IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 3, 2018, accepted June 27, 2018, date of publication July 3, 2018, date of current version July 25, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2852628

Towards Secure and Energy-Efficient CRNs Via Embracing Interference: A Stochastic Geometry Approach

XIAOYING LIU[1], KECHEN ZHENG[2], XIAO-YANG LIU[3], (Member, IEEE), XINBING WANG[4], (Senior Member, IEEE), AND GUOJUN DAI[1], (Member, IEEE)

[1]School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou 310018, China
[2]School of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China
[3]Department of Electrical Engineering, Columbia University, New York, NY 10027, USA
[4]Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

Corresponding author: Xinbing Wang (xwang8@sjtu.edu.cn)

This work was supported by the NSF China under Grant 61532012, Grant 61325012, Grant 61521062, Grant 61602303, and Grant 61428205.

ABSTRACT In a cognitive radio network (CRN), the interference caused by secondary users (SUs) is conventionally regarded as an obstacle to the throughput of the primary network. However, when considering security, the interference brings potential benefits to the secrecy throughput of the primary network. For a stand-alone primary network, the secrecy guard zone, including the cooperative mode and non-cooperative mode, has been shown as an efficient method to enhance the network security. The cooperative mode is traditionally thought to outperform the non-cooperative mode due to the jamming effect of the artificial noise generated by primary transmitters on eavesdroppers. However, allowing SUs to access the licensed spectrum, the resulting interference can be used as a source of the artificial noise instead of that generated on purpose by primary transmitters, which in return benefits the energy efficiency of the primary network. Inspired by the two benefits brought by SUs, this paper considers a random underlay CRN with eavesdroppers overhearing primary transmissions. To enhance both the security and energy efficiency of the primary network, we apply a secrecy guard zone around each primary transmitter, and adopt the non-cooperative mode. We exploit the stochastic geometry to model such a random CRN and analyze the connection/secrecy probability of primary links. We propose a criterion for guaranteeing the performance of secure primary network. The main idea is that compared with the primary network with the cooperative mode, the access of SUs should not reduce the secrecy throughput and energy efficiency of the primary network with the non-cooperative mode. Based on the obtained analytical results, we design the optimal secondary link scheduling schemes under the criterion. Both analytical and numerical results show that the interference from SUs can be exploited toward a secure and energy-efficient primary network and provide SUs with extra transmission opportunities.

INDEX TERMS Cognitive radio networks, underlay spectrum sharing, secrecy guard zone, secrecy throughput, energy efficiency, stochastic geometry.

I. INTRODUCTION

The conflicts between spectrum scarcity and spectrum under-utilization have fueled the recent upsurge of wireless cognitive radios (CRs), which are pioneered by Mitola [1] to promote the spectrum utilization. Consequently, CRs, together with the introduction of secondary spectrum licensing, have spawned the appearance of cognitive radio networks (CRNs), where unlicensed secondary users (SUs) employ cognitive abilities, such as spectrum sensing and adaptive communications, to access the spectrum of licensed primary users (PUs) without interfering primary transmissions. Traditionally, the access paradigm is classified into two categories [2], [3]: overlay and underlay. In overlay paradigm, SUs sense the spectrum holes that are not occupied by PUs and then transmit via the spectrum holes; Whereas in underlay paradigm, SUs access the spectrum of licensed PUs as long as the interference from SUs is under an acceptable level at primary receivers.

Nevertheless, allowing SUs to share the licensed spectrum with PUs makes wireless transmissions vulnerable to

security attacks [4] due to the open spectrum characteristic of CRNs and the broadcast characteristic of wireless channels, which creates more opportunities for malicious nodes to listen/analyze the transmitted information. Typical security attacks at the physical layer include PU emulation [5], jamming attacks [6], and eavesdropping [7], [8]. Here we concentrate on the eavesdropping attack targeted at primary transmissions, for the reason that eavesdroppers are more interested in the information of PUs than that of SUs [9]. To protect the confidential message transmission against eavesdropping, information-theoretic secrecy, employing the randomness of channel codewords, has been extensively studied. As a crucial metric of secure communication systems, secrecy throughput refers to the rate of information that is reliably and securely transmitted between legitimate source and destination. The secrecy throughput has been widely investigated at the information-theoretic aspect of CRNs in the context of game theory [10], mutiuser scheduling [11], and relay selection [12].

Many advanced techniques have been developed to enhance the network security, and in particular, the secrecy guard zone, applied around each legitimate transmitter, has been proven to achieve a significant improvement on secrecy throughput [13]. The mode with secrecy guard zone includes cooperative one and non-cooperative one. Moreover, the cooperative mode outperforms the non-cooperative mode for networks with high security requirement in terms of secrecy throughput [13]. Xu *et al.* [14] employed the cooperative mode with secrecy guard zone for secondary transmitters to achieve secure communication. Xu *et al.* [15] analyzed the secure spectral spectrum and energy efficiency of the secondary network by the cooperative mode with secrecy guard zone.

