{-1}-1\right)^{\rho}\right). \tag{19}$$

Then, substituting (19), (18) into (5) and changing to a polar coordinate system to evaluate the integral, we can obtain the result in (16).

We can also easily observe that the asymptotic expression of the secrecy outage probability of the cellular link is independent of the number of antennas, M, which agrees with the conclusion drawn from Proposition 1.

Then, it is straightforward to obtain the following corollary by letting $N_0 \to 0$.

Corollary 6 *In the interference-limited network, when eavesdroppers have the multi-user decedability and each base station has infinity antennas, the asymptotic secrecy outage probability can be further given by:*

$$P_{c,sop}^{II,asy,int} = 1 - \exp\left(-\frac{\pi\lambda_e}{\eta}e^{-\hat{\gamma}_e(M-1)\xi}\right). \tag{20}$$

Note that we define $\eta = \pi\lambda_b p_a\Gamma\left(1-\rho\right)\left(\phi^{-1}-1\right)^{\rho}\hat{\gamma}_e^{\rho}$ for notational conciseness.

3.2 Connection outage probability of D2D links

Considering the typical D2D link whose receiver is located at the origin, we conduct the expression of the connection outage probability and analyze some properties in this subsection. It is assumed that the typical D2D transmitter is located l away from the typical D2D receiver. Since the injected artificial noise at each base station is just in the null space of the wireless channel of the desired cellular user, it will degrade the reliable communication of the typical D2D link. Based on the analysis above, the received SINR at the typical D2D receiver is recast as:

$$\mathrm{SINR}_d = \frac{p_d h_{0d} l^{-\alpha}}{I_d + N_0}, \tag{21}$$

where p_d is the transmission power of all D2D transmitters. $I_d = \sum_{x_i\in\Phi_b^a} p_I\|x_i\|^{-\alpha}\left|\mathbf{g}_{id}^T\mathbf{w}_i\right|^2 + \sum_{x_i\in\Phi_b^a}\frac{p_A}{M-1}\|x_i\|^{-\alpha}\left\|\mathbf{g}_{id}^T\mathbf{W}_i\right\|^2 + \sum_{y_i\in\Phi_d\setminus\{y_0\}} p_d h_{id}\left\|y_i\right\|^{-\alpha}$ represents the totally cumulative interference from the base station that is located at x_i and other D2D transmitters (except the typical D2D transmitter located at y_0). $I_{c-d} = \sum_{x_i\in\Phi_b^a}\left(p_I\left|\mathbf{g}_i^T\mathbf{w}_i\right|^2 + \frac{p_A}{M-1}\left\|\mathbf{g}_i^T\mathbf{W}_i\right\|^2\right)\|x_i\|^{-\alpha}$ represents the interference induced by the information-bearing signal and the artificial noise from all the base station. $I_{d-d} = \sum_{y_i\in\Phi_d\setminus\{y_0\}} p_d h_{id}\left\|y_i\right\|^{-\alpha}$ represents the interference from other D2D links sharing the same resource except the typical D2D transmitter. h_{id} represents the small-scale fading channel from the D2D transmitter located at y_i, especially, h_{0d} means the small-scale fading channel from the typical D2D transmitter. Similarly, $\mathbf{g}_{id}$ represents the small-scale fading channel from the base station located at x_i to the typical D2D receiver. It is assumed that h_{id} follows the exponential distribution with unit mean, i.e., $h_{id} \sim \exp(1)$. N_0 represents the covariance of the additive Gaussian noise at the typical D2D receiver. Hence, we can have $I_d = I_{c-d} + I_{d-d}$.

Given the target transmission rate R_d, the connection outage probability of the typical D2D receiver can be expressed as:

$$\begin{aligned} p_{d,cop} &= \mathbb{P}\left\{\mathrm{SINR}_d < \hat{\gamma}_d\right\} \\ &= 1 - e^{-N_0\zeta}\,\mathbb{E}_{\Phi_b^a,\Phi_d}\left(e^{-I_d\zeta}\right) \\ &= 1 - e^{-N_0\zeta}\,\mathcal{L}_{I_d}(\zeta), \end{aligned} \tag{22}$$

where $\hat{\gamma}_d = 2^{R_d} - 1$ represents the SINR target threshold to satisfy the communication requirement of the typical D2D link and $\zeta = \frac{\hat{\gamma}_d l^\alpha}{p_d}$. $\mathcal{L}_{I_d}(\zeta)$ denotes the Laplace transform of I_d, i.e., $\mathcal{L}_{I_d}(\zeta) = \mathbb{E}(-\zeta I_d)$. According to the property of the Laplace transform, we can easily have $\mathcal{L}_{I_d}(\zeta) = \mathcal{L}_{I_{c-d}}(\zeta) \bullet \mathcal{L}_{I_{d-d}}(\zeta)$ because of $I_d = I_{c-d} + I_{d-d}$.

Theorem 3 *The close-form expression of the connection outage probability of the typical D2D link in artificial noise assisted D2D-enabled cellular network is given by:*

$$p_{d,cop} = 1 - e^{-N_0\zeta}\exp\left(-\left(\pi\lambda_b p_a k + \frac{\pi\lambda_d p_d^\rho}{\sin c\rho}\right)\zeta^\rho\right). \tag{23}$$

Note that $k = \begin{cases} 2p_I^\rho\kappa_{M+1}, & \text{if } \xi = 1, \\ 2p_I^\rho\left(\frac{\kappa_2}{(1-\xi)^{M-1}} - \sum_{m=0}^{M-2}\frac{\xi^{1+\rho}\kappa_{m+2}}{(1-\xi)^{M-m-1}}\right), & \text{otherwise.} \end{cases}$

