SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2018, Vol. 61 022310:1–022310:15
doi: 10.1007/s11432-016-9149-4

Physical layer security in multi-antenna cognitive heterogeneous cellular networks: a unified secrecy performance analysis

Xiaohui QI[1], Kaizhi HUANG[1], Bin LI[2*], Liang JIN[1] & Xinsheng JI[1]

[1]*National Digital Switching System Engineering & Technological Research Center, Zhengzhou* 450002*, China;*
[2]*School of Information and Electronics, Beijing Institute of Technology, Beijing* 100081*, China*

Received 25 December 2016/Revised 4 April 2017/Accepted 24 May 2017/Published online 22 September 2017

Abstract Cognitive heterogeneous cellular networks (CHCNs) are emerging as a promising approach to next-generation wireless communications owing to their seamless coverage and high network throughput. In this paper, we describe our reliance on multi-antenna technology and a secrecy transmission protocol to ensure the reliability and security of downlink underlay CHCNs. First, we introduce a two-tier CHCN model using a stochastic geometry framework, and derive the probability distribution of the indicator function for a secrecy transmission scheme. We then investigate the connection outage probability, secrecy outage probability (SOP), and transmission SOP of both primary and cognitive users under a secrecy guard scheme and a threshold-based scheme. Furthermore, we reveal some insights into the secrecy performance by properly setting the predetermined access threshold and the radius of detection region for the secrecy transmission scheme. Finally, simulation results are provided to show the influence of the antenna system, eavesdropper density, predetermined access threshold, and radius of the detection region on the reliability and security performance of a CHCN.

Keywords cognitive heterogeneous cellular network, physical layer security, secrecy guard scheme, threshold-based scheme, multi-antenna technique

Citation Qi X H, Huang K Z, Li B, et al. Physical layer security in multi-antenna cognitive heterogeneous cellular networks: a unified secrecy performance analysis. Sci China Inf Sci, 2018, 61(2): 022310, doi: 10.1007/s11432-016-9149-4

1 Introduction

The fifth-generation (5G) wireless network will serve as a key enabler in meeting the ever-increasing demand for higher data rates, larger numbers of devices, and wider radio coverage [1–3]. As one of the flexible solutions of 5G, heterogeneous cellular networks (HCNs) represent a development trend benefiting from high network throughput and seamless wireless coverage, which have a continuously increasing demand for wireless spectrum [4, 5]. On the other hand, the cognitive radio (CR) technique can be used to solve the conflict between the wireless spectrum under-utilization and scarcity by allowing cognitive users (CUs) to transmit concurrently on the same frequency bands as licensed primary users (PUs) as long as the quality of service (QoS) of the primary network is satisfied [6]. However, the dynamic and inherent openness of CR networks (CRNs) have generated several security threats and challenges [7]. As an effective means to safeguard wireless channels, physical layer security (PLS) has been proposed as

* Corresponding author (email: libin_sun@bit.edu.cn)

a complement to traditional cryptographic techniques, and has elicited substantial research interests in recent years [8–12].

The PLS applications have been introduced into CRNs, e.g., cooperative relays [13, 14], multiple antennas [15], multi-user scheduling [16], and transmission schemes [7]. In particular, Ref. [13] investigated single-relay and multiply-relays selection schemes in a CRN to enhance the secrecy transmission. In [14], the authors studied the robust resource allocation problem for secure communication in a relaying CRN with multiple eavesdroppers, where the power and sub-carrier can be obtained using robust optimization theory. A secure multiple antenna transmission scheme in which the CUs can obtain a transmission opportunity to achieve their own data traffic by providing a secrecy guarantee for a PU with artificial noise (AN) was proposed to maximize the secrecy throughput of PUs for a CRN [15]. In [16], the authors proposed a user-scheduling scheme to obtain multiple-user diversity and enhance the security of CUs while guaranteeing the QoS requirements of the PUs. In [7], four transmission schemes were proposed to achieve PLS in CRNs with different assumptions regarding the location knowledge at the eavesdroppers, as well as the channel knowledge at cognitive femto base stations (CFBSs). However, the CRN model with low randomness mentioned above cannot apply to HCNs with a highly dynamic topology. As a useful mathematical tool to model a random network topology, stochastic geometry theory has been used to study the average behavior of a random network [17–20]. In [17], the authors studied the secrecy performance of a multi-antenna transmission with AN in the presence of randomly distributed eavesdroppers under slow fading channels. In [18], the researchers investigated a single-input multi-output communication system coexisting with randomly located eavesdroppers and proposed an opportunistic jammer selection scheme for improving the PLS. In [19], the impact of AN on securing the communications in a multi-cell cellular network and optimizing power allocation between the AN and desired signals was investigated. In [20], an access threshold-based secrecy mobile association policy was proposed, and a comprehensive study on the PLS in a multi-tier HCN was described.

Recently, the PLS of a cognitive HCN (CHCN) has attracted considerable attention [21–23]. In CHCNs, most studies have assumed that the base stations (BSs), users, and eavesdroppers are randomly distributed following independent homogeneous Poisson point processes (HPPPs). While considering the HPPP of the CUs and the eavesdroppers, the effects of the stochastic interference generated by CFBSs on the secrecy capacity of the PUs were analyzed in [21]. With the QoS constraint of a PU, the beamforming and AN generation at the CFBSs were investigated to secure secondary transmission in a large-scale CHCN [22]. A tradeoff metric of the secrecy energy efficiency and secrecy spectrum efficiency for safeguarding a wireless transmission in an underlay CHCN were examined in [23]. However, the majority of existing studies on the PLS in a CHCN have not considered the joint performance of security and reliability in a primary user network (PUN) or a cognitive user network (CUN). The total secrecy throughput of a multi-antenna network with a secrecy transmission scheme has also not been taken into consideration in existing research on the combination of PLS and CHCNs.

Motivated by these previous studies, in this paper, we focus on the PLS in an underlay multi-antenna CHCN. The location sets of the primary BSs (PBSs), CFBSs, CUs, and eavesdroppers are modeled as independent HPPPs. Both the secrecy guard zone scheme and the threshold-based scheme for point-to-point communication [7] are introduced into our scenario. Unlike [7], we analyze the impacts on the security, reliability, and their joint performance for multi-antenna CHCNs. In addition, the effects of the secrecy guard zone scheme designed in [7] and threshold-based scheme designed in [20] on the secrecy throughput are also studied. Assuming that eavesdroppers can intercept a primary and secondary transmission simultaneously, the security and reliability of both a PUN and a CUN are further considered in this paper.

Our contributions can be summarized as follows.

(1) We model CHCNs using the threshold-based scheme and secrecy guard scheme, and provide an indicator function for whether the CUs can share the radio spectrum of the PUs. Based on the secrecy transmission scheme, we derive the probability of the indicator function being equal to 1, as well as the activation probability of the CFBS.

(2) We analyze the connection outage probability (COP), secrecy outage probability (SOP), and trans-

mission SOP (TSOP) of both PUs and CUs, which are outage metrics for evaluating the probability of achieving reliable and secure transmission. We then analyze the security, reliability, and joint performance of the security and reliability of both a PUN and a CUN.

(3) We further derive the average secrecy throughput of a PUN and a CUN. Based on the results obtained, the average secrecy throughput of multi-antenna CHCNs is derived. The optimum value of the average secrecy throughput is then given by analyzing the simulation results, which shows how the threshold-based scheme and the secrecy guard scheme influence the average secrecy throughput.

Notations. The probability and expectation are denoted by $\mathbb{P}(\cdot)$ and $\mathrm{E}(\cdot)$, respectively. $\|\cdot\|$, $|\cdot|$, and $(\cdot)^{\dagger}$ denote the Euclidean norm, absolute value, and conjugate, respectively. $\Gamma(a,b)$ indicates the Gamma distribution with shape a and scale parameter b. $\Gamma(\cdot)$ is a Gamma function. $\exp(c)$ represents the exponent distribution with parameter c. Finally, $B'(a,b,z)=\int_z^1 t^{a-1}(1-t)^{b-1}\mathrm{d}t$ is a Beta function.

2 System model

We consider a two-tier multi-antenna downlink CHCN consisting of a PUN and a CUN, where the CUN shares the spectrum resource licensed to the PUN. The PUN consists of multiple PBSs that transmit signals to multiple PUs. In addition, the CUN has multiple CFBSs serving multiple CUs. With CR capability, a CFBS is able to not only actively obtain the knowledge from ambient environment, but also constrict the interference to the PUs to less than a predefined threshold [24]. In PUNs, the transmit power of a PBS is P_{p}, the number of antennas is M_{p}, and the number of PUs served in each resource block of the PBS is Ψ_{p}. In CUNs, the transmit power of the CFBS is P_{c}, the number of antennas is M_{c}, and the number of CUs served in each resource block of the CFBS is Ψ_{c}.

We denote the set of PBSs, CFBSs, CUs, and eavesdropper locations as Φ_{p}, Φ_{c}, Φ_{CU}, and Φ_{E}, which follow independent HPPPs with densities λ_{p}, $\bar{\lambda}_{\mathrm{c}}$, λ_{CU}, and λ_{E}, respectively, the feasibility of which has been verified through both theoretical validation [25] and empirical evidence [26]. According to Slivnyak's theorem [27], the analysis can be performed at a typical user located at the origin. Compared with interference, noise has almost no effect on legitimate users in a CHCN [27]. For the sake of simplicity, we assume that the noise received by users and eavesdroppers is negligible.

In this paper, the system model has four other restraints: (1) All the channels undergo independent and identically distributed quasi-static Rayleigh fading. (2) All the BSs use pre-coding $\boldsymbol{w}=\boldsymbol{h}^{\dagger}/\|\boldsymbol{h}\|$, where $\boldsymbol{h}$ is the corresponding channel. (3) Perfect CSI is available at the BSs, and (4) the eavesdroppers can intercept the secret information intended for the PUs and that intended for the CUs simultaneously.