Compared to the systems without the security concern, transmitters need to consume more energy to achieve the same throughput due to the eavesdropping attack [16]. Therefore, along with throughput, energy efficiency is another vital performance for secure CRNs [17]–[22]. El-Halabi *et al.* [17] defined secure energy efficiency as the ratio of secrecy throughput to the consumed total power. Garbry *et al.* [18] adjusted the optimal power allocation at the secondary transmitter to maximize the energy efficiency of the secondary network. Wu and Chen [19] minimized the transmission power at the secondary transmitter under the eavesdropping rate constraint. Liu *et al.* [20] studied the tradeoff between secrecy throughput and energy efficiency in CRNs.

However, the majority of aforementioned works concentrate on the performance of the secondary network, and meanwhile the interference caused by SUs is considered to be harmful for the primary network. As a network comprised of licensed PUs, the performance of the primary network should be preferentially guaranteed. In addition, from the aspect of security, the interference from SUs may bring potential benefits to the primary network [23], [24]. We consider a large-scale underlay CRN with eavesdroppers overhearing primary transmissions. Different from [23] generating the interference in a positive way by the optimal design of a beamformer at the secondary transmitter with multiple antennas, and [24] utilizing the artificial noise generated on purpose by secondary transmitter and receiver in turn to improve the security of the primary network, we consider that all the nodes are equipped with single antenna, and utilize the interference from the secondary transmission to enhance the security of the primary network without the extra artificial noise. Specifically, to ensure the security of the primary network, we apply a secrecy guard zone around each primary transmitter, and adopt the non-cooperative mode: Confidential message transmissions take place only if no eavesdroppers are detected inside the corresponding secrecy guard zone, and the primary transmitter keeps silent otherwise. For a stand-alone primary network, the secrecy throughput of the primary network with the cooperative mode outperforms that of the primary network with the non-cooperative mode [13]. However, in contrast with the non-cooperative mode, the primary transmitter consumes part of its energy to generate the artificial noise if eavesdroppers are detected inside the secrecy guard zone. Inspired by this, compared to the primary network with the cooperative mode, allowing SUs to access the licensed spectrum improves the secrecy throughput and energy efficiency of the primary network with the non-cooperative mode, by controlling the number of SUs accessing the licensed spectrum and the SUs' transmission power. In this respect, the interference from SUs can be exploited to achieve the secure and energy-efficient primary network, and meanwhile provide SUs with extra transmission opportunities.

In practical CRNs, the locations and the number of users often change dynamically due to mobility and random access mechanism [15], [25], [26]. Stochastic geometry is a powerful mathematical and statistical tool to deal with the random nature of wireless networks, and authors in [27]–[29] studied the secure multi-antenna transmission under a stochastic geometry framework. In contrast with the previous works, we consider a more complete and complex scenario where a large-scale CRN, consisting of a primary network modeled as a Poisson point process (PPP) and a secondary network modeled as a PPP, is overheard by randomly distributed eavesdroppers modeled as a PPP, and study the impact of secondary communications on secure primary communications. The analysis of such a complete and complex scenario is more challenging than that of large-scale CRNs without eavesdroppers [30], large-scale ad hoc network with eavesdroppers [31] and small-scale CRNs with eavesdroppers [14].

The main contributions are summarized as follows:

- We provide a tractable analytical framework for a large-scale underlay CRN in the presence of eavesdroppers by stochastic geometry. Then we derive the general expressions for the connection/secrecy probability of primary links, and the connection probability of secondary links. Based on the obtained probabilities, we analyze the secrecy throughput and energy efficiency of primary network. We find that the scheduling scheme of secondary

links (i.e., the intensity and transmit power of secondary transmitters) can be fully exploited to improve the secrecy throughput and energy efficiency of primary network.

- We propose the performance guarantee criterion for the primary network. The main idea is that compared to the primary network with the cooperative mode, the access of SUs should not reduce the secrecy throughput and energy efficiency of the primary network with the non-cooperative mode. Then we explore the feasible region of secondary link scheduling that satisfies the criterion. Besides, we design optimal scheduling schemes of secondary links within the feasible region to maximize the secrecy throughput of the primary network and the throughput of the secondary network, respectively.
- Numerical results verify that the scheme, that maximizes the throughput of the secondary network under the optimal secrecy throughput of the primary network, achieves the optimal performance for the primary network; The scheme, that maximizes the throughput of the secondary network under the performance guarantee criterion for the primary network, provides a higher throughput performance level for the secondary network. Moreover, numerical results show that the throughput of the secondary network increases with the intensity of eavesdroppers.