Proof Please refer to Appendix 4. □

Remarks 2 *From the derived result in* (23)*, it is obvious that the connection outage probability, $p_{d,cop}$, has close relationships with various system parameters, such as the densities λ_b, λ_e, the total transmission power p of each base station, the D2D transmission power p_d and so on. Especially, for the given λ_b, λ_e and ϕ, $p_{d,cop}$ is positively correlated with the transmission power ratio p/p_d. This is because that a larger transmission power of each base station will introduce stronger interference to the typical D2D link from the cellular downlink, resulting in a larger connection outage probability of the typical D2D link.*

Remarks 3 *The expression of the connection outage probability in* (23) *is derived just under the assumption that the distance l between the typical D2D transmitter and its corresponding D2D receiver is constant. The derived result can be easily expanded to the scenario where l is a random variable. The expression of the connection outage probability of the typical D2D link in the expanded scenario can be obtained by calculating the integral formula $\int_0^\infty \mathbb{P}(SINR_d < \beta_d | l) f_l(l)\, dl$, where $f_l(l)$ denotes the PDF of the distance l.*

By letting $N_0 = 0$, we will get the expression of the connection outage probability shown in the following corollary for the interference-limited network.

Corollary 7 *Considering the interference-limited in this hybrid network, the close-form expression of the connection outage probability of the typical D2D link is given by:*

$$p_{d,cop}^{int} = 1 - \exp\left(-\left(\pi\lambda_b p_a k + \frac{\pi\lambda_d p_d^\rho}{\sin c\rho}\right)\zeta^\rho\right), \tag{24}$$

where k is given in (23)*.*

Proof Corollary 7 can be straightforwardly obtained from Theorem 3 with $N_0 \to 0$. □

Similarly, next we will provide the asymptotic expression of the connection outage probability of the typical D2D link when each base station has infinity antennas.

Proposition 3 *When the number of antennas at each base station approaches infinity, we can obtain the asymptotic expression of the connection outage probability of the typical D2D link by:*

$$P_{d,cop}^{asy} = 1 - e^{-\zeta N_0}\exp\left(-\left(\pi\lambda_b p_a \Gamma(1-\rho)\,\Psi p_I^\rho + \frac{\pi\lambda_d p_d^\rho}{\sin c\rho}\right)\zeta^\rho\right). \tag{25}$$

Proof According to Lemma 1, when the number of antennas at each base station approaches infinity, the received asymptotic SINR at the typical D2D receiver can be expressed as:

$$\mathrm{SINR}_d^\infty = \frac{p_d h_0 l^{-\alpha}}{I_d + N_0}, \tag{26}$$

where $I_d^\infty = \sum_{x_i\in\Phi_b^a}\left(p_I\left|\mathbf{g}_{id}^T\mathbf{w}_i\right|^2 + p_A\right)\|x_i\|^{-\alpha} + \sum_{y_i\in\Phi_d\setminus\{y_0\}} p_d h_{id}\|y_i\|^{-\alpha}$ represents the totally cumulative interference when each base station has infinity number of antennas. $I_{d,c-d}^\infty = \sum_{x_i\in\Phi_b^a}\left(p_I\left|\mathbf{g}_{id}^T\mathbf{w}_i\right|^2 + p_A\right)\|x_i\|^{-\alpha}$ represents the cumulative interference from all the base stations, $I_3 = \sum_{y_i\in\Phi_d\setminus\{y_0\}} p_d h_{id}\|y_i\|^{-\alpha}$ represents the cumulative interference from other D2D transmitters. Hence, it is intuitive that $I_d^\infty = I_{d,c-d}^\infty + I_3$. □

Denote $I_{d,c-d\setminus\{0\}}^\infty = \sum_{x_i\in\Phi_b^a\setminus\{0\}}\left(p_I\left\|\mathbf{g}_{id}^T\mathbf{w}_i\right\|^2 + p_A\right)\|x_i\|^{-\alpha}$. Owing to Slivnyak-Mecke Theorem [24], we can have $\mathcal{L}_{I_{d,c-d\setminus\{0\}}^\infty}(s) = \mathcal{L}_{I_{d,c-d}^\infty}(s)$. Employing ([27], Eq. (68)), we can obtain:

$$\mathcal{L}_{I_{d,c-d}^\infty}(s) = \exp\left(-\pi\lambda_b p_a \Gamma(1-\rho)(\phi p\zeta)^\rho\Psi\right), \tag{27}$$

where Ψ is given by (10).

Substituting (27), (41) into (22) could yield the result in (25). Then, we can easily get the following corollary from Proposition 3.

Corollary 8 *In the interference-limited network, when the number of antennas at each base station approaches infinity, the asymptotic expression of the connection outage probability of the typical D2D link can be given by:*

$$P_{d,cop}^{inf,int} = 1 - \exp\left(-\left(\pi\lambda_b p_a \Gamma(1-\rho)\Psi p_I^{\rho} + \frac{\pi\lambda_d p_d^{\rho}}{\sin c\rho}\right)\zeta^{\rho}\right). \tag{28}$$

Proof Following from Proposition 3 by letting $N_0 \to 0$. □

4 Numerical results and analysis

In this suction, more detailed simulation and numerical results are provided to evaluate the theoretical analysis. The path loss exponent is $\alpha = 3$ and $\mu = 3.5$ for the nearest base station association. The total transmission power of each base station is 60 dBm and the transmission power of all the D2D transmitters is 20 dBm. The density of the cellular user is $0.0005/m^2$, i.e., $\lambda_c = 0.0005/m^2$. The number of antennas equipped at each base station is set to be $M = 10$. For simplicity, it is assumed that the distance between D2D pairs is $l = 1m$.

The results of the secrecy outage probability in scenario I and in scenario II versus the density of the base station, λ_b, are respectively plotted in Figs. 2 and 3 with different system parameters. We can observe that it will improve the secrecy performance of the cellular link with the density of the base station increasing. This is because more base stations will bring more interference to confuse eavesdroppers to overhear confidential messages of the cellular link. From Figs. 2 and 3, we can observe that theoretical results are quite close to asymptotic results. In addition, we can see that the secrecy outage probability in scenario I is lower than the one in scenario II because the information-bearing signal except for the artificial noise in scenario I also can confuse eavesdroppers, resulting in lower secrecy outage probability.