2.1 Channel model in PUNs

In a PUN, the PU is served by the PBS $x_{\mathrm{p}}\in\Phi_{\mathrm{p}}$. Here, $\|x_{\mathrm{p}}\|$ denotes the distance between the serving PBS and a typical PU. The received signal-interference-plus-noise ratio (SINR) of the user served by the PBSs is given as

$$\mathrm{SINR}_{\mathrm{U,p}}=\frac{P_{\mathrm{p}}h_{x_{\mathrm{p}},o}\|x_{\mathrm{p}}\|^{-\alpha}}{I_{\mathrm{U,p}}}, \tag{1}$$

where $P_{\mathrm{p}}h_{x_{\mathrm{p}},o}\|x_{\mathrm{p}}\|^{-\alpha}$ is the received power of the PU, $h_{x_{\mathrm{p}},o}\sim\Gamma(\Delta_{\mathrm{p}},1)$ [28] indicates the array gain of the main channel ($\Delta_{\mathrm{p}}=M_{\mathrm{p}}-\Psi_{\mathrm{p}}+1$), and $\|x_{\mathrm{p}}\|^{-\alpha}$ is the path loss. In addition, $I_{\mathrm{U,p}}=I_{\mathrm{c,p}}^{\mathrm{U}}+I_{\mathrm{p,p}}^{\mathrm{U}}$ represents the received interference of the PU, where $I_{\mathrm{c,p}}^{\mathrm{U}}=\sum_{y_{\mathrm{c}}\in\Phi_{\mathrm{c\_act}}}P_{\mathrm{c}}g_{y_{\mathrm{c}},\mathrm{p}}\|y_{\mathrm{c}}\|^{-\alpha}$ is the interference power of the PU from all of the active CFBSs, $\|y_{\mathrm{c}}\|$ is the distance between the typical user and the CFBS y_{c}, $I_{\mathrm{p,p}}^{\mathrm{U}}=\sum_{y_{\mathrm{p}}\in\Phi_{\mathrm{p}}\setminus x_{\mathrm{p}}}P_{\mathrm{p}}g_{y_{\mathrm{p}},\mathrm{p}}\|y_{\mathrm{p}}\|^{-\alpha}$ is the interference power of the PU from the PBSs, $\|y_{\mathrm{p}}\|$ is the distance between a typical user and a PBS y_{p}, $g_{y_i,\mathrm{p}}\sim\Gamma(\Psi_i,1)$ [28] is the array gain of the corresponding interference channel, and $i\in\{\mathrm{p},\mathrm{c}\}$. The set of active CFBSs is a thinning of Φ_{c}, which is denoted by $\Phi_{\mathrm{c\_act}}$ with density $\lambda_{\mathrm{c}}=P_{\mathrm{c\_act}}\bar{\lambda}_{\mathrm{c}}$, where $P_{\mathrm{c\_act}}$ is determined based on the secrecy transmission scheme given in Subsection 2.3, which denotes the activation probability of the CFBSs.

In this paper, we consider a non-colluding and passive eavesdropping scenario in which each eavesdropper intercepts the signal of a typical PU independently without any attacks. In this case, we only pay

attention to the eavesdropper that has the largest received SINR [24]. Such an eavesdropper is considered to be the most malicious, and its received SINR can be written as

$$\mathrm{SINR}_{\mathrm{E,p}} = \max_{e\in\Phi_{\mathrm{E}}} \left\{ \frac{P_{\mathrm{p}} h_{e,\mathrm{p}} \|x_{e,\mathrm{p}}\|^{-\alpha}}{I_{\mathrm{E},p}} \right\}, \tag{2}$$

where $h_{e,\mathrm{p}} \sim \exp(1)$ [28] denotes the equivalent small-scale fading channel power gain for the eavesdropper's received SINR, $\|x_{e,\mathrm{p}}\| = \|x_{\mathrm{p}} - e\|$ denotes the distance between the eavesdropper e and its target BS, $I_{\mathrm{E,p}} = I_{\mathrm{p,p}}^{\mathrm{E,intra}} + I_{\mathrm{p,p}}^{\mathrm{E,\,inter}} + I_{\mathrm{c,p}}^{\mathrm{E}}$ represents the interference received by the eavesdroppers who intercept the signal of the PUs, $I_{\mathrm{p,p}}^{\mathrm{E,intra}} = P_{\mathrm{p}} g_{e,\mathrm{p}} \|x_{e,\mathrm{p}}\|^{-\alpha}$ is the intra-cell interference in PUNs with $g_{e,\mathrm{p}} \sim \Gamma(\Psi_{\mathrm{p}} - 1, 1)$ [28] (the signals intended for all users located in the same cell excluding the target user are treated as interference), $I_{\mathrm{p,p}}^{\mathrm{E,\,inter}} = \sum_{y_{\mathrm{p}}\in\Phi_{\mathrm{p}}\setminus x_{\mathrm{p}}} P_{\mathrm{p}} g_{e,y_{\mathrm{p}}} \|y_{\mathrm{p}} - e\|^{-\alpha}$ is the inter-cell interference in the PUNs with $g_{e,y_{\mathrm{p}}} \sim \Gamma(\Psi_{\mathrm{p}}, 1)$ [28], $\|y_{\mathrm{p}} - e\|$ is the distance between the eavesdropper and the PBS y_{p}, $I_{\mathrm{c,p}}^{\mathrm{E}} = \sum_{y_{\mathrm{c}}\in\Phi_{\mathrm{c\_act}}} P_{\mathrm{c}} g_{e,y_{\mathrm{c}}} \|y_{\mathrm{c}} - e\|^{-\alpha}$ is the interference from all of the active CFBSs with $g_{e,y_{\mathrm{c}}} \sim \Gamma(\Psi_{\mathrm{c}}, 1)$ [28], and $\|y_{\mathrm{c}} - e\|$ is the distance between the eavesdropper and the CFBS y_{c}. For convenience, the most malicious eavesdropper denotes a non-colluding eavesdropper throughout the remainder of this article.

2.2 Channel model in CUNs

In a CUN, a typical CU is served by the CFBS $x_{\mathrm{c}} \in \Phi_{\mathrm{c}}$. Here, $\|x_{\mathrm{c}}\|$ denotes the distance between the serving CFBS and a typical CU. When the secrecy transmission condition is satisfied, i.e., $\mu = 1$, the received SINR of the user served by the CFBSs is

$$\mathrm{SINR}_{\mathrm{U,c}} = \frac{P_{\mathrm{c}} h_{x_{\mathrm{c}},o} \|x_{\mathrm{c}}\|^{-\alpha}}{I_{\mathrm{U,c}}}, \tag{3}$$

where μ denotes an indicator function given in Subsection 2.3, $P_{\mathrm{c}} h_{x_{\mathrm{c}},o} \|x_{\mathrm{c}}\|^{-\alpha}$ is the received power of a typical CU, $h_{x_{\mathrm{c}},o} \sim \Gamma(\Delta_{\mathrm{c}}, 1)$ [28] denotes the array gain of the main channel ($\Delta_{\mathrm{c}} = M_{\mathrm{c}} - \Psi_{\mathrm{c}} + 1$), and $\|x_{\mathrm{c}}\|^{-\alpha}$ represents the path loss. The received interference power of a typical CU is $I_{\mathrm{U,c}} = I_{\mathrm{p,c}}^{\mathrm{U}} + I_{\mathrm{c,c}}^{\mathrm{U}}$, where $I_{\mathrm{p,c}}^{\mathrm{U}} = \sum_{y_{\mathrm{p}}\in\Phi_{\mathrm{p}}} P_{\mathrm{p}} g_{y_{\mathrm{p}},\mathrm{c}} \|y_{\mathrm{p}}\|^{-\alpha}$ is the received interference power of a CU from the PBSs y_{p}, $I_{\mathrm{c,c}}^{\mathrm{U}} = \sum_{y_{\mathrm{c}}\in\Phi_{\mathrm{c\_act}}\setminus x_{\mathrm{c}}} P_{\mathrm{c}} g_{y_{\mathrm{c}},\mathrm{c}} \|y_{\mathrm{c}}\|^{-\alpha}$ is the received interference power of a CU from the CFBSs y_{c}, $g_{y_i,\mathrm{c}} \sim \Gamma(\Psi_i, 1)$ [28] denotes the array gain of the corresponding interference channel, and $i \in \{\mathrm{p}, \mathrm{c}\}$.

When the target BS is a CFBS and the secrecy transmission condition is satisfied, the SINR of the most malicious eavesdropper is

$$\mathrm{SINR}_{\mathrm{E,c}} = \max_{e\in\Phi_{\mathrm{E}}} \left\{ \frac{P_{\mathrm{c}} h_{e,\mathrm{c}} \|x_{e,\mathrm{c}}\|^{-\alpha}}{I_{\mathrm{E,c}}} \right\}, \tag{4}$$

where $h_{e,\mathrm{c}} \sim \exp(1)$ [28], $\|x_{e,\mathrm{c}}\| = \|x_{\mathrm{c}} - e\|$ denotes the distance between the eavesdropper e and its target BS, $I_{\mathrm{E,c}} = I_{\mathrm{c,c}}^{\mathrm{E,intra}} + I_{\mathrm{c,c}}^{\mathrm{E,inter}} + I_{\mathrm{p,c}}^{\mathrm{E}}$ represents the interference received by any eavesdroppers who intercept a signal of the CUs, $I_{\mathrm{c,c}}^{\mathrm{E,intra}} = P_{\mathrm{c}} g_{e,\mathrm{c}} \|x_{e,\mathrm{c}}\|^{-\alpha}$ denotes the intra-cell interference in CUNs with $g_{e,\mathrm{c}} \sim \Gamma(\Psi_{\mathrm{c}} - 1, 1)$ [28], $I_{\mathrm{c,c}}^{\mathrm{E,inter}} = \sum_{y_{\mathrm{c}}\in\Phi_{\mathrm{c\_act}}\setminus x_{\mathrm{c}}} P_{\mathrm{c}} g_{e,y_{\mathrm{c}}} \|y_{\mathrm{c}} - e\|^{-\alpha}$ is the inter-cell interference in the CUNs, $I_{\mathrm{p,c}}^{\mathrm{E}} = \sum_{y_{\mathrm{p}}\in\Phi_{\mathrm{p}}} P_{\mathrm{p}} g_{e,y_{\mathrm{p}}} \|y_{\mathrm{p}} - e\|^{-\alpha}$ denotes interference from the MBSs, and the distribution of $g_{e,y_{\mathrm{p}}}$ and $g_{e,\mathrm{c}}$ is as given in Subsection 2.1.