The rest of this paper is organized as follows. Section II introduces the system model. Section III derives the connection probability and secrecy probability of primary links, and the connection probability of secondary links. Section IV designs the optimal scheduling schemes of secondary links with respect to the performance guarantee criterion for the primary network. Section V provides numerical results and discussions. Section VI concludes this paper.

II. SYSTEM MODEL

We first elaborate on the network model, followed by the introduction of secrecy coding. Then we describe the secrecy guard zone for primary transmitters, and define two performance metrics, i.e., secrecy throughput and energy efficiency.

A. NETWORK MODEL

We consider a secure CRN consisting of primary links, secondary links, and a set of eavesdroppers that overhear primary transmissions[1] over a large two-dimensional space, as shown in Fig. 1. The secondary network accesses the licensed spectrum by underlay paradigm. The primary transmitters are spatially distributed as a homogeneous PPP Φ_P with intensity λ_P, and the secondary transmitters are spatially distributed as another independent homogeneous PPP Φ_S with intensity λ_S. We consider the scenario where each transmitter has a unique associated receiver, and the set of receivers is disjoint with

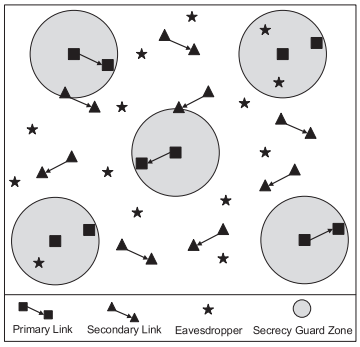

FIGURE 1. Network model.

that of transmitters. Besides, the distance between a transmitter and the associated receiver is fixed as [32]–[34]. Hence the primary receivers (secondary receivers) are also spatially distributed as a PPP with intensity λ_P (λ_S). The transmit power of each primary transmitter is P_P, and that of each secondary transmitter is P_S. We assume that each primary receiver is located at a distance r_P away from the associated primary transmitter, and each secondary receiver is located at a distance r_S away from the associated secondary transmitter.

The locations of eavesdroppers follow an independent homogeneous PPP Φ_E with intensity λ_E. We assume the intensity of eavesdroppers is given like many recent works studying the secure random networks [14], [15], [35]. This assumption allows a quantitative study on the impacts of eavesdroppers on the secure performance in random networks. The primary links are exposed to all the eavesdroppers, which do not collude with each other.[2] Hence eavesdroppers have to decode confidential messages individually, and the secrecy data rate of the primary link is determined by the most detrimental eavesdropper.

We adopt a unified channel model that comprises Rayleigh fading and standard path loss for primary, secondary and eavesdropper links [36]. Specifically, given the transmit power P_i at transmitter S_i, the received power P_{ij} at receiver D_j is expressed as

$$P_{ij} = P_i h_{ij}^2 r_{ij}^{-\alpha} = P_i H_{ij} r_{ij}^{-\alpha}, \quad r_{ij} > 1,$$

where r_{ij} denotes the distance between S_i and D_j. $\alpha > 2$ is the path loss exponent. h_{ij} is the fading channel gain between S_i and D_j, and follows a Rayleigh distribution. H_{ij} is the fading factor, and follows an exponential distribution with unit mean, i.e., $H_{ij} \sim \exp(1)$, where $\exp(1)$ denotes the exponential distribution with mean 1. For analysis purpose, we concentrate on the *interference-limited* CRN, where the effect of additive white Gaussian noise (AWGN) on receivers could be negligible. Also, we consider that the perfect channel state information (CSI) and channel distribution information (CDI), are available at the receiver side, while the

[1] We mainly investigate the effects of the secondary interference on the primary communication from the perspective of secrecy. The secrecy of the secondary communication is beyond the scope of this paper.

[2] The analysis of non-colluding eavesdroppers could be extended to that of colluding eavesdroppers, since multiple eavesdroppers can be regarded as a single eavesdropper with multiple distributed antennas.

feedback from the receiver side to the transmitter side is not available. Besides, the CSI and CDI of eavesdroppers are not available to legitimate users due to the passive eavesdropping mode.

B. SECRECY CODING

As for the security concern, we adopt the well-known Wyner codes [37] at primary transmitters for message transmissions against eavesdropping. To be specific, two kinds of rates, namely, the rate of transmitted codewords Q_{tp} and the rate of confidential messages Q_{mp} are taken into consideration with $Q_{mp} < Q_{tp}$. The difference $Q_{ep} = Q_{tp} - Q_{mp}$ is provided for secure primary transmissions against eavesdropping. All the primary transmitters have the same Q_{tp} and Q_{mp} since fixed-rate transmissions are often adopted in practice to reduce the complexity of systems.