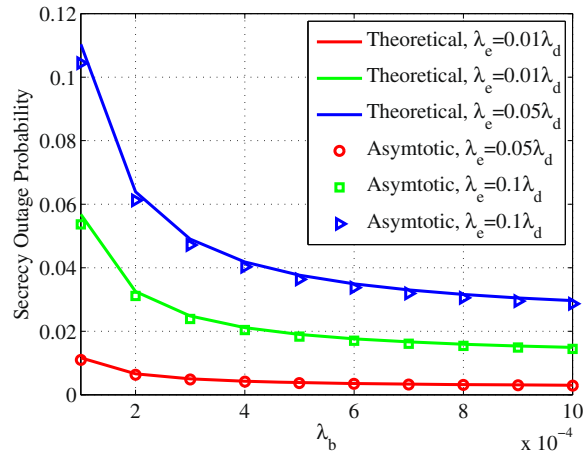

Fig. 2 The secrecy outage probability of the typical cellular link versus the density of the base station λ_b under different densities of the eavesdropper λ_e in scenario I where $\lambda_d = 0.001/m^2, \phi = 0.6$. Figure 2 illustrates the close-form expression and asymptotic expression of the secrecy outage probability of the typical cellular link in scenario I

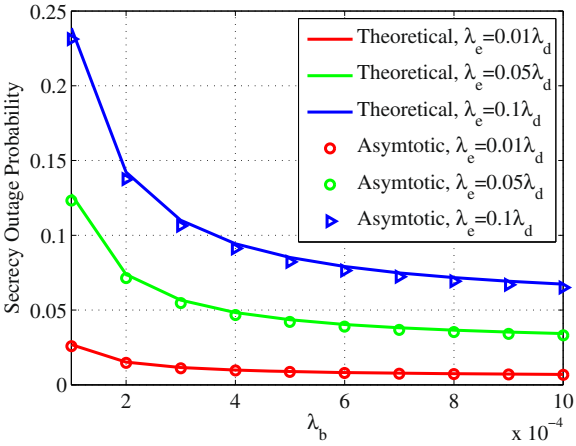

Fig. 3 The secrecy outage probability of the typical cellular link versus the density of the base station λ_b under different densities of the eavesdropper λ_e in scenario II where $\lambda_d = 0.001/m^2, \phi = 0.6$. Figure 3 shows the close-form expression and asymptotic expression of the secrecy outage probability of the typical cellular link in scenario II

Additional, the results of the secrecy outage probability of the typical cellular link in both scenario I and scenario II versus the density of the cellular user, λ_c, are illustrated in Fig. 4 with different system parameters. It is obvious that it will improve the secrecy performance of the cellular link with the density of the cellular user increasing, as shown in Fig. 4. This is because that more base stations will be more possible to be active to serve for the nearest cellular user as the number of the cellular user increases, which can be also easily obtained from Eq. (4). Hence, it will bring more interference to confuse eavesdroppers to overhear confidential messages of the cellular link, thus improving the secrecy performance of the cellular link. More particularly, although eavesdroppers have the multi-user decidability in scenario II and the interference brought by information-bearing signals has no impact on eavesdroppers, more active base stations will generate the artificial noise to degrade channel capacity over the eavesdropping link, resulting in much lower secrecy outage probability.

On the other hand, the results of the secrecy outage probability of the typical cellular link in scenario I versus the density of the D2D user , λ_d, are depicted in Fig. 5 with different system parameters. Since eavesdroppers have the multi-user decidability in scenario II, the number of D2D

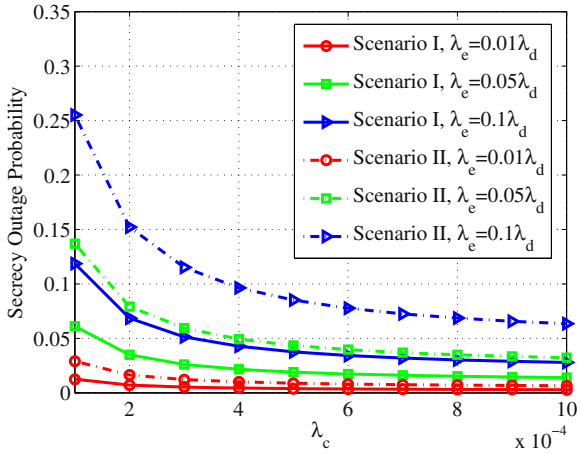

Fig. 4 The secrecy outage probability of the typical cellular link in both scenario I and scenario II versus the density of the cellular user λ_c under different densities of the eavesdropper λ_e where $\lambda_b = 0.0005/m^2$. Figure 4 shows the relationship between the secrecy outage probability of the typical cellular link in both scenario I and scenario II and the density of the cellular user

users has no impact on the secrecy outage probability of the cellular link in scenario II. Hence, in Fig. 5, we just investigate the impact of the number of D2D users on the cellular performance in scenario I. We can can observe that it will improve the secrecy performance of the cellular link with the density of the D2D user increasing, as illustrated in Fig. 5. This is because more D2D users will bring more inter-cell interference to confuse eavesdroppers to overhear confidential messages of the cellular link, resulting in much lower secrecy outage probability.