2.3 Secrecy transmission scheme

In an underlay CHCN, a PUN allows a CUN to share the spectrum using an underlay method, and requires that the instantaneous interference power at the PU from the CFBSs be lower than a predefined threshold [7]. In this paper, the threshold-based scheme designed in [20], and the secrecy guard scheme designed in [7], are used to improve the security and/or reliability performance of a CHCN. For the threshold-based scheme, the served CFBS x_{c} broadcasts data only when the truncated average received

signal power (ARSP) at the CUs (i.e., $P_{\rm c}\Delta_{\rm c}\|x_{{\rm c},x_{\rm CU}}\|^{-\alpha}$, where $\|x_{{\rm c},x_{\rm CU}}\| = \|x_{\rm c} - x_{\rm CU}\|$ is the distance between $x_{\rm c}$ and a typical CU $x_{\rm CU}$) is larger than a predetermined access threshold γ_μ. Otherwise, the served CFBSs suspend the transmission. For the secrecy guard scheme, a CFBS $x_{\rm c}$ is permitted to send messages only when no eavesdroppers are detected within the detection region. To this end, we let μ denote the expression of the indicator function for whether the CUs can share the radio spectrum of the PUs (i.e., a transmission is on or off in a CFBS), which can be given as

$$\mu = \begin{cases} 1, \ P_{\rm c}\Delta_{\rm c}\|x_{{\rm c},x_{\rm CU}}\|^{-\alpha} > \gamma_\mu \text{ and } \forall \text{eavesdropper} \notin \Phi_{R_\mu}, \\ 0, \ P_{\rm c}\Delta_{\rm c}\|x_{{\rm c},x_{\rm CU}}\|^{-\alpha} \leqslant \gamma_\mu \text{ or at least one eavesdropper} \in \Phi_{R_\mu}, \end{cases} \tag{5}$$

where Φ_{R_μ} is the detection region with a radius R_μ. Such an "on-off" transmission strategy can effectively enhance the reliability and/or security in a CRN, which has been confirmed in [7].

Lemma 1. The probability of $\mu = 1$ is given by

$$\begin{aligned} P_{\mu=1} =& \mathbb{P}\left(P_{\rm c}\Delta_{\rm c}\|x_{{\rm c},x_{\rm CU}}\|^{-\alpha} > \gamma_\mu\right)\mathbb{P}\left(\text{No eavesdropper within detection region } \Phi_{R_\mu}\right) \\ =& {\rm e}^{-\pi\lambda_{\rm E}R_\mu^2}\int_0^{\left(\frac{P_{\rm c}\Delta_{\rm c}}{\gamma_\mu}\right)^{1/\alpha}} f_{\|x_{{\rm c},x_{\rm CU}}\|}(x)\,{\rm d}x \\ =& \left(1 - \exp\left(-\pi\lambda_{\rm CU}\left(P_{\rm c}\Delta_{\rm c}\gamma_\mu^{-1}\right)^{2/\alpha}\right)\right){\rm e}^{-\pi\lambda_{\rm E}R_\mu^2}, \end{aligned} \tag{6}$$

where $f_{\|x_{{\rm c},x_{\rm CU}}\|}(x) = 2\pi\lambda_{\rm CU}x\exp(-\pi\lambda_{\rm CU}x^2)$ is the probability distribution functions (PDF) of the distance between a CFBS and CUs [29].

Using the null probability of 2-D HPPP in [29], we have

$$\mathbb{P}\left(\text{No eavesdropper within detection region}\right) = {\rm e}^{-\pi\lambda_{\rm E}R_\mu^2}. \tag{7}$$

It is worth noting that a CFBS will be active when an associated CU exists, and the activation probability of the CFBS is defined as

$$\begin{aligned} P_{\rm c\_act} =& \mathbb{P}(\text{The CFBS associates with at least one CU} \\ & \text{and no eavesdropper is present within the detection region}) \\ =& \left[1 - {\rm E}_{\Phi_{\rm CU}}\left[\prod_{x_{\rm CU}\in\Phi_{\rm CU}} \mathbb{P}(x_{\rm CU}\text{is not associated with the CFBS})\right]\right] \\ & \times \mathbb{P}(\text{no eavesdropper within } \Phi_{R_\mu}). \end{aligned} \tag{8}$$

From Subsections 2.1 and 2.2, we can observe that the activation probability of the CFBS $P_{\rm c\_act}$ is necessary, which is derived in the following Lemma 2.

Lemma 2. The activation probability of the CFBS is given by

$$P_{\rm c\_act} = \left[1 - \exp\left[-\lambda_{\rm CU}\bar{\lambda}_{\rm c}^{-1}\left(1 - {\rm e}^{-\pi\bar{\lambda}_{\rm c}\left(P_{\rm c}\Delta_{\rm c}\gamma_\mu^{-1}\right)^{2/\alpha}}\right)\right]\right]{\rm e}^{-\pi\lambda_{\rm E}R_\mu^2}. \tag{9}$$

Proof. Please refer to Appendix A.

3 Performance analysis in PUNs

In this section, we analyze the performance of PLS in a PUN. In the following, we consider three secrecy performance metrics, namely, COP, SOP, and TSOP.

3.1 COP in PUNs

When a message of a legitimate user cannot be decoded without error, a connection outage occurs. The expression of the COP is given by

$$P_{\mathrm{co},i}\left(\hat{R}_i\right)=\mathbb{P}\left(\log\left(1+\mathrm{SINR}_{\mathrm{U},i}\right)<\hat{R}_i\,|\mu=1\right), \tag{10}$$

where $i\in\{\mathrm{c},\mathrm{p}\}$, $\hat{R}_i$ is the target channel capacity of $P_{\mathrm{co},i}(\hat{R}_i)$. The COP of a PU is given in the following theorem.

Theorem 1. For a typical PU served by a PBS, its COP is provided as

$$P_{\mathrm{co,p}}\left(\hat{R}_{\mathrm{p}}\right)=\mathbb{P}\left(R_{\mathrm{p}}<\hat{R}_{\mathrm{p}}\,|\mu=1\right)=F_{\mathrm{SINR}_{\mathrm{U,p}}}\left(2^{\hat{R}_{\mathrm{p}}}-1\right), \tag{11}$$

where $R_{\mathrm{p}}=\log\left(1+\mathrm{SINR}_{\mathrm{U,p}}\right)$ denotes the channel capacity of a PU, $\hat{R}_{\mathrm{p}}$ is the target channel capacity of a PU, and $F_{\mathrm{SINR}_{\mathrm{U,p}}}(\gamma)$ is the cumulative distribution function (CDF) of the SINR recorded at a PU. $F_{\mathrm{SINR}_{\mathrm{U,p}}}(\gamma)$ is derived as

$$\begin{aligned}F_{\mathrm{SINR}_{\mathrm{U,p}}}(\gamma)=&1-\int_0^{\infty}\mathbb{P}\left(h_{x_{\mathrm{p}},o}>\frac{\gamma I_{\mathrm{U,p}}}{P_{\mathrm{p}}x^{-\alpha}}\right)f_{\|x_{\mathrm{p}}\|}\left(x\right)\mathrm{d}x\\=&1-\int_0^{\infty}\sum_{n=0}^{\Delta_{\mathrm{p}}-1}\frac{1}{n!}(-s)^n\frac{\mathrm{d}^n}{\mathrm{d}s^n}\left(L_{I_{\mathrm{U,p}}}\left(s\right)\right)f_{\|x_{\mathrm{p}}\|}\left(x\right)\mathrm{d}x\\\overset{\mathrm{(a)}}{=}&1-\pi\lambda_{\mathrm{p}}\sum_{n=0}^{\Delta_{\mathrm{p}}-1}\frac{1}{n!}\left(\frac{\gamma}{P_{\mathrm{p}}}\right)^n\sum_{\bar{m}\in M(n)}\frac{C\left(\bar{m}\right)F_{\mathrm{p}}\left(\bar{m},\gamma\right)\Gamma\left(\sum m_l+1\right)}{\left[\sum_{j=\mathrm{p,c}}\lambda_j\tilde{C}_{j,\mathrm{p}}^{\gamma}(\gamma\hat{P}_{j,\mathrm{p}})^{2/\alpha}+\pi\lambda_{\mathrm{p}}\right]^{\sum m_l+1}},\end{aligned} \tag{12}$$

where (a) can be achieved by $\frac{\mathrm{d}^n L_{I_{\mathrm{U,p}}}(s)}{\mathrm{d}s^n}$ and $f_{\|x_{\mathrm{p}}\|}(x)$. $L_{I_{\mathrm{U,p}}}(s)=\mathrm{E}[\mathrm{e}^{-sI_{\mathrm{U,p}}}]$, $s=\gamma P_{\mathrm{p}}^{-1}x^{\alpha}$, $\tilde{C}_{j,\mathrm{p}}^{\gamma}=\frac{2\pi}{\alpha}\sum_{m=1}^{\Psi_j}\binom{\Psi_j}{m}B'(\Psi_j-m+\frac{2}{\alpha},m-\frac{2}{\alpha},u_{j,\mathrm{p}}^{\gamma})$, $M(n)=\{\bar{m}=(m_1,m_2,\ldots,m_n):\sum_{i=1}^{n}im_i=n\}$, $C(\bar{m})=\frac{n!}{\prod_i(m_i!(i!)^{m_i})}$, $F_{\mathrm{p}}(\bar{m},\gamma)=\frac{\prod_{l=1}^{n}(\sum_{j=\mathrm{p,c}}D_{j,\mathrm{p}}^{\gamma}(l)P_j^{2/\alpha})^{m_l}}{(\gamma P_{\mathrm{p}}^{-1})^{-\frac{2}{\alpha}\sum m_l+n}(2\pi)^{-\sum m_l}}$, $u_{j,\mathrm{p}}^{\gamma}=(1+\gamma/(\hat{\Delta}_{j,\mathrm{p}}\hat{B}_{j,\mathrm{p}}))^{-1}$, $\hat{P}_{i,j}=P_i/P_j$, $\hat{\Delta}_{i,j}=\Delta_i/\Delta_j$, $\hat{B}_{i,j}=B_i/B_j$, $B_i=\sqrt{\Psi_i/\Delta_i}$, $i,j\in\{\mathrm{c},\mathrm{p}\}$, and $D_{j,\mathrm{p}}^{\gamma}(l)=\frac{(\Psi_j+l-1)!B'(\Psi_j+\frac{2}{\alpha},l-\frac{2}{\alpha},u_{j,\mathrm{p}}^{\gamma})}{\lambda_j^{-1}\alpha(\Psi_j-1)!}$. $f_{\|x_{\mathrm{p}}\|}(x)=2\pi\lambda_{\mathrm{p}}x\exp(-\pi\lambda_{\mathrm{p}}x^2)$, is the PDF of the distance between a PU and its serving PBS [30]. Additionally, $\frac{d^n L_{I_{\mathrm{U,p}}}(s)}{ds^n}=\mathrm{e}^{-\sum_{j=\mathrm{p,c}}\lambda_j\tilde{C}_{j,\mathrm{p}}^{\gamma}(\gamma\hat{P}_{j,\mathrm{p}})^{2/\alpha}x^2}\sum_{\bar{m}\in M(n)}C(\bar{m})x^{-n\alpha+2\sum m_l}(-1)^nF_{\mathrm{p}}(\bar{m},\gamma)$ has been given in [31].