Clearly, the successful primary transmission embodies that both the connection and secrecy performance of the primary link are achieved.

1) *Connection*: If the rate of transmitted codewords Q_{tp} is smaller than the capacity of the primary link, the received signal at the primary receiver can be decoded with an arbitrarily small error. Hence the reliable primary transmission can be achieved.
2) *Secrecy*: If the rate redundancy $Q_{ep} = Q_{tp} - Q_{mp}$ is greater than the capacity of the corresponding eavesdropped link, the received signal at eavesdroppers can not be decoded with transmitted messages. Hence the secure transmission of the primary link can be achieved.

For the secondary network, we assume that the secondary transmitters have the same transmission rate, denoted by Q_{ts}. Since we consider the scenario where eavesdroppers are not interested in secondary transmissions, the successful transmission of a secondary link implies that the connection of the secondary link is achieved.

C. SECRECY GUARD ZONE

As for the mechanism of secrecy guard zone [13]–[15], [38], we model the finite region around each primary transmitter as a secrecy guard zone, which is centered at a primary transmitter with radius D. For each primary transmitter, we adopt the *non-cooperative mode* [13]: each primary transmitter is allowed to transmit confidential messages only when no eavesdroppers are located inside the secrecy guard zone, and the primary transmitter keeps silent when eavesdroppers are found inside the secrecy guard zone. With the consideration of the secrecy guard zone, the set of active primary transmitter locations, denoted by Φ'_P, has the intensity of

$$\lambda'_P = \lambda_P \cdot p_t, \tag{1}$$

where

$$p_t = e^{-\pi \lambda_E D^2}. \tag{2}$$

Here p_t represents the probability that no eavesdroppers are located inside the secrecy guard zone of an arbitrary primary transmitter. Actually, with the secrecy guard zone, the distribution of the active primary transmitters does not follow a homogeneous PPP. In [38], Hasan and Andrews applied standard Possion tests to show that from the perspective of a receiver at position o, the distribution of the active transmitters can be well-approximated by a homogeneous PPP outside $\mathcal{B}(o, D)$, which represents a disk of radius D centered at position o. Based on this result, we employ two approximations: First, from the perspective of eavesdropper at position z, the distribution of active primary transmitters $\Phi_{P'}$ follows a homogeneous PPP with intensity λ'_P outside $\mathcal{B}(z, D)$. Second, from the perspective of each primary receiver, the distribution of active primary transmitters $\Phi_{P'}$ follows a homogeneous PPP with intensity λ'_P.

D. PERFORMANCE METRICS

We introduce two performance metrics, i.e., secrecy throughout and energy efficiency. The successful primary transmission embodies that both connection and secrecy of the primary link are achieved, hence we introduce the connection probability and secrecy probability of the primary link at first.

1) CONNECTION PROBABILITY

The reliability performance is measured by the connection probability. The connection probability quantifies the probability that the received signal at the primary receiver side can be decoded with an arbitrarily small error. The connection probabilities of an arbitrary primary link and an arbitrary secondary link are expressed as

$$p_{cp} = \mathbb{P}\big(\log_2(1+\gamma_P) > Q_{tp}\big) = \mathbb{P}(\gamma_P > \beta_{cp}), \tag{3}$$

and

$$p_{cs} = \mathbb{P}\big(\log_2(1+\gamma_S) > Q_{ts}\big) = \mathbb{P}(\gamma_S > \beta_{cs}), \tag{4}$$

respectively, where $\beta_{cp} = 2^{Q_{tp}} - 1$ and $\beta_{cs} = 2^{Q_{ts}} - 1$. In addition, γ_P denotes the signal-to-interference ratio (SIR) of an arbitrary primary link, and γ_S denotes the SIR of an arbitrary secondary link.

2) SECRECY PROBABILITY

The secrecy performance is measured by the secrecy probability. The secrecy probability quantifies the probability that the received signal at the eavesdropper can not be decoded with transmitted messages. The secrecy probability of an arbitrary primary link is given by

$$\begin{aligned} p_{sp} &= \mathbb{P}\big(\max_{z\in\Phi_E} \log_2(1+\gamma_E(z)) < Q_{tp} - Q_{mp}\big) \\ &= \mathbb{P}(\max_{e\in\Phi_E} \gamma_E(z) < \beta_{sp}), \end{aligned} \tag{5}$$

where $\beta_{sp} = 2^{Q_{tp}-Q_{mp}} - 1$, and $\gamma_E(z)$ denotes the SIR received by the eavesdropper at z.

Based on definitions of the connection probability and secrecy probability, we introduce definitions of secrecy throughput and energy efficiency, respectively.