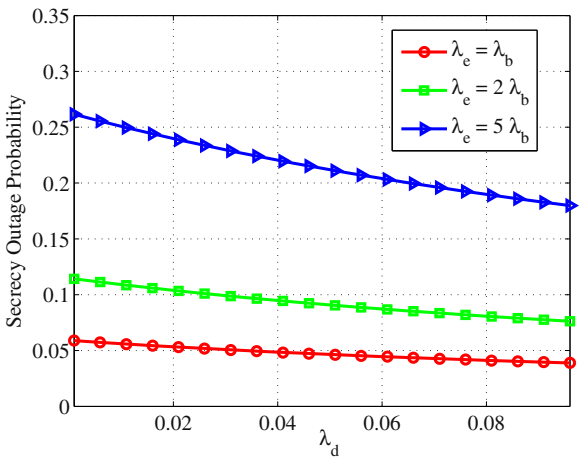

Fig. 5 The secrecy outage probability of the typical cellular link in scenario I versus the density of the D2D user λ_d under different densities of the eavesdropper λ_e where $\lambda_b = 0.0001/m^2$. Figure 5 illustrates the relationship between the secrecy outage probability of the typical cellular link in scenario I and the density of the D2D user

The secrecy outage probability of the cellular link in scenario I versus the power allocation ratio ϕ is demonstrated in Fig. 6. From Fig. 6, we can observe that the secrecy outage probability increases with ϕ increasing. This is because that the signal power received at eavesdroppers is proportional to ϕ, while the average received aggregate interference is independent of ϕ. In addition, Fig. 7 reveals the power allocation ratio of the information-bearing signal to the total transmission power versus the density of the base station λ_b. From Fig. 7, deploying more base stations and increasing λ_c represent that more base stations will be active to serve for cellular users and meanwhile generate the artificial noise to confuse eavesdroppers, which will cause the secrecy outage probability to decrease. Hence, the secrecy requirement of the cellular link will be satisfied even if each base station allocates lower transmission power to generate the artificial noise, thus resulting in a larger ϕ.

Figure 8 shows the results of the connection outage probability versus the density of the base station, λ_b, under some system parameters. From Fig. 8, we can observe that deploying more base station will degrade the connection performance of the cellular link. Since both the information-bearing signal and the artificial noise of each base station can bring the interference to the typical D2D link, more base station will bring more interference to degrade the reliable communication of the typical D2D link. From Fig. 8, we can also see that the theoretical results are quite close to the asymptotic results.

We also investigate the impact of the power allocation ratio, ϕ, on the connection outage probability of the typical D2D link in Fig. 9. As expected, the connection outage probability of the typical D2D link will increase with a

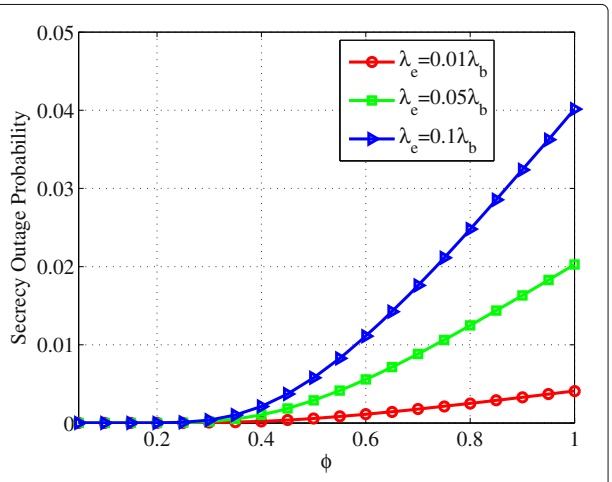

Fig. 6 The secrecy outage probability of the typical cellular link in scenario I versus power allocation ratio ϕ. Figure 6 depicts the relationship between the secrecy outage probability of the typical cellular link and the power allocation ratio

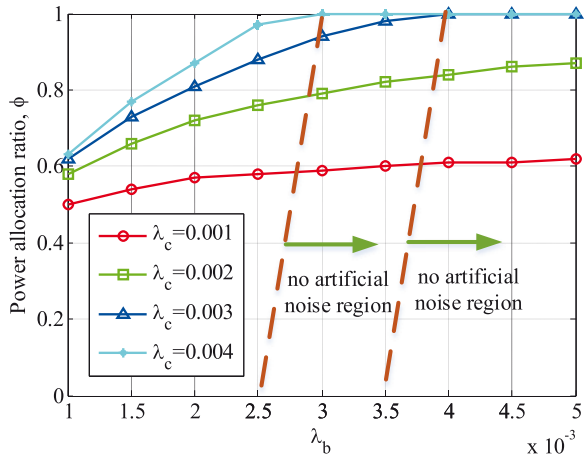

Fig. 7 The power allocation ratio in scenario I versus the density of the base station λ_b where $\lambda_e = 0.0003/m^2$, $R_e = 0.5$ *bps/Hz*, $\varepsilon = 0.1$. Figure 7 illustrates the transmission power allocated to the information-bearing signal under the density of the base station , and shows that it is unnecessary to generate the artificial noise under specific condition

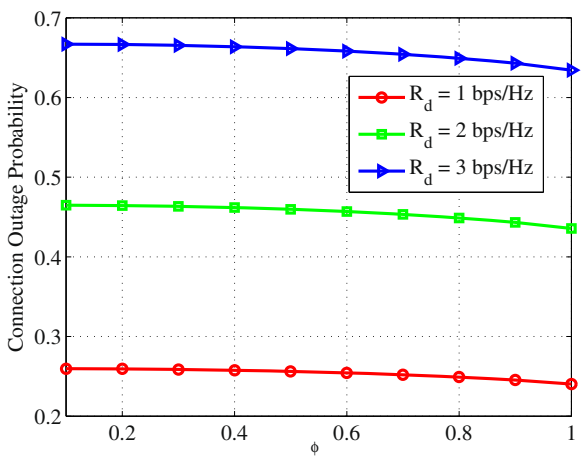

Fig. 9 The connection outage probability of the typical D2D link versus power allocation ratio ϕ. Figure 9 depicts the relationship between the connection outage probability of the typical D2D link and the power allocation ratio

larger R_d from Fig. 9. In Fig. 9, we can also observe that the connection outage probability will be smaller with a larger ϕ, which implies that the information-bearing signal has less impact on the reliable communication of the typical D2D link compared with the artificial noise. However, the difference of the connection outage probability under different power allocation ratios is very little because both the information-bearing signal and the artificial noise will degrade the reliable communication of the typical D2D link. That is to say, the average aggregate interference at the typical D2D transmitter keeps approximately same under different power allocation ratios when the transmission power of the base station is constant.