3.2 SOP in PUNs

When the eavesdroppers have a better channel than the threshold, a secrecy outage occurs to ensure the secrecy of the messages. As an important PLS indicator, the SOP is expressed as

$$P_{\mathrm{so},i}\left(\hat{R}_{\mathrm{s},i}\right)=\mathbb{P}\left(\log_2\left(1+\mathrm{SINR}_{\mathrm{E},i}\right)>\hat{R}_i-\hat{R}_{\mathrm{s},i}\,|\mu=1\right), \tag{13}$$

where $i\in\{\mathrm{c},\mathrm{p}\}$, and $\hat{R}_{\mathrm{s},i}$ is the target secrecy rate of $P_{\mathrm{so},i}(\hat{R}_{\mathrm{s},i})$ [7].

In this subsection, assuming that randomly distributed eavesdroppers are non-colluding, we evaluate the SOP of the PUs.

Theorem 2. In PUNs, the SOP of a typical PU in the presence of multiple non-colluding eavesdroppers is given by

$$P_{\mathrm{so,p}}\left(\hat{R}_{\mathrm{s,p}}\right)=1-F_{\mathrm{SINR}_{\mathrm{E,p}}}\left(2^{\hat{R}_{\mathrm{p}}-\hat{R}_{\mathrm{s,p}}}-1\right)=1-\exp\left(\frac{-\lambda_{\mathrm{E}}\alpha\left(2^{\hat{R}_{\mathrm{p}}-\hat{R}_{\mathrm{s,p}}}\right)^{-(\Psi_{\mathrm{p}}-1)}}{A_{\mathrm{p}}\left(2^{\hat{R}_{\mathrm{p}}-\hat{R}_{\mathrm{s,p}}}-1\right)^{2/\alpha}}\right), \tag{14}$$

where $\hat{R}_{\mathrm{s,p}}$ is the target secrecy rate of $P_{\mathrm{so,p}}(\hat{R}_{\mathrm{s,p}})$, $F_{\mathrm{SINR}_{\mathrm{E,p}}}(\cdot)$ is the CDF of $\mathrm{SINR}_{\mathrm{E,p}}$, $C_{\alpha,\Psi_j,i}=\frac{\Gamma(i-2/\alpha)\Gamma(-i+2/\alpha+\Psi_j)}{\Gamma(\Psi_j)}$, and $A_{\mathrm{p}}=2\sum_{j=\mathrm{p,c}}\lambda_j\sum_{i=1}^{\Psi_j}\binom{\Psi_j}{i}(\frac{P_j}{P_{\mathrm{p}}})^{2/\alpha}C_{\alpha,\Psi_j,i}$.

Proof. Please refer to Appendix B.

3.3 TSOP in PUNs

We use the TSOP of the PUs to characterize the probability that either a connection outage or a secrecy outage will occur in a PUN, which can be expressed as [7]

$$P_{\mathrm{tso,p}} = 1 - \left(1 - P_{\mathrm{co,p}}\left(\hat{R}_{\mathrm{p}}\right)\right)\left(1 - P_{\mathrm{so,p}}\left(\hat{R}_{\mathrm{s,p}}\right)\right), \tag{15}$$

where $P_{\mathrm{co,p}}(\cdot)$ and $P_{\mathrm{so,p}}(\cdot)$ are derived in (11) and (14), respectively. Note that the TSOP can also reveal a tradeoff between reliability and security.

4 Performance analysis in CUNs

In this section, the COP, SOP, and TSOP of the CUs are obtained to analyze the security and reliability performance in a CUN. According to the above-defined spectrum sharing scheme and secrecy transmission scheme, to determine the COP, SOP, and TSOP in a CUN, the served CFBS must be able to transmit its data, i.e., $\mu = 1$.

4.1 COP in CUNs

The definition of COP is given in Subsection 3.1, and the COP of the CUs is provided in the following theorem.

Theorem 3. For a typical CU served by a CFBS, its COP is computed as

$$\begin{aligned} P_{\mathrm{co,c}}\left(\hat{R}_{\mathrm{c}}\right) =& \mathbb{P}\left(\log_2\left(1+\mathrm{SINR}_{\mathrm{U,c}}\right) < \hat{R}_{\mathrm{c}} \,|\mu = 1\right) \\ =& F_{\mathrm{SINR}_{\mathrm{U,c}}}\left(2^{\hat{R}_{\mathrm{c}}} - 1 \,\middle|\, P_{\mathrm{c}}\Delta_{\mathrm{c}}\|x_{\mathrm{c}}\|^{-\alpha} > \gamma_{\mu}\right) \\ =& \frac{F_{\mathrm{SINR}_{\mathrm{U,c}}}\left(2^{\hat{R}_{\mathrm{c}}} - 1\right)}{1 - \exp\left(-\pi\lambda_{\mathrm{CU}}\left(P_{\mathrm{c}}\Delta_{\mathrm{c}}\gamma_{\mu}^{-1}\right)^{2/\alpha}\right)}, \end{aligned} \tag{16}$$

where $\hat{R}_{\mathrm{c}}$ is the target channel capacity of a CU. $F_{\mathrm{SINR}_{\mathrm{U,c}}}(\gamma)$ is the CDF of the received SINR of the CU, and is derived as

$$\begin{aligned} & F_{\mathrm{SINR}_{\mathrm{U,c}}}(\gamma) \\ &= 1 - \int_0^{\left(\frac{P_{\mathrm{c}}\Delta_{\mathrm{c}}}{\gamma_{\mu}}\right)^{1/\alpha}} \mathbb{P}\left(h_{x_{\mathrm{c}},o} > \frac{\gamma I_{\mathrm{U,c}}}{P_{\mathrm{c}}x^{-\alpha}}\right) f_{\|x_{\mathrm{c}}\|}(x)\,\mathrm{d}x \\ &= 1 - \int_0^{\left(\frac{P_{\mathrm{c}}\Delta_{\mathrm{c}}}{\gamma_{\mu}}\right)^{1/\alpha}} \sum_{n=0}^{\Delta_{\mathrm{c}}-1} \frac{2\pi\lambda_{\mathrm{c}}}{n!}\left(\frac{\gamma}{P_{\mathrm{c}}}\right)^n \mathrm{e}^{-\sum\limits_{j=\mathrm{p,c}}\lambda_j\tilde{C}_{j,\mathrm{c}}^{\gamma}(\gamma\hat{P}_{j,\mathrm{c}})^{\frac{2}{\alpha}}x^2 - \pi\lambda_{\mathrm{c}}x^2} \\ &\quad \times \sum_{\bar{m}\in M(n)} C(\bar{m})x^{2\sum m_l} F_{\mathrm{c}}(\bar{m},\gamma)\mathrm{d}x, \end{aligned} \tag{17}$$

where $F_{\mathrm{c}}(\bar{m},\gamma) = \frac{\prod_{l=1}^{n}\left(\sum_{j=\mathrm{p,c}} D_{j,\mathrm{c}}^{\gamma}(l)P_j^{2/\alpha}\right)^{m_l}}{(\gamma P_{\mathrm{c}}^{-1})^{-\frac{2}{\alpha}\sum m_l + n}(2\pi)^{-\sum m_l}}$, $\tilde{C}_{j,\mathrm{c}}^{\gamma} = \frac{2\pi}{\alpha}\sum_{m=1}^{\Psi_j}\binom{\Psi_j}{m}B'(\Psi_j - m + \frac{2}{\alpha}, m - \frac{2}{\alpha}, u_{j,\mathrm{c}}^{\gamma})$, $D_{j,\mathrm{c}}^{\gamma}(l) = \frac{\lambda_j}{\alpha}\frac{(\Psi_j + l - 1)!B'(\Psi_j + \frac{2}{\alpha}, l - \frac{2}{\alpha}, u_{j,\mathrm{c}}^{\gamma})}{(\Psi_j - 1)!}$, and $u_{j,\mathrm{c}}^{\gamma} = (1 + \gamma/(\hat{\Delta}_{j,\mathrm{c}}\hat{B}_{j,\mathrm{c}}))^{-1}$. The derivation of (17) is similar to (12). From (17), we note that a connection outage of a CUN occurs only if $P_{\mathrm{c}}\Delta_{\mathrm{c}}\|x_{\mathrm{c}}\|^{-\alpha} > \gamma_{\mu}$ and no eavesdropper exists in the detection region of the served CFBS.

4.2 SOP in CUNs

In this subsection, we evaluate the SOP of the CUs under the assumption that the random distributed eavesdroppers are non-colluding. The definition of SOP is given in Subsection 3.2, and the SOP of the CUs is given in the following theorem.

Theorem 4. For a typical CU served by a CFBS, its SOP is derived as

$$\begin{aligned} P_{\mathrm{so,c}}\left(\hat{R}_{\mathrm{s,c}}\right) &= \mathbb{P}\left(\log_2\left(1+\mathrm{SINR}_{\mathrm{E,c}}\right) > \hat{R}_{\mathrm{c}} - \hat{R}_{\mathrm{s,c}} | \mu = 1\right) \\ &= 1 - \exp\left(\frac{-\lambda_{\mathrm{E}}\alpha\left(2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}\right)^{-(\Psi_{\mathrm{c}}-1)}}{A_{\mathrm{c}}\left(2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}-1\right)^{2/\alpha}} \exp\left(-\frac{\pi R_{\mu}^2}{\alpha}\left(2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}-1\right)^{\frac{2}{\alpha}} A_{\mathrm{c}}\right)\right), \end{aligned} \tag{18}$$

where $\hat{R}_{\mathrm{s,c}}$ is the target secrecy rate of $P_{\mathrm{so,c}}(\hat{R}_{\mathrm{s,c}})$ and $A_{\mathrm{c}} = 2\sum_{j=\mathrm{p,c}}\lambda_j \sum_{i=1}^{\Psi_j}\binom{\Psi_j}{i}\left(\frac{P_j}{P_{\mathrm{c}}}\right)^{2/\alpha} C_{\alpha,\Psi_j,i}$.

Proof. Please refer to Appendix C.

4.3 TSOP in CUNs

Similar to Subsection 3.3, we use the TSOP of the CUs to characterize the probability that either a connection outage or a secrecy outage occurs in a CUN, the expression of which is given in the following theorem.