Definition 1 (Secrecy Throughput): Given rate Q_{mp} of the confidential message, secrecy throughput is defined as the number of the confidential message bits that are reliably and securely transmitted per second from all the active primary transmitters to the associated primary receivers. Formally, the secrecy throughput is expressed as

$$C_P = Q_{mp}\lambda'_P \cdot p_{cp}p_{sp} \quad (bps). \tag{6}$$

Remark 1: When the transmit power of each primary transmitter is fixed, the connection probability and secrecy probability are independent [13]–[15], [39].

Definition 2 (Energy Efficiency): Energy efficiency is defined as the number of the confidential message bits that are reliably and securely transmitted per Joule from all the active primary transmitters to the associated primary receivers. Formally, the energy efficiency is expressed as

$$\eta_P = \frac{Q_{mp}\lambda'_P \cdot p_{cp}p_{sp}}{p_t\lambda_P P_P} \quad (bpJ), \tag{7}$$

where p_t represents the probability that the primary transmitter is active as shown in (2).

Remark 2: We focus on the power consumption consumed by primary transmitters, regardless of the circuit power consumption, static power consumption, and the radiated power.

III. PERFORMANCE ANALYSIS

We first derive the SIR distribution of typical links in the secure CRN. Then we obtain the connection/secrecy probability of primary links, and the connection probability of secondary links. Finally, we propose the performance guarantee criterion for the primary network.

A. CONNECTION PROBABILITY OF PRIMARY LINKS

We conduct analysis on a typical primary link that consists of a typical primary transmitter at x and a typical primary receiver at y. Let r_{xy} denote the distance between x and y, and H_{xy} denote the fading factor of the typical primary link with $H_{xy} \sim \exp(1)$. Then the SIR received by the typical primary receiver at y from the associated primary transmitter at x is expressed as

$$\gamma_P(y) = \frac{P_P H_{xy} r_{xy}^{-\alpha}}{I_{pp} + I_{sp}}, \tag{8}$$

where

$$I_{pp} = \sum_{p_i \in \Phi_{P'} \setminus \{x\}} P_P H_{p_iy} r_{p_iy}^{-\alpha}, \tag{9}$$

and

$$I_{sp} = \sum_{s_j \in \Phi_S} P_S H_{s_jy} r_{s_jy}^{-\alpha}. \tag{10}$$

Here I_{pp} is the cumulative interference from the other active primary transmitters that are located at p_i with fading factor H_{p_iy}, and I_{sp} is the cumulative interference from the other active secondary transmitters that are located at s_j with fading factor H_{s_jy}.

Based on the SIR of the typical primary link in (8) and the definition of the connection probability in (3), we derive the connection probability of a typical primary link for a given r_P by the following theorem.

Theorem 1: In the limited-interference CRN, the connection probability of a typical primary link is

$$p_{cp} = \exp\left\{-\pi(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{cp}^{\frac{2}{\alpha}} r_P^2 \lambda'_P \left(1+\left(\frac{P_S}{P_P}\right)^{\frac{2}{\alpha}} \frac{\lambda_S}{\lambda'_P}\right)\right\}. \tag{11}$$

Proof: The connection probability of a typical primary link is expressed as

$$\begin{aligned}
p_{cp} &= \mathbb{P}\big(\gamma_P(y) > \beta_{cp}\big) \\
&= \mathbb{E}_{\Phi_{P'}}\left\{\mathbb{E}_{\Phi_S}\left\{\mathbb{P}\big(\gamma_P(y) > \beta_{cp} | \Phi_{P'}, \Phi_S\big)\right\}\right\} \\
&= \mathbb{E}_{\Phi_{P'}}\left\{\mathbb{E}_{\Phi_S}\left\{\mathbb{P}\left(H_{xy} > \frac{\beta_{cp}(I_{pp}+I_{sp})}{P_P r_{xy}^{-\alpha}} \middle| \Phi_{P'}, \Phi_S\right)\right\}\right\} \\
&\overset{(a)}{=} \mathbb{E}_{I_{pp}+I_{sp}}\left[e^{-\beta_{cp}P_P^{-1}r_{xy}^{\alpha}(I_{pp}+I_{sp})}\right] \\
&= \mathbb{E}_{I_{pp}}\left[e^{-\beta_{cp}P_P^{-1}r_{xy}^{\alpha}I_{pp}}\right] \cdot \mathbb{E}_{I_{sp}}\left[e^{-\beta_{cp}P_P^{-1}r_{xy}^{\alpha}I_{sp}}\right] \\
&\overset{(b)}{=} \mathcal{L}_{I_{pp}}\big(\beta_{cp}P_P^{-1}r_{xy}^{\alpha}\big) \cdot \mathcal{L}_{I_{sp}}\big(\beta_{cp}P_P^{-1}r_{xy}^{\alpha}\big).
\end{aligned} \tag{12}$$