Furthermore, we exploit the impact of the total transmission power p of each base station on the connection outage probability of the typical D2D link, as demonstrated in Fig. 10. As expected, the connection outage probability of the typical D2D link will be larger as p increases. This is because that it will bring stronger interference to the typical D2D link with a larger p, resulting in a larger connection outage probability.

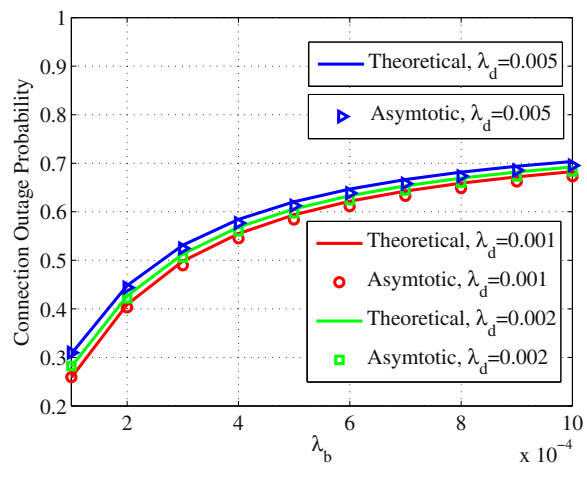

Fig. 8 The connection outage probability of the typical D2D link versus the density of the base station λ_b where $\phi = 0.3$, $R_d = 1$ *bps/Hz*. Figure 8 represents the close-form expression and asymptotic expression of connection outage probability of the typical D2D link

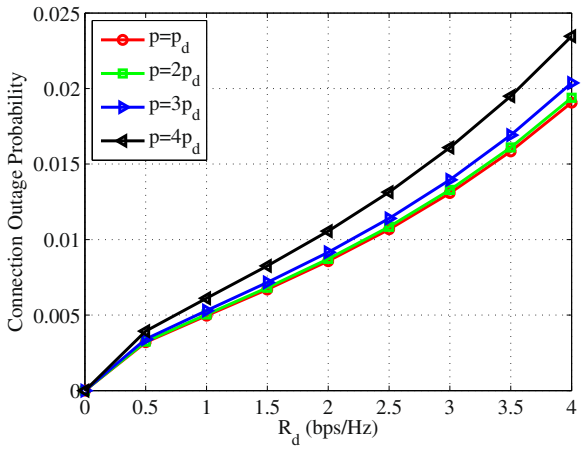

Fig. 10 The connection outage probability of the typical D2D link versus R_d under different total transmission power p where $p_d = 10$ *dBm*. Figure 10. describes comparison results of the connection outage probability of the typical D2D link under different total transmission power of each base station

5 Conclusion

In this paper, secure communication for the cellular downlink is investigated in this hybrid network. A case was considered, in which each base station has no CSI from D2D users because they are generally deployed in the cell edge. To guarantee secure communication of the cellular link, each base station employed the artificial noise assisted transmission strategy. Firstly, we considered two different scenarios depending on whether eavesdroppers have the multi-user decedability or not and derived the close-form expression of the secrecy outage probability of the cellular link. To characterize the reliable communication of the D2D link, its close-form expression of connection outage probability was derived and some comprehensive analysis were provided to guide the system design. Finally, simulation results are provided to validate the effective of the theoretical results. Furthermore, more complex D2D scenes need to be studied.

Endnotes

[1] The performance metrics to characterize the secrecy performance from different perspectives in existing works can be classified into two types: the secrecy outage probability and the achievable secrecy rate. The ergodic achievable secrecy rate is not suitable for the system having strictly real-time requirements. However, in the 5G mobile communication, it has higher real-time requirements. Hence, we focus on the secrecy outage probability to depict the secrecy performance of the cellular link in this paper.

[2] In this paper, we adopt the TDMA scheme to derive the results and discuss the performance of this hybrid network, but the derived results can be easily expanded to other systems, such as the frequency-division multiple access (FDMA) scheme and so on.

[3] For the null-space based beamforming, the matrix inversion in massive MIMO systems will incur very high computation cost. However, alternatively, we may use the random artificial noise scheme which has been adopted in [30]. From the derived results and numerical results [30], we can come to a conclusion that main system parameters have the same effect on the secrecy performance for different design schemes. The conclusions drawn from the derived result in this paper could also guide the system design when the artificial noise is in random form.

Appendix 1: Proof of Theorem 1

Let us define $\gamma_{0,e} = p_I \left(\left| \mathbf{g}_{0e}^T \mathbf{w}_0 \right|^2 - \xi \hat{\gamma}_e \left\| \mathbf{g}_{0e}^T \mathbf{W}_0 \right\|^2 \right)$.