Theorem 5. For a typical CU served by a CFBS, its TSOP is derived as

$$\begin{aligned} P_{\mathrm{tso,c}} =& 1 - \mathbb{P}\left(\log_2\left(1+\mathrm{SINR}_{\mathrm{U,c}}\right) > \hat{R}_{\mathrm{c}} \ \&\ \log_2\left(1+\mathrm{SINR}_{\mathrm{E,c}}\right) < \hat{R}_{\mathrm{c}} - \hat{R}_{\mathrm{s,c}} \ | \mu = 1\right) \\ =& 1 - \left(1 - P_{\mathrm{co,c}}\left(\hat{R}_{\mathrm{c}}\right)\right)\left(1 - P_{\mathrm{so,c}}\left(\hat{R}_{\mathrm{s,c}}\right)\right), \end{aligned} \tag{19}$$

where $P_{\mathrm{co,c}}(\cdot)$ and $P_{\mathrm{so,c}}(\cdot)$ are derived in (16) and (18), respectively.

Proof. Please refer to Appendix D.

5 Average secrecy throughput of CHCNs

In general, the average secrecy rate is the average of the instantaneous secrecy rate. As such, the average secrecy rate of a PU is given by [22]

$$\begin{aligned} \bar{R}_{\mathrm{s,p}} =& \int_0^{\infty}\int_0^{\infty} R_{\mathrm{s,p}} f_{\mathrm{SINR_{U,p}}}(x_1)\, f_{\mathrm{SINR_{E,p}}}(x_2)\,\mathrm{d}x_1\mathrm{d}x_2 \\ =& \frac{1}{\ln 2}\int_0^{\infty}\frac{F_{\mathrm{SINR_{E,p}}}(x_2)}{1+x_2}\left(1 - F_{\mathrm{SINR_{U,p}}}(x_2)\right)\mathrm{d}x_2, \end{aligned} \tag{20}$$

where $F_{\mathrm{SINR_{U,p}}}(\cdot)$ and $F_{\mathrm{SINR_{E,p}}}(\cdot)$ are given in (12) and (14). We note that the average secrecy rate of the CUs exists only if $\mu = 1$, and is computed as

$$\begin{aligned} \bar{R}_{\mathrm{s,c}} =& \int_0^{\infty}\int_0^{x_1}\left(\log_2(1+x_1) - \log_2(1+x_2)\right) f_{\mathrm{SINR_{U,c}}}(x_1\,|\mu=1)\, f_{\mathrm{SINR_{E,c}}}(x_2\,|\mu=1)\,\mathrm{d}x_2\mathrm{d}x_1 \\ =& \int_0^{\infty} F_{\mathrm{SINR_{U,c}}}(x_1\,|\mu=1)\left(-\frac{f_{\mathrm{SINR_{E,c}}}(x_1\,|\mu=1)}{(1+x_1)\ln 2} + \frac{F_{\mathrm{SINR_{E,c}}}(x_1\,|\mu=1)}{(1+x_1)^2\ln 2}\right)\mathrm{d}x_1, \end{aligned} \tag{21}$$

where

$$f_{\mathrm{SINR_{E,c}}}(\gamma\,|\mu=1) = \exp\left(\frac{-\lambda_{\mathrm{E}}\alpha(\gamma+1)^{-(\Psi_{\mathrm{c}}-1)}}{A_{\mathrm{c}}\gamma^{2/\alpha}}\right)\frac{\lambda_{\mathrm{E}}(\gamma+1)^{-\Psi_{\mathrm{c}}}}{A_{\mathrm{c}}\gamma^{2/\alpha}}\left((\Psi_{\mathrm{c}}-1)\alpha + 2\frac{\gamma+1}{\gamma}\right). \tag{22}$$

In addition, $F_{\mathrm{SINR_{U,c}}}(\gamma|\mu=1) = F_{\mathrm{SINR_{U,c}}}(2^{\hat{R}_{\mathrm{c}}}-1|P_{\mathrm{c}}\Delta_{\mathrm{c}}\|x_{\mathrm{c}}\|^{-\alpha} > \gamma_{\mu})$ and $F_{\mathrm{SINR_{E,c}}}(x_1|\mu=1)$ are given in (17) and (C2), respectively.

As mentioned in [7], the secrecy throughput for the network is defined as the product of the BS density, secrecy rate, COP, and SOP. Mathematically, the average secrecy throughput of a CHCN is given by

$$\bar{T}_{\mathrm{CHCN}} = \bar{T}_{\mathrm{s,p}} + \bar{T}_{\mathrm{s,c}}, \tag{23}$$

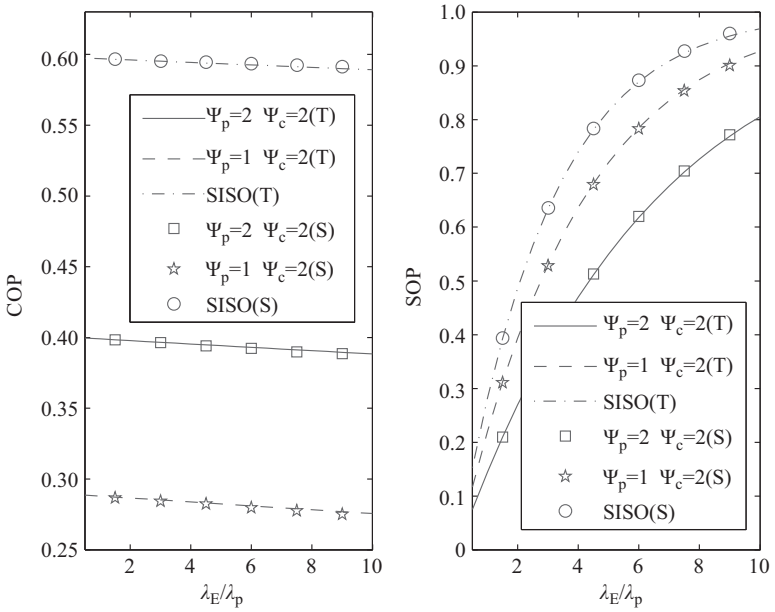

Figure 1 COP and SOP of PU vs. $\lambda_{\mathrm{E}}/\lambda_{\mathrm{p}}$.

where $\bar{T}_{\mathrm{s,p}}$ is the average secrecy throughput of a PUN, and $\bar{T}_{\mathrm{s,c}}$ is the average secrecy throughput of a CUN. To be more specific, $\bar{T}_{\mathrm{s,p}}$ can be written as

$$\bar{T}_{\mathrm{s,p}} = \lambda_{\mathrm{p}} \left(1 - P_{\mathrm{tso,p}}\right) \bar{R}_{\mathrm{s,p}}. \tag{24}$$

Then according to the fact that $\bar{T}_{\mathrm{s,c}}$ exists only when $\bar{R}_{\mathrm{s,c}}$ exists, the following can be derived

$$\bar{T}_{\mathrm{s,c}} = \lambda_{\mathrm{c}} P_{\mu=1} \left(1 - P_{\mathrm{tso,c}}\right) \bar{R}_{\mathrm{s,c}}. \tag{25}$$

Based on the results in (23)–(25), the average secrecy throughput of a CHCN under the secrecy transmission scheme is given as a function of γ_μ and R_μ, which is expressed as

$$\bar{T}_{\mathrm{CHCN}}\left(\gamma_\mu, R_\mu\right) = \bar{T}_{\mathrm{s,p}}\left(\gamma_\mu, R_\mu\right) + \bar{T}_{\mathrm{s,c}}\left(\gamma_\mu, R_\mu\right). \tag{26}$$

As a result, the threshold γ_μ and radius R_μ are the key elements of the average secrecy throughput of a CHCN, which will be shown in the simulation results in the next section.

6 Simulation results

In this section, the validity of the theoretical derivations is verified by analyzing both the theoretical and simulation results. In addition, all of the theoretical performance results are evaluated. First, the influence of the eavesdropper density, Ψ_{p} and Ψ_{c}, on the security and reliability are shown. We then present the effects of the detection region radius and the predetermined access threshold on the COP, SOP, and TSOP of a PU and a CU. Finally, we show the numerical results of the average secrecy throughput in a CHCN based on the detection region radius and predetermined access threshold. All simulation results shown in this section are averaged over 100000 Monte Carlo simulations. In the following results, we assume the following path loss exponent, $\alpha = 4$, $\lambda_{\mathrm{p}} = 10^{-4}$ m^{-2}, $\lambda_{\mathrm{c}} = 2 \times 10^{-4}$ m^{-2}, $P_{\mathrm{p}}/P_{\mathrm{c}} = 5$, $\Delta_{\mathrm{p}} = 4$, $\Delta_{\mathrm{c}} = 2$ (for a single-input single-output (SISO) system, $\Delta_{\mathrm{p}} = 1$, $\Delta_{\mathrm{c}} = 1$), and $\lambda_{\mathrm{CU}} = 2 \times 10^{-3}$ m^{-2}.

In Figures 1 and 2, the impacts caused by the density of the eavesdroppers, Ψ_{p} and Ψ_{c}, on both the reliability and security of a PUN and a CUN are evaluated, respectively. Figure 1 plots the COP and SOP of a PU versus $\lambda_{\mathrm{E}}/\lambda_{\mathrm{p}}$ for the different Ψ_{p} given in Figure 1, in which $\gamma_\mu = -45$ dBm, $R_\mu = 5$ m, $\hat{R}_{\mathrm{p}} = 1$ bits/s/Hz, $\hat{R}_{\mathrm{s,p}} = 0.5$ bits/s/Hz, T denotes the theoretical results, and S denotes the simulation results. It is clear that the SOP of a PU ascends with λ_{E}, whereas the COP of a PU descends with

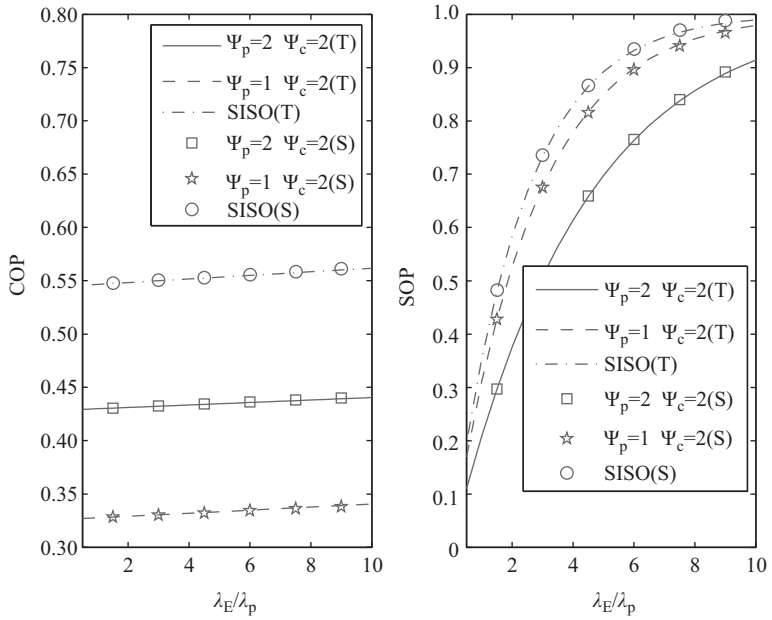

Figure 2 COP and SOP of CU vs. λ_E/λ_p.