The derivation of (a) follows from the Rayleigh distribution of channel fading. In (b), $\mathcal{L}_{I_{pp}}(\cdot)$ represents the Laplace transform of I_{pp}. In order to obtain p_{cp}, we derive the product of $\mathcal{L}_{I_{pp}}(s) \cdot \mathcal{L}_{I_{sp}}(s)$. According to (9), the Laplace transform of I_{pp} is given by

$$\begin{aligned}
\mathcal{L}_{I_{pp}}(s) &\overset{(c)}{=} \mathbb{E}_{\Phi_{P'}}\Big[\prod_{p_i \in \Phi_{P'}} \mathbb{E}_{H_{p_iy}}\big[e^{-sP_P H_{p_iy} r_{p_iy}^{-\alpha}}\big]\Big] \\
&\overset{(d)}{=} \exp\left\{-\lambda'_P \int_{\mathbb{R}^2} \big(1 - \mathbb{E}_{H_{p_iy}}\big[e^{-sP_P H_{p_iy} r^{-\alpha}}\big]\big) dr\right\} \\
&\overset{(e)}{=} \exp\left\{-2\pi\lambda'_P \int_{r=0}^{\infty} \big(1 - \mathbb{E}_{H_{p_iy}}\big[e^{-sP_P H_{p_iy} r^{-\alpha}}\big]\big) r dr\right\} \\
&\overset{(f)}{=} \exp\left\{-2\pi\lambda'_P \int_{r=0}^{\infty} \frac{sP_P r^{-\alpha} r}{1 + sP_P r^{-\alpha}} dr\right\} \\
&\overset{(g)}{=} \exp\left\{\lambda'_P \pi (sP_P)^{\frac{2}{\alpha}} \Gamma\big(1 - \frac{2}{\alpha}\big)\Gamma\big(1 + \frac{2}{\alpha}\big)\right\} \\
&\overset{(h)}{=} \exp\left\{-(\mathrm{sinc}^{-1}\frac{2}{\alpha})\lambda'_P \pi (sP_P)^{\frac{2}{\alpha}}\right\}.
\end{aligned} \tag{13}$$

Note that (c) is obtained due to the Slivnyak Theorem of PPP [40]. (d) follows from the probability generating functional of PPP [40], which is given by

$$\mathbb{E}\Big[\prod_{x \in \Phi} f(x)\Big] = \exp\left\{-\lambda \int_{\mathbb{R}^2} (1 - f(x)) dx\right\}. \tag{14}$$

(e) is obtained due to the double integral in polar coordinates. (f) follows from the Rayleigh distribution of channel fading. In (g), $\Gamma(\cdot)$ denotes the gamma function as $\Gamma(x) = \int_0^{\infty} t^{x-1}e^{-t}$. (h) is obtained due to the property of gamma function: for $x \in (0, 1)$, $\Gamma(1+x) = x\Gamma(x)$ and $\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin \pi x}$ are established. Hence we have $\Gamma(1+x)\Gamma(1-x) = \frac{\pi x}{\sin \pi x} = \mathrm{sinc}^{-1}x$.

Similar to the argument in (13), we have the Laplace transform of I_{sp} as

$$\mathcal{L}_{I_{sp}}(s) = \exp\Big\{ -(\mathrm{sinc}^{-1}\frac{2}{\alpha})\lambda_S \pi (sP_S)^{\frac{2}{\alpha}} \Big\}. \quad (15)$$

By substituting (13) and (15) into (12), and substituting r_P for r_{xy}, we complete the proof. ■

B. SECRECY PROBABILITY OF PRIMARY LINKS

Here we derive the secrecy probability of the typical primary link that consists of a typical primary transmitter at x and a typical primary receiver at y. For a eavesdropper at z, r_{xz} denotes the distance between x and z, and H_{xz} denotes the fading factor of this eavesdropping link with $H_{xz} \sim \exp(1)$. Accordingly, the SIR received by the eavesdropper at z from the typical primary transmitter at x is expressed as

$$\gamma_E(z) = \frac{P_P H_{xz} r_{xz}^{-\alpha}}{I_{pz} + I_{sz}}, \quad (16)$$

where

$$I_{pz} = \sum_{p_i \in \Phi_{P'} \setminus \{x\}} P_P H_{p_i z} r_{p_i z}^{-\alpha}, \quad (17)$$

and

$$I_{sz} = \sum_{s_j \in \Phi_S} P_S H_{s_j z} r_{s_j z}^{-\alpha}. \quad (18)$$

Here I_{pz} is the cumulative interference from the other active primary transmitters that are located at p_i with fading factor $H_{p_i z}$, and I_{sz} is the cumulative interference from the other active secondary transmitters that are located at s_j with fading factor $H_{s_j z}$.