Because $\left| \mathbf{g}_{0e}^T \mathbf{w}_0 \right|^2 \sim \exp(1)$, $\left\| \mathbf{g}_{0e}^T \mathbf{W}_0 \right\|^2 \sim \text{Gamma}(N-1, 1)$, we can obtain its cumulative distribution function (CDF) $F_{\gamma_{0,e}}(x)$ as follows:

$$F_{\gamma_{0,e}}(x) = 1 - \left(1 + \hat{\gamma}_e \xi\right)^{1-M} e^{-\frac{x}{p_I}}. \tag{29}$$

According to the definition of the secrecy outage probability, then, we can easily obtain:

$$\begin{aligned} &\mathbb{P}\left(\text{SINR}_e(x_z) \le \hat{\gamma}_e\right) \\ &= \mathbb{P}\left(\hat{\gamma}_{0,e} \le \hat{\gamma}_e \|x_z\|^\alpha \left(I_{e\setminus\{0\}} + N_0\right)\right) \\ &= 1 - \left(1 + \hat{\gamma}_e \xi\right)^{1-M} e^{-sN_0} \mathcal{L}_{I_{e\setminus\{0\}}}(s), \end{aligned} \tag{30}$$

where $\mathcal{L}_{I_{e\setminus\{0\}}}(s)$ denotes the Laplace transform of $I_{e\setminus\{0\}}$, i.e., $\mathcal{L}_{I_{e\setminus\{0\}}}(s) = \mathbb{E}\left(-sI_{e\setminus\{0\}}\right)$. Since $I_{e\setminus 0} = I_{e,c-e} + I_{e,d-e}$, then it is straightforward to obtain according to the property of PPP [24]:

$$\mathcal{L}_{I_{e\setminus 0}}(s) = \mathcal{L}_{I_{e,c-e}}(s) \bullet \mathcal{L}_{I_{e,d-e}}(s). \tag{31}$$

Owing to the property of PPP [24] that the coordinates translations will not change the distribution of PPP, we shift the coordinates so that the eavesdropper at x_z is located at the origin. Then, employing ([27], Eq. (64)) we can obtain:

$$\mathcal{L}_{I_{e,c-e}}(s) = \exp\left(-\pi \lambda_b p_a \omega (p_I s)^\rho\right), \tag{32}$$

where ω is given by (7).

Because $I_{e,d-e} = \sum_{y_i \in \Phi_d} p_d h_{id} \left\| y_i \right\|^{-\alpha}$ and employing ([13], Eq. (7)) we can directly obtain:

$$\mathcal{L}_{I_{e,d-e}}(s) = \exp\left(-\frac{\pi \lambda_d p_d^\rho s^\rho}{\sin c\rho}\right). \tag{33}$$

where $\frac{1}{\sin c\rho} = \frac{\pi\rho}{\sin \pi\rho} = \Gamma(1+\rho)\Gamma(1-\rho)$.

By plugging (33), (32), (31) into (30), we can have:

$$\begin{aligned} \mathbb{P}\left(\text{SINR}_e(x_z) \le \hat{\gamma}_e\right) = 1 - \left(1 + \hat{\gamma}_e \xi\right)^{1-M} e^{-sN_0} \\ \exp\left(-\left(\pi \lambda_b p_a \omega p_I^\rho + \frac{\pi \lambda_d p_d^\rho}{\sin c\rho}\right) s^\rho\right). \end{aligned} \tag{34}$$

Substituting (34) into (5) and changing to a polar coordinate system to evaluate the integral yields the result in (7).

Appendix 2: Proof of *Proposition 1*

Since $I_{e,c-e}^\infty = \sum_{x_i \in \Phi_b^a \setminus\{0\}} \left(p_I \left\| \mathbf{g}_{ie}^T \mathbf{w}_i \right\|^2 + p_A\right) \|x_i - x_z\|^{-\alpha}$, we first shift the coordinates so that the eavesdropper at x_z is located at the origin. Then, by employing ([27], Eq. (68)) it is direct to yield:

$$\mathcal{L}_{I_{e,c-e}}^\infty(s) = \exp\left(-\pi \lambda_b p_a \Gamma(1-\rho)(\phi p s)^\rho \Psi\right), \tag{35}$$

where Ψ is given by (10).

Since $I^{\infty}_{e\backslash 0} = I^{\infty}_{e,c-e} + I^{\infty}_{e,d-e}$, we can have $\mathcal{L}^{\infty}_{I_{e\backslash 0}}(s) = \mathcal{L}^{\infty}_{I_{e,c-e}}(s) \bullet \mathcal{L}^{\infty}_{I_{e,d-e}}(s)$. When the number of antennas at each base station approaches infinity, the cumulative interference from D2D transmitters at the most detrimental eavesdropper is same with. Hence, its Laplace transform can be obtained from (33). Then it is straightforward to obtain:

$$\mathcal{L}^{\infty}_{I_{e\backslash 0}}(s) = \exp\left(-\left(\pi\lambda_b p_a \Gamma(1-\rho)\Psi p_I^{\rho} + \frac{\pi\lambda_d p_d^{\rho}}{\sin c\rho}\right)s^{\rho}\right). \tag{36}$$

Substituting (36) into (5) and changing to a polar coordinate system to evaluate the integral yields the results in (10).

Appendix 3: Proof of Theorem 2

According to the definition of the secrecy outage probability and similar to (18), we can have:

$$\begin{aligned}&\mathbb{P}\left(\mathrm{SINR}_e^{worse}(x_z) \le \hat{\gamma}_e\right)\\ &= \mathbb{P}\left(\hat{\gamma}_{0,e} \le \hat{\gamma}_e \|x_z\|^{-\alpha}\left(I_{A\backslash\{0\}} + N_0\right)\right)\\ &= 1 - \left(1+\hat{\gamma}_e\xi\right)^{1-M} e^{-sN_0}\mathcal{L}_{I_{A\backslash\{0\}}}(s),\end{aligned} \tag{37}$$

where $\mathcal{L}_{I_{A\backslash\{0\}}}(s)$ denotes the Laplace transform of $I_{A\backslash\{0\}}$, i.e., $\mathcal{L}_{I_{A\backslash\{0\}}}(s) = \mathbb{E}\left(-sI_{A\backslash\{0\}}\right)$.