λ_E. Furthermore, the COP of a PU ascends with Ψ_p, and the SOP of a PU descends with Ψ_p. This is because the increase in λ_E reduces the received inter-cell interference of the PUs and eavesdroppers by decreasing the number of active CFBSs, and improves the average distance between the eavesdroppers and served PBS. The increased number of resource block of a PBS not only increases the received intra-cell interference of the eavesdroppers, but also increases interference of the CUs from the PBS, and decreases the activation probability of the CFBS. This implies that the increased number of PUs has an influence on the reliability and security of a PUN.

Figure 2 plots the COP and SOP of a CU versus λ_E/λ_p with different Ψ_c under the condition that the served BS is active, in which $\hat{R}_c = 0.6$ bits/s/Hz, $\hat{R}_{s,c} = 0.3$ bits/s/Hz, and the other parameters are the same as those used in the simulations shown in Figure 1. It can be observed that the SOP of the CU increases as λ_E increases. Another fact clearly shown from Figure 2 is that the COP of the CU increases very slowly and remains nearly constant with λ_E. This is due to the fact that increasing λ_E decreases the activation probability of the CFBSs, and improves the average distance between the eavesdroppers and served CFBS. We note that the influence caused by Ψ_c on the security in a CUN is similar with that caused by Ψ_p on the security in a PUN. From Figures 1 and 2, we can clearly observe that a multi-antenna system performs better than a SISO system in improving both the security and reliability.

For more comprehensive insight into the performance of a PUN, the COP and SOP of a PU versus the predetermined access threshold γ_μ and the radius R_μ of the detection region are evaluated and presented in Figures 3 and 4, with $\Psi_p = 1$, $\Psi_c = 1$, $\lambda_E = 2\times10^{-4}$ m^{-2}, $\hat{R}_p = 2.5$ bits/s/Hz, and $\hat{R}_{s,p} = 1$ bits/s/Hz. We note that the COP of a PU decreases with an increase in γ_μ and R_μ when the COP is larger than zero. However, the SOP of a PU is completely the opposite, and increases with R_μ and γ_μ, which implies an existing tradeoff between the SOP and COP of a PU. Obviously, R_μ and γ_μ affect the active CFBSs, which in turn generates interference to the PBSs. However, increasing γ_μ and decreasing R_μ can reduce the interference from the CFBSs to the PUs and the eavesdroppers. To describe the joint performance of security and reliability in a PUN, the TSOP of a PU is shown in Figure 5. As expected, by optimizing R_μ and γ_μ, we can reach a tradeoff between security and reliability of a PU. Moreover, the minimum TSOP of a PU with the optimal pair of $(\gamma_\mu, R_\mu) = (-30, 25)$ is given in Figure 5.

From (16) and (18), we know that both the COP and SOP of a CU are correlated with the predetermined access threshold γ_μ and the radius R_μ of the detection region under the condition that the served BS is active. This can be explained using the results in Figures 6 and 7, which show the COP and SOP of a CU versus γ_μ and R_μ. The results presented here are all for a CUN with $\Psi_p = 1$, $\Psi_c = 1$,

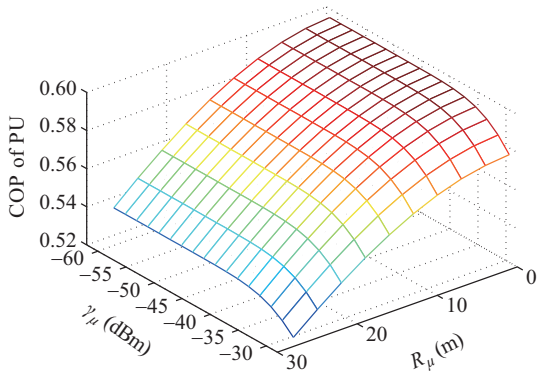

Figure 3 (Color online) COP of PU vs. γ_μ and R_μ.

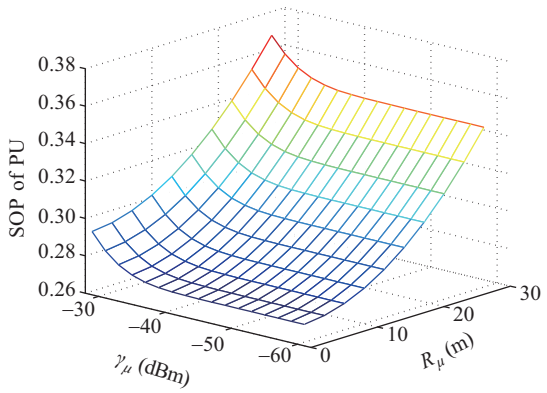

Figure 4 (Color online) SOP of PU vs. γ_μ and R_μ.

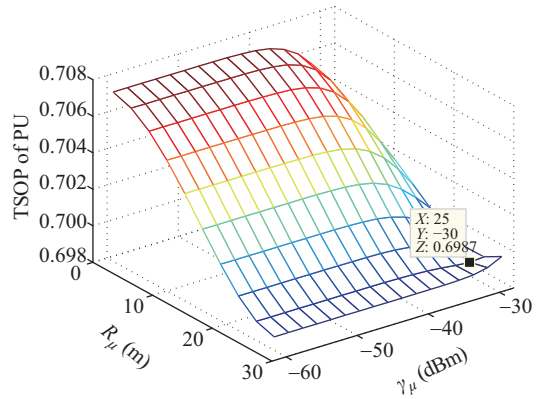

Figure 5 (Color online) TSOP of PU vs. γ_μ and R_μ.

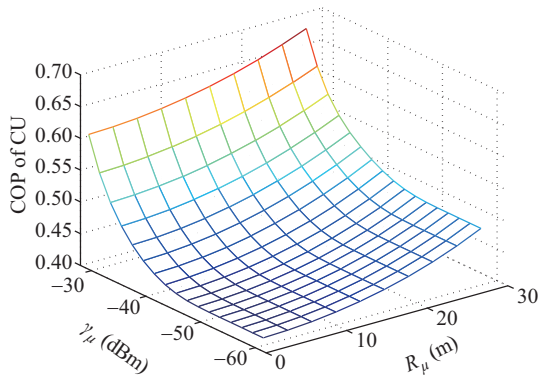

Figure 6 (Color online) COP of CU vs. γ_μ and R_μ.

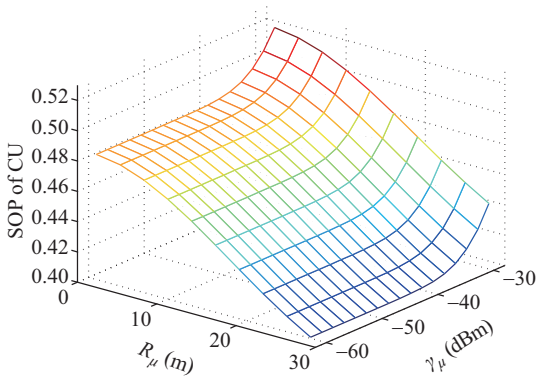

Figure 7 (Color online) SOP of CU vs. γ_μ and R_μ.

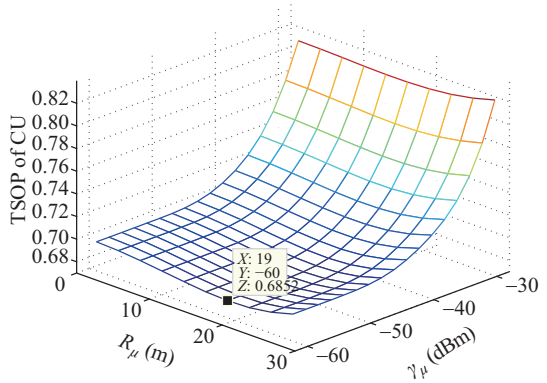

Figure 8 (Color online) TSOP of CU vs. γ_μ and R_μ.

$\lambda_{\rm E} = 2 \times 10^{-4}$ m^{-2}, $\hat{R}_{\rm c} = 1$ bits/s/Hz, and $\hat{R}_{\rm s,c} = 0.5$ bits/s/Hz. It can be readily seen that the COP of a CU increases with both γ_μ and R_μ, and the SOP of a CU decreases with both γ_μ and R_μ. Furthermore, the increase in γ_μ reduces the activation probability of a CFBS with low reliability, and the increase in R_μ reduces the activation probability of a CFBS with low security. Hence, by optimizing R_μ and γ_μ, we can reach a tradeoff between security and reliability of a CU. To describe the joint performance of security and reliability in a CUN, the TSOP of a CU is shown in Figure 8, where the minimum value for a given network with the optimal pair of $(\gamma_\mu, R_\mu) = (-60, 19)$ is given.

For the next simulations, Figure 9 illustrates the effect caused by R_μ and γ_μ on the average secrecy

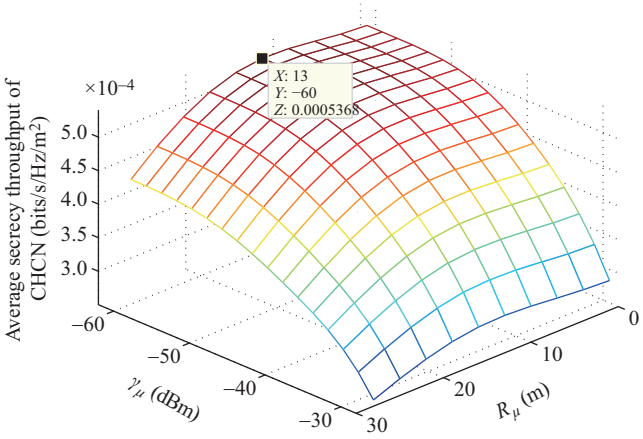

Figure 9 (Color online) Average secrecy throughput of CHCN vs. γ_μ and R_μ.

throughput of a CHCN. From (26), we note that the average secrecy throughput of a CHCN is not a monotonous function of R_μ and γ_μ. Consequently, the optimal value of the CHCN can be obtained through the proper design of R_μ and γ_μ. Here, the same parameters as those in Figures 6–8 are used. In addition, the average secrecy throughput of a multi-antenna CHCN, shown in Figure 9, reaches the maximum value for a given network with the optimal pair of $(\gamma_\mu, R_\mu) = (-60, 13)$, as indicated in Figure 9. At around this optimal average secrecy throughput, the TSOPs of a PU and CU are also quite low.