According to the SIR of the typical eavesdropping link in (16) and the definition of the secrecy probability in (5), we derive the secrecy probability of a typical primary link for a given r_P as follows.

Theorem 2: In the limited-interference CRN, the secrecy probability of a typical primary link is

$$p_{sp} = \exp\left\{ -\frac{\lambda_E e^{-D^2 \pi (\mathrm{sinc}^{-1}\frac{2}{\alpha}) \beta_{sp}^{\frac{2}{\alpha}} \lambda'_P \left(1 + \left(\frac{P_S}{P_P}\right)^{\frac{2}{\alpha}} \frac{\lambda_S}{\lambda'_P}\right)}}{(\mathrm{sinc}^{-1}\frac{2}{\alpha}) \beta_{sp}^{\frac{2}{\alpha}} \lambda'_P \left(1 + \left(\frac{P_S}{P_P}\right)^{\frac{2}{\alpha}} \frac{\lambda_S}{\lambda'_P}\right)} \right\}. \quad (19)$$

Proof: Since we consider the scenario where the non-colluding eavesdroppers intend to overhear the primary transmission, the secure transmission of a primary link is determined by the most detrimental eavesdropper. Therefore, the secrecy probability of a typical primary link is

$$\begin{aligned}
p_{sp} &= \mathbb{P}\big(\max_{z \in \Phi_E} \gamma_E(z) < \beta_{sp} \big) \\
&= \mathbb{E}_{\Phi_E}\Big\{ \mathbb{E}_{\Phi_{P'}}\Big\{ \mathbb{E}_{\Phi_S}\Big\{ \mathbb{P}\big(\max_{z \in \Phi_E} \gamma_E(z) < \beta_{sp} | \Phi_{P'}, \Phi_S, \Phi_E \big) \Big\} \Big\} \Big\} \\
&= \mathbb{E}_{\Phi_E, \Phi_{P'}, \Phi_S}\Big\{ \prod_{z \in \Phi_E \setminus \mathcal{B}(z,D)} \mathbb{P}\big(\gamma_E(z) < \beta_{sp} \big) \Big\} \\
&\overset{(a)}{=} \mathbb{E}_{\Phi_E}\Big\{ \prod_{z \in \Phi_E \setminus \mathcal{B}(z,D)} \big(1 - \mathbb{E}_{I_{pz}+I_{sz}}\big[e^{-\beta_{sp} P_P^{-1} r_{xz}^{\alpha} (I_{pz}+I_{sz})} \big] \big) \Big\} \\
&= \mathbb{E}_{\Phi_E}\Big\{ \prod_{z \in \Phi_E \setminus \mathcal{B}(z,D)} \big(1 - \mathcal{L}_{I_{pz}+I_{sz}}\big(\beta_{sp} P_P^{-1} r_{xz}^{\alpha} \big) \big) \Big\} \\
&\overset{(b)}{=} \exp\Big\{ -\lambda_E \int_{\mathbb{R}^2 \setminus \mathcal{B}(z,D)} \mathcal{L}_{I_{pz}+I_{sz}}\big(\beta_{sp} P_P^{-1} r_{xz}^{\alpha} \big) dr_{xz} \Big\} \\
&\overset{(c)}{=} \exp\Big\{ -2\pi\lambda_E \int_D^{\infty} \mathcal{L}_{I_{pz}+I_{sz}}\big(\beta_{sp} P_P^{-1} r_{xz}^{\alpha} \big) r_{xz} dr_{xz} \Big\}. \quad (20)
\end{aligned}$$

In (20), (a) follows from the Rayleigh distribution of channel fading. (b) is obtained by the probability generating functional of PPP as shown in (14). (c) follows from the double integral in polar coordinates, and the lower limit of integral is due to the secrecy guard zone.

Similar to the argument in (12), we have

$$\begin{aligned}
&\mathcal{L}_{I_{pz}+I_{sz}}\big(\beta_{sp} P_P^{-1} r_{xz}^{\alpha} \big) \\
&= \mathcal{L}_{I_{pz}}\big(\beta_{sp} P_P^{-1} r_{xz}^{\alpha} \big) \cdot \mathcal{L}_{I_{pz}}\big(\beta_{sp} P_P^{-1} r_{xz}^{\alpha} \big) \\
&= \exp\Big\{ -\pi (\mathrm{sinc}^{-1}\frac{2}{\alpha}) \beta_{sp}^{\frac{2}{\alpha}} r_{xz}^2 \Big(\lambda'_P + \Big(\frac{P_S}{P_P} \Big)^{\frac{2}{\alpha}} \lambda_S \Big) \Big\}. \quad (21)
\end{aligned}$$