In this case, only the artificial noise has the impact on the secrecy performance of the typical cellular link. Due to the property of PPP [24] that the coordinates translations will not change the distribution of PPP, we shift the coordinates so that the eavesdropper at x_z is located at the origin. Because $\left\|\mathbf{g}_{ie}^T\mathbf{W}_i\right\|^2 \sim$ Gamma $(M-1,1)$ and using ([25], Eq. (56)) we can obtain:

$$\begin{aligned}\mathcal{L}_{I_{A\backslash\{0\}}}(s) &= \exp\left(-\lambda_b p_a C_{\rho,M}\left(\frac{p_A}{M-1}\right)^{\rho} s^{\rho}\right)\\ &= \exp\left(-\lambda_b p_a C_{\rho,M}\left(\frac{\hat{\gamma}_e(1-\phi)}{(M-1)\phi}\right)^{\rho} r^2\right).\end{aligned} \tag{38}$$

Then, substituting (38), (37) into (5) and changing to a polar coordinate system to evaluate the integral, we can get the result in (14).

Appendix 4: Proof of Theorem 3

We define the received interference power at the typical D2D receiver from each base station as $X_i = p_I\left(\left|\mathbf{g}_i^T\mathbf{w}_i\right|^2 + \xi\left\|\mathbf{g}_i^T\mathbf{W}_i\right\|^2\right)$, since $\mathbf{g}_i$, $\mathbf{w}_i$ and $\mathbf{W}_i$ are independent of each other, $\left|\mathbf{g}_i^T\mathbf{w}_i\right|^2 \sim \exp(1)$, $\left\|\mathbf{g}_i^T\mathbf{W}_i\right\|^2 \sim$ Gamma $(M-1,1)$. Using ([25], Lemma 1), then we can derive the probability density function (pdf) of X_i as:

$$f_{X_i}(x) = \begin{cases}\frac{x^{M-1}}{(M-1)!p_I^M}e^{-\frac{x}{p_I}}, & if\ \xi = 1,\\ \frac{(1-\xi)^{1-M}}{(M-2)!p_I}e^{-\frac{x}{p_I}}\gamma\left(M-1, \frac{(1-\xi)x}{\xi p_I}\right), & otherwise.\end{cases} \tag{39}$$

The Laplace transform of I_{c-d} can be expressed as:

$$\begin{aligned}\mathcal{L}_{I_{c-d}}(\zeta) &= \mathbb{E}_{I_{c-d}}\left\{\exp\left(-\zeta\sum_{x_i\in\Phi_b^a} X_i\|x_i\|^{-\alpha}\right)\right\}\\ &= \mathbb{E}_{\Phi_b^a}\left\{\prod_{x_i\in\Phi_b^a}\mathbb{E}_{X_i}\left\{\exp\left(-\zeta X_i\|x_i\|^{-\alpha}\right)\right\}\right\}\\ &\overset{(a)}{=} \exp\left(-2\pi\lambda_b p_a\int_0^{\infty}(1-\chi)\,rdr\right),\end{aligned} \tag{40}$$

where (a) follows from the PGFL over PPP. Let us define the integral $\chi = \int_0^{\infty} e^{-\zeta x r^{-\alpha}} f_{X_i}(x)dx$ as the Laplace transform of X_i. Employing ([28], Eq. (8.352.1)) we can have:

$$\chi = \begin{cases}\left(1+\varphi r^{-\alpha}\right)^{-M}, & if\ \xi = 1,\\ \frac{(1-\xi)^{1-M}}{1+\varphi r^{-\alpha}} - \sum_{m=0}^{M-2}\frac{\xi(1-\xi)^{m+1-M}}{\left(1+\xi\varphi r^{-\alpha}\right)^{m+1}}, & otherwise,\end{cases} \tag{41}$$

where $\varphi = \phi p\zeta$. We define $\tau_1 = \int_0^{\infty}(1-\chi)\,rdr$, and by using ([29], Eq. (8)) it can be derived as:

$$\tau_1 = \begin{cases}\varphi^{\rho}\kappa_{M+1}, & if\ \xi = 1,\\ \frac{\varphi^{\rho}\kappa_2}{(1-\xi)^{M-1}} - \sum_{m=0}^{M-2}\frac{\varphi^{\rho}\xi^{1+\rho}\kappa_{m+2}}{(1-\xi)^{M-m-1}}, & otherwise,\end{cases} \tag{42}$$

Hence, we can obtain:

$$\mathcal{L}_{I_{c-d}}(\zeta) = \exp\left(-\pi\lambda_b p_a k\zeta^{\rho}\right), \tag{43}$$

where k is given in (23).

Employing ([13], Eq. (7-10)) we can easily obtain:

$$\mathcal{L}_{I_{d-d}}(\zeta) = \exp\left(-\frac{\pi\lambda_d p_d^{\rho}\zeta^{\rho}}{\sin c\rho}\right). \tag{44}$$

Then, combing (43), (44) and plugging into (22), we can obtain the result in (23).

Acknowledgements

This work is supported in part by China's High-Tech R&D Program (863 Program) SS2015AA011306; the open research fund of National Mobile Communications Research Laboratory, Southeast University (No.2013D09) and National Natural Science Foundation of China under Grants No.61379006, 61521003, and 61401510.

Authors' contributions

YC put forward the idea and wrote the manuscript. XJ and KH took part in the discussion and they also guided, reviewed, and checked the writing. JY, XH, and YX carried out experiments and analyzed experimental results. All authors read and approved the final manuscript.

Competing interests

The authors declare that they have no competing interests.

Author details

[1] National Digital Switching System Engineering and Technological R&D Center, No.7, Jianxue Road, 450002 Zhengzhou, China. [2] National Mobile

Communications Research Laboratory, Southeast University, No.2, Southeast University Road, 211189 Nanjing, China. [3]National Engineering Lab for Mobile Networking Security, No.10, Westtucheng Road, 100876 Beijing, China.