7 Conclusion

In this paper, we studied the PLS of a downlink underlay CHCN, where the locations of the network nodes were characterized through independent HPPPs. To ensure the reliability and security of a CHCN, both multi-antenna technology and a secrecy transmission scheme were employed. We first described a two-tiered CHCN model under the secrecy transmission scheme, and derived the PDF of the indicator function and the activation probability of a CFBS. We then analyzed the security, reliability, and joint performance of the security and reliability of a CHCN by deriving the COP, SOP, and TSOP of the PUs and CUs under the secrecy transmission scheme. Finally, the exact expression for the average secrecy throughput of a CHCN was obtained, which can achieve the optimal value through the design of a predetermined access threshold and based on the radius of the detection region. The simulation results indicate that the reliability and security of a CHCN can be improved using multi-antenna technology and a secure transmission scheme.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61401510, 61379006, 61601514, 61521003), National High Technology Research and Development Program of China (863) (Grant No. 2015AA01A708).

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

References

1 Li B, Fei Z S, Chen H. Robust artificial noise-aided secure beamforming in wireless-powered non-regenerative relay. IEEE Access, 2016, 4: 7921–7929
2 Yang N, Wang L, Geraci G, et al. Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun Mag, 2015, 53: 20–27
3 Li B, Fei Z S. Probabilistic-constrained robust secure transmission for energy harvesting over MISO channels. Sci China Inf Sci, 2018, 61: 022303
4 Andrews J, Claussen H, Dohler M, et al. Femtocells: past, present, and future. IEEE J Sel Areas Commun, 2012, 30: 497–508
5 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

6 Zou Y, Yao Y D, Zheng B. Cooperative relay techniques for cognitive radio systems: spectrum sensing and secondary user transmissions. IEEE Commun Mag, 2012, 50: 98–503
7 Xu X, He B, Yang W, et al. Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers. IEEE Trans Inf Forensic Secur, 2015, 11: 373–387
8 Zou Y, Zhu J, Yang L, et al. Securing physical-layer communications for cognitive radio networks. IEEE Commun Mag, 2015, 53: 48–54
9 Li B, Fei Z S. Robust beamforming and cooperative jamming for secure transmission in DF relay systems. EURASIP J Wirel Commun Netw, 2016, 68: 1–11
10 Li X Y, Jin L, Huang K Z, et al. Transmission frequency-band hidden technology in physical layer security. Sci China Inf Sci, 2016, 59: 019301
11 Gong S Q, Xing C W, Fei Z S, et al. Cooperative beamforming design for physical-layer security of multi-hop MIMO communications. Sci China Inf Sci, 2016, 59: 062304
12 Zhong B, Wu M G, Li T, et al. Physical layer security via maximal ratio combining and relay selection over Rayleigh fading channels. Sci China Inf Sci, 2016, 59: 062305
13 Zou Y, Champagne B, Zhu W P, et al. Relay-selection improves the security-reliability trade-off in cognitive radio systems. IEEE Trans Commun, 2015, 63: 215–228
14 Mokari N, Parsaeefard S, Saeedi H, et al. Secure robust ergodic uplink resource allocation in relay-assisted cognitive radio networks. IEEE Trans Signal Proc, 2015, 63: 291–304
15 Wang C, Wang H M. On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels. IEEE Trans Inf Forensic Secur, 2014, 9: 1814–1827
16 Zou Y, Wang X, Shen W. Physical-layer security with multiuser scheduling in cognitive radio networks. IEEE Trans Commun, 2013, 61: 5103–5113
17 Zheng T X, Wang H M, Yuan J, et al. Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers. IEEE Trans Commun, 2015, 63: 4347–4362
18 Wang C, Wang H M, Xia X G, et al. Uncoordinated jammer selection for securing SIMOME wiretap channels: a stochastic geometry approach. IEEE Trans Wirel Commun, 2015, 14: 2596–2612
19 Wang H M, Wang C, Zheng T X, et al. Impact of artificial noise on cellular networks: a stochastic geometry approach. IEEE Trans Wirel Commun, 2016, 15: 7390–7404
20 Wang H M, Zheng T X, Yuan J, et al. Physical layer security in heterogeneous cellular networks. IEEE Trans Commun, 2016, 64: 1204–1219
21 Shu Z H, Yang Y Q, Qian Y, et al. Impact of interference on secrecy capacity in a cognitive radio network. In: Proceedings of IEEE Global Telecommunications Conference, Kathmandu, 2011
22 Deng Y, Wang L, Zaidi S A R, et al. Artificial-noise aided secure transmission in large scale spectrum sharing networks. IEEE Trans Commun, 2016, 64: 2116–2129
23 Xu X, Yang W, Cai Y, et al. On the secure spectral-energy efficiency tradeoff in random cognitive radio networks. IEEE J Sel Areas Commun, 2016, 34: 2706–2722
24 Panahi F H, Ohtsuki T. Stochastic geometry based analytical modeling of cognitive heterogeneous cellular networks. In: Proceedings of IEEE International Conference on Communications, Sydney, 2014. 5281–5286
25 Blaszczyszyn B, Karray M K, Keeler H P. Using poisson processes to model lattice cellular networks. In: Proceedings of IEEE INFOCOM, Turin, 2013. 773–781
26 Taylor D B, Dhillon H S, Novlan T D, et al. Pairwise interaction processes for modeling cellular network topology. In: Proceedings of IEEE Global Communications Conference, Anaheim, 2012. 4524–4529
27 Dhillon H S, Ganti R K, Baccelli F, et al. Modeling and analysis of K-tier downlink heterogeneous cellular networks. IEEE J Sel Areas Commun, 2012, 30: 550–560
28 Deng Y S, Wang L F, Wong K K, et al. Safeguarding massive MIMO aided hetnets using physical layer security. In: Proceedings of IEEE International Conference on Wireless Communications & Signal Processing, Nanjing, 2015. 1–5
29 Wang H, Zhou X, Reed M C. Physical layer security in cellular networks: a stochastic geometry approach. IEEE Trans Wirel Commun, 2013, 12: 2776–2787
30 Wu H, Tao X, Li N, et al. Secrecy outage probability in multi-RAT heterogeneous networks. IEEE Commun Lett, 2016, 20: 53–56
31 Gupta A K, Dhillon H S, Vishwanath S, et al. Downlink coverage probability in MIMO HetNets with flexible cell selection. In: Proceedings of IEEE Global Communications Conference, Austin, 2014. 1534–1539

Appendix A

The activation probability of the CFBS is derived by

$$\begin{aligned} P_{\mathrm{c\_act}} &= \left[1-\mathrm{E}_{\Phi_{\mathrm{CU}}}\left[\prod_{x_{\mathrm{CU}}\in\Phi_{\mathrm{CU}}}\mathbb{P}\left(x_{\mathrm{CU}}\text{ is not associated with }B_{\mathrm{c}}\right)\right]\right]\mathbb{P}\left(\text{No eavesdropper within detection region}\right)\\ &= \left[1-\mathrm{E}_{\Phi_{\mathrm{CU}}}\left[\prod_{x_{\mathrm{CU}}\in\Phi_{\mathrm{CU}}}\mathbb{P}\left(P_{\mathrm{c}}\Delta_{\mathrm{c}}\|x_{x_{\mathrm{CU}},B_{\mathrm{c}}}\|^{-\alpha}<\max_{x_{\mathrm{c}}\in\Phi_{\mathrm{c}}\setminus B_{\mathrm{c}}}P_{\mathrm{c}}\Delta_{\mathrm{c}}\|x_{\mathrm{c},x_{\mathrm{CU}}}\|^{-\alpha}\right)\right]\right]\mathrm{e}^{-\pi\lambda_{\mathrm{E}}R_{\mu}^{2}}\end{aligned}$$

$$\overset{(b)}{=}\left[1-\mathrm{E}_{\Phi_{\mathrm{CU}}}\left[\prod_{x_{\mathrm{CU}}\in\Phi_{\mathrm{CU}}}\left(1-\mathrm{e}^{-\pi\bar{\lambda}_{\mathrm{c}}\left\|x_{x_{\mathrm{CU}},B_{\mathrm{c}}}\right\|^{2}}\right)\right]\right]\mathrm{e}^{-\pi\lambda_{\mathrm{E}}R_{\mu}^{2}}$$
$$\overset{(c)}{=}\left[1-\exp\left[-\lambda_{\mathrm{CU}}\bar{\lambda}_{\mathrm{c}}^{-1}\left(1-\mathrm{e}^{-\pi\bar{\lambda}_{\mathrm{c}}\left(P_{\mathrm{c}}\Delta_{\mathrm{c}}\gamma_{\mu}^{-1}\right)^{2/\alpha}}\right)\right]\right]\mathrm{e}^{-\pi\lambda_{\mathrm{E}}R_{\mu}^{2}}, \tag{A1}$$

where $\mathbb{P}\{\text{No eavesdropper within detection region}\}$ is given in (7), $\|x_{x_{\mathrm{CU}},B_{\mathrm{c}}}\|=\|x_{\mathrm{CU}}-B_{\mathrm{c}}\|$, $\|x_{\mathrm{c},x_{\mathrm{CU}}}\|=\|x_{\mathrm{CU}}-x_{\mathrm{c}}\|$, the derivation of step (b) is given in [20], and step (c) is obtained based on the probability generating functional lemma (PGFL) over HPPP Φ_{E} [22].