Received: 27 July 2017 Accepted: 24 October 2017
Published online: 02 November 2017

References

1. M Agiwal, A Roy, N Saxena, Next Generation 5G Wireless Networks: A Comprehensive Survey. IEEE Commun. Surv. Tutor. **18**(3), 1617–1655 (2016)
2. A Asadi, Q Wang, V Mancuso, A survey on device-to-device communication in cellular networks. IEEE Commun. Surv. Tutor. **16**(4), 1801–1819 (2014)
3. G Ding, J Wang, Q Wu, Q Yao, Y Song, F Tsiftsis, Cellular-base-station-assisted device-to-device communications in TV white space. IEEE J. Sel. Areas Commun. **34**(3), 107–121 (2016)
4. Technical specification group services and system aspects; feasibility study for proximity services (ProSe). Cedex, France, 3GPP TR 22.803, 2012, Rel-12
5. LS on agreements from TSG RAN on work on public safety related use cases in Release 12. Cedex, France, 3GPP TD SP-130478, Sep. 2013
6. J Yue, C Ma, H Yu, W Zhou, Secrecy-based access control for device-to-device communication underlaying cellular networks. IEEE Commun. Lett. **17**(11), 2068–2071 (2013)
7. R Zhang, X Cheng, L Yang, Cooperation via spectrum sharing for physical layer security in device-to-device communications underlaying cellular networks. IEEE Trans. Wirel. Commun. **15**(8), 5651–5663 (2016)
8. L Sun, Q Du, P Ren, Y Wang, Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation. IEEE Trans. Veh. Technol. **65**(10), 8767–8774 (2016)
9. X Kang, X Ji, K Huang, X Li, Security-oriented distributed access selection for D2D underlaying cellular networks. IET Electron. Lett. **53**(1), 32–34 (2017)
10. Y Chen, X Ji, K Huang, X Kang, Secrecy-outage-probability-based Access Strategy for Device-to-device Communications Underlaying Cellular Networks. J. Commun. **37**(8), 86–94 (2016)
11. Y Chen, X Ji, K Huang, B Li, X Kang, Opportunistic access control for enhancing security in D2D-enabled cellular networks. Sci China Inf Sci (2016). doi:10.1007/s11432-017-9160-y
12. Y Liu, L Wang, S Zaidi, M Elkashlan, T Duong, Secure D2D Communication in Large-Scale Cognitive Cellular Networks: A Wireless Power Transfer Model. IEEE Trans. Commun. **64**(1), 329–342 (2016)
13. C Ma, J Liu, X Tian, H Yu, Y Cui, X Wang, Interference exploitation in D2D-enabled cellular networks: A secrecy perspective. IEEE Trans. Commun. **63**(1), 229–242 (2015)
14. Z Chu, K Cumanan, M Xu, Z Ding, Robust secrecy rate optimizations for multiuser multiple-input-single-output channel with device-to-device communications. IET Commun. **9**(3), 396–403 (2015)
15. Z Chu, X Nguyen, T Le, M Karamanoglu, et al., *Game theory based secure wireless powered D2D communications with cooperative jamming*, (2017 Wireless Days, Porto, 2017), pp. 95–98
16. S Goel, R Negi, Guaranteeing secrecy using artificail noise. IEEE Trans. Wirel. Commun. **7**(6), 2180–2189 (2008)
17. Z Chu, Z Zhu, M Johnston, et al., Simultaneous Wireless Information Power Transfer for MISO Secrecy Channel. IEEE Trans. Veh. Technol. **65**(9), 6913–6925 (2016)
18. X Kang, X Ji, K Huang, Secure D2D Underlaying Cellular Communication Based on Artificial Noise Assisted. J. Commun. **36**(10), 149–156 (2015)
19. X Kang, X Ji, K Huang, Z Zhong, Secure D2D communication Underlaying Cellular Networks: Artificial Noise Assisted. *in Proceedings of the IEEE International Conference on Vehicular Technology (VTC).* (Montreal, 2016)
20. A Thangaraj, S Dihidar, AR Calderbank, SW McLaughlin, J-M Merolla, Applications of LDPC codes to the wiretap channel. IEEE Trans. Inf. Theory. **53**(8), 2933–2945 (2007)
21. X Xu, B He, W Yang, X Zhou, Y Cai, Secure Transmission Design for Cognitive Radio Networks With Poisson Distributed Eavesdroppers. IEEE Trans. Inf. Forensic Secur. **11**(2), 373–387 (2016)
22. C Li, J Zhang, KB Letaief, Throughput and energy efficiency analysis of small cell networks with multi-antenna base stations. IEEE Trans. Wirel. Commun. **13**(5), 2505–2517 (2014)
23. C Liu, L Wang, Optimal cell load and throughput in green small cell networks with generalized cell association. IEEE J. Sel. Areas Commun. **34**(5), 1058–1072 (2016)
24. D Stoyan, W Kendall, J Mecke, *Stochastic Geometry and Its Applications*, 2nd ed. (Wiley, Hoboken, 1996)
25. X Zhang, X Zhou, MR McKay, Enhancing secrecy with multiantenna transmission in wireless ad hoc networks. IEEE Trans. Inf. Forensic Secur. **8**(11), 1802–1814 (2013)
26. H Wang, T Zheng, J Yuan, D Towsley, M Lee, Physical Layer Security in Heterogeneous Cellular Networks. IEEE Trans. Commun. **64**(3), 1204–1219 (2016)
27. W Wang, KC Teh, KH Li, Artificial Noise Aided Physical Layer Security in Multi-Antenna Small-Cell Networks. IEEE Trans. Inf. Forensic Secur. **12**(6), 1470–1483 (2017)
28. I Gradshteyn, I Ryzhik, A Jeffrey, D Zwillinger, S Technica, *Table of Integrals, Series, and Products*. (Academic, New York, 2007)
29. M Haenggi, JG Andrews, F Baccelli, O Dousse, M Franceschetti, Stochastic geometry and random graphs for the analysis and design of wireless networks. IEEE J. Sel. Areas Commun. **27**(7), 1029–1046 (2009)
30. J Zhu, R Schober, V Bhargava, Secure transmission in multi-cell massive MIMO systems. IEEE Trans. Wirel. Commun. **13**(9), 4766–4781 (2014)