Appendix B

The SOP of PU is derived as

$$P_{\mathrm{so,p}}\left(\hat{R}_{\mathrm{s,p}}\right)=1-F_{\mathrm{SINR_{E,p}}}\left(2^{\hat{R}_{\mathrm{p}}-\hat{R}_{\mathrm{s,p}}}-1\right)=1-\exp\left(\frac{-\lambda_{\mathrm{E}}\alpha\left(2^{\hat{R}_{\mathrm{p}}-\hat{R}_{\mathrm{s,p}}}\right)^{-(\Psi_{\mathrm{p}}-1)}}{A_{\mathrm{p}}\left(2^{\hat{R}_{\mathrm{p}}-\hat{R}_{\mathrm{s,p}}}+1\right)^{2/\alpha}}\right). \tag{B1}$$

Then, the CDF of $\mathrm{SINR_{E,p}}$ is derived as

$$F_{\mathrm{SINR_{E,p}}}(\gamma)\overset{(d)}{=}\mathrm{E}_{\Phi_{\mathrm{E}}}\left[\prod_{e\in\Phi_{\mathrm{E}}}\left[1-\mathrm{E}\left[\exp\left(\frac{\gamma I_{\mathrm{E},p}}{P_{\mathrm{p}}\|x_{e,\mathrm{p}}-e\|^{-\alpha}}\right)\right]\right]\right]$$
$$\overset{(e)}{=}\exp\left(-2\pi\lambda_{\mathrm{E}}\int_{0}^{\infty}L_{I_{\mathrm{p,p}}^{\mathrm{E,intra}}}(s)\,L_{I_{\mathrm{p,p}}^{\mathrm{E,inter}}+I_{\mathrm{c,p}}^{\mathrm{E}}}(s)\,x\mathrm{d}x\right), \tag{B2}$$

where step (d) is derived by the PDF of $h_{e,\mathrm{p}}$ with $h_{e,\mathrm{p}}\sim\exp(1)$, and step (e) is achieved based on the PGFL over PPP Φ_{E} [22]. Additionally, the Laplace transform of $I_{\mathrm{p,p}}^{\mathrm{E,intra}}$ and $I_{\mathrm{p,p}}^{\mathrm{E,inter}}+I_{\mathrm{c,p}}^{\mathrm{E}}$ can be given by

$$L_{I_{\mathrm{p,p}}^{\mathrm{E,intra}}}(s)=\mathrm{E}\left[\exp\left(-\frac{\gamma I_{\mathrm{p,p}}^{\mathrm{E,intra}}x^{\alpha}}{P_{\mathrm{p}}}\right)\right]=(\gamma+1)^{-(\Psi_{\mathrm{p}}-1)}, \tag{B3}$$

and

$$L_{I_{\mathrm{p,p}}^{\mathrm{E,inter}}+I_{\mathrm{c,p}}^{\mathrm{E}}}(s)=\mathrm{E}\left[\exp\left(-\frac{\gamma\left(I_{\mathrm{p,p}}^{\mathrm{E,inter}}+I_{\mathrm{c,p}}^{\mathrm{E}}\right)x^{\alpha}}{P_{\mathrm{p}}}\right)\right]=\exp\left(-\frac{\pi x^{2}A_{\mathrm{p}}}{\alpha\gamma^{-2/\alpha}}\right). \tag{B4}$$

Eq. (B4) is achieved from the PGFL over PPP Φ_{c} and the result of (3.241) [1)] . Substituting (B3) and (B4) into (B2), we obtain step (g). Moreover, we can derive the PDF of $\mathrm{SINR_{E,p}}$ as follows:

$$f_{\mathrm{SINR_{E,p}}}(\gamma)=\exp\left(\frac{-\lambda_{\mathrm{E}}\alpha(\gamma+1)^{-(\Psi_{\mathrm{p}}-1)}}{A_{\mathrm{p}}\gamma^{2/\alpha}}\right)\left((\Psi_{\mathrm{p}}-1)\frac{\lambda_{\mathrm{E}}\alpha(\gamma+1)^{-\Psi_{\mathrm{p}}}}{A_{\mathrm{p}}\gamma^{2/\alpha}}+\frac{2\lambda_{\mathrm{E}}(\gamma+1)^{-(\Psi_{\mathrm{p}}-1)}}{A_{\mathrm{p}}}\gamma^{-2/\alpha-1}\right). \tag{B5}$$

Appendix C

The SOP in a CUN is derived as

$$P_{\mathrm{so,c}}\left(\hat{R}_{\mathrm{s,c}}\right)=\mathbb{P}\left(\log_{2}\left(1+\mathrm{SINR_{E,c}}\right)>\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}\,|\mu=1\right)$$
$$=1-\mathrm{E}_{\Phi_{\mathrm{E}}}\left[\prod_{e\in\Phi_{\mathrm{E}}}\mathbb{P}\left(\frac{P_{c}h_{e,\mathrm{c}}\|x_{e,\mathrm{c}}\|^{-\alpha}}{I_{\mathrm{c,c}}^{\mathrm{E,intra}}+I_{\mathrm{c,c}}^{\mathrm{E,inter}}+I_{\mathrm{p,c}}^{\mathrm{E}}}\leqslant 2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}-1\,|\|x_{e,\mathrm{c}}\|>R_{\mu}\right)\right]$$
$$=1-F_{\mathrm{SINR_{E,c}}}\left(2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}-1\,|\|x_{e,\mathrm{c}}\|>R_{\mu}\right), \tag{C1}$$

where $F_{\mathrm{SINR_{E,c}}}(\gamma\,|\|x_{e,\mathrm{c}}\|>R_{\mu})=F_{\mathrm{SINR_{E,c}}}(\gamma\,|\mu=1)$ is the CDF of $\mathrm{SINR_{E,c}}$ under the condition of $\mu=1$, and its detailed derivation process is given by

$$F_{\mathrm{SINR_{E,c}}}(\gamma\,|\mu=1)=\exp\left(-2\pi\lambda_{\mathrm{E}}\int_{R_{\mu}}^{\infty}\left(1-\mathbb{P}\left(h_{e,\mathrm{c}}\leqslant\frac{I_{\mathrm{c,c}}^{\mathrm{E,intra}}+I_{\mathrm{c,c}}^{\mathrm{E,inter}}+I_{\mathrm{p,c}}^{\mathrm{E}}}{P_{c}\gamma^{-1}x^{-\alpha}}\right)\right)x\mathrm{d}x\right)$$
$$=\exp\left(-2\pi\lambda_{\mathrm{E}}\int_{R_{\mu}}^{\infty}L_{I_{\mathrm{c,c}}^{\mathrm{E,intra}}}(s)\,L_{I_{\mathrm{c,c}}^{\mathrm{E,inter}}+I_{\mathrm{p,c}}^{\mathrm{E}}}(s)\,x\mathrm{d}x\right)$$
$$=\exp\left(\frac{-\lambda_{\mathrm{E}}\alpha(\gamma+1)^{-(\Psi_{\mathrm{c}}-1)}}{A_{\mathrm{c}}\gamma^{2/\alpha}}\exp\left(-\frac{\pi R_{\mu}^{2}A_{\mathrm{c}}}{\alpha\gamma^{-2/\alpha}}\right)\right), \tag{C2}$$

1) Gradshteyn I S, Ryzhik I M. Table of Integrals, Series and Products. 7th ed. San Diego: Academic Press, 2007. 322–323.

where

$$L_{I_{\mathrm{c,c}}^{\mathrm{E,intra}}}(s)=\mathrm{E}\left[\exp\left(-\frac{\gamma I_{\mathrm{c,c}}^{\mathrm{E,intra}}x^{\alpha}}{P_{\mathrm{c}}}\right)\right]=(\gamma+1)^{-(\Psi_{\mathrm{c}}-1)} \tag{C3}$$

and

$$L_{I_{\mathrm{c,c}}^{\mathrm{E,inter}}+I_{\mathrm{p,c}}^{\mathrm{E}}}(s)=\mathrm{E}\left[\exp\left(-\frac{\gamma\left(I_{\mathrm{c,c}}^{\mathrm{E,inter}}+I_{\mathrm{p,c}}^{\mathrm{E}}\right)x^{\alpha}}{P_{\mathrm{c}}}\right)\right]=\exp\left(\frac{-\lambda_{\mathrm{E}}\alpha}{A_{\mathrm{c}}\gamma^{2/\alpha}}\exp\left(-\frac{\pi R_{\mu}^{2}A_{\mathrm{c}}}{\alpha\gamma^{-2/\alpha}}\right)\right). \tag{C4}$$

Appendix D

The expression of TSOP in a CUN is derived as follows:

$$\begin{aligned}
P_{\mathrm{tso,c}}=&1-\mathbb{P}\left(\log_2\left(1+\mathrm{SINR}_{\mathrm{U,c}}\right)>\hat{R}_{\mathrm{c}}\ \&\ \log_2\left(1+\mathrm{SINR}_{\mathrm{E,c}}\right)<\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}\ |\mu=1\right)\\
=&1-\mathbb{P}\left(\mathrm{SINR}_{\mathrm{U,c}}>2^{\hat{R}_{\mathrm{c}}}-1,\|x_{\mathrm{c}}\|<\left(P_{\mathrm{c}}\Delta_{\mathrm{c}}\gamma_{\mu}^{-1}\right)^{1/\alpha},\mathrm{SINR}_{\mathrm{E,c}}<2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}-1,\|x_{e,\mathrm{c}}\|>R_{\mu}\right)/P_{\mu=1}\\
=&1-\left(1-F_{\mathrm{SINR}_{\mathrm{U,c}}}\left(2^{\hat{R}_{\mathrm{c}}}-1\left|P_{\mathrm{c}}\Delta_{\mathrm{c}}\|x_{\mathrm{c}}\|^{-\alpha}>\gamma_{\mu}\right.\right)\right)F_{\mathrm{SINR}_{\mathrm{E,c}}}\left(2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}-1\,|\|x_{e,\mathrm{c}}\|>R_{\mu}\right)\\
=&1-\left(1-P_{\mathrm{co,c}}\left(\hat{R}_{\mathrm{c}}\right)\right)\left(1-P_{\mathrm{so,c}}\left(\hat{R}_{\mathrm{s,c}}\right)\right),
\end{aligned} \tag{D1}$$

where $F_{\mathrm{SINR}_{\mathrm{U,c}}}(2^{\hat{R}_{\mathrm{c}}}-1|P_{\mathrm{c}}\Delta_{\mathrm{c}}\|x_{\mathrm{c}}\|^{-\alpha}>\gamma_{\mu})$ and $F_{\mathrm{SINR}_{\mathrm{E,c}}}(2^{\hat{R}_{\mathrm{c}}-\hat{R}_{\mathrm{s,c}}}-1|\|x_{e,\mathrm{c}}\|>R_{\mu})$ are derived in (17) and (C2), respectively.