By substituting (21) into (20), we have

$$p_{sp} = \exp\Big\{ -\frac{\pi \lambda_E e^{-D^2 \theta}}{\theta} \Big\}, \quad (22)$$

where

$$\theta = \pi (\mathrm{sinc}^{-1}\frac{2}{\alpha}) \beta_{sp}^{\frac{2}{\alpha}} \Big(\lambda'_P + \Big(\frac{P_S}{P_P} \Big)^{\frac{2}{\alpha}} \lambda_S \Big). \quad (23)$$

This completes the proof. ■

C. CONNECTION PROBABILITY OF SECONDARY LINKS

For a typical secondary link consisting of a secondary transmitter at u and a secondary receiver at v, r_{uv} denotes the distance between u and v, and H_{uv} denotes the fading factor of the secondary link with $H_{uv} \sim \exp(1)$. Then the SIR received by the secondary receiver at v from the typical secondary transmitter at u is expressed as

$$\gamma_S(v) = \frac{P_S H_{uv} r_{uv}^{-\alpha}}{I_{ps} + I_{ss}}, \quad (24)$$

where

$$I_{ps} = \sum_{p_i \in \Phi_{P'}} P_P H_{p_i v} r_{p_i v}^{-\alpha}, \quad (25)$$

and

$$I_{ss} = \sum_{s_j \in \Phi_S / \{u\}} P_S H_{s_j v} r_{s_j v}^{-\alpha}. \quad (26)$$

Here I_{ps} is the cumulative interference from the other active primary transmitters that are located at p_i with fading factor $H_{p_i v}$, and I_{ss} is the cumulative interference from the other active secondary transmitters that are located at s_j with fading factor $H_{s_j v}$.

Based on the SIR of the typical secondary link in (24) and the definition of the connection probability in (4), we derive the connection probability of a typical secondary link for a given r_S by the following theorem.

Theorem 3: In the limited-interference CRN, the connection probability of a typical secondary link is

$$p_{cs}=\exp\left\{-\pi(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{cs}^{\frac{2}{\alpha}}r_S^2\left(\lambda_S+\left(\frac{P_P}{P_S}\right)^{\frac{2}{\alpha}}\lambda_P'\right)\right\}. \quad (27)$$

Proof: The proof is similar to that of Theorem 1. By substituting P_S, λ_S, P_P, λ_P, r_S, β_{cs} for P_P, λ_P, P_S, λ_S, r_P, β_{cp} in Theorem 1, the proof is completed. ■

D. PERFORMANCE GUARANTEE FOR PRIMARY NETWORK

In this paper, we employ the non-cooperative mode (NCM) for primary transmitters, i.e., the primary transmitter keeps silent when eavesdroppers are found inside the secrecy guard zone. However, Zhou *et.al* [13] indicated that for a single network, the cooperative mode (CM) for transmitters, i.e., the transmitter generates artificial noise when eavesdroppers are found inside the secrecy guard zone, outperforms the non-cooperative transmission mode for transmitters in terms of secrecy throughput. Contrary to a single network, we consider the coexistence of primary network and secondary network. The secondary transmissions, instead of the signals generated by primary transmitters, can be regarded as the artificial noise when eavesdroppers are found inside its secrecy guard zone. As a result, almost all the energy of the primary network is used for primary transmissions.

According to Theorems 2-3, by allowing SUs to access the licensed spectrum, the secrecy probability of primary links p_{sp} and the connection probability of secondary links p_{cs} can be improved. However, according to Theorem 1, the access of SUs would reduce the connection probability of primary links p_{cp}. Thus the secondary parameters, i.e., λ_S and P_S, should be carefully designed to enhance the performance of the secondary network, and meanwhile guarantee the performance of the primary network.

Based on the above considerations, we propose the following *performance guarantee criterion for the primary network*: Compared to the primary network with the cooperative mode, the access of SUs should not reduce the secrecy throughput and energy efficiency of the primary network with the non-cooperative mode.

1) For the secrecy throughput, the performance guarantee in (28) should be satisfied.

$$\begin{aligned} C_P &\geq C_P^{(0)}, \\ &\Longrightarrow Q_{mp}\lambda_P' p_{cp}p_{sp} \geq Q_{mp}\lambda_P' p_{cp}^{(0)}p_{sp}^{(0)}, \\ &\Longrightarrow p_{cp}p_{sp} \geq p_{cp}^{(0)}p_{sp}^{(0)}, \end{aligned} \quad (28)$$

where $C_P^{(0)}$ represents the secrecy throughput of the stand-alone primary network with the cooperative mode. $p_{cp}^{(0)}$ and $p_{sp}^{(0)}$ denote the connection probability and secrecy probability of primary links with the cooperative mode, respectively. Mathematically, they are given by

$$p_{cp}^{(0)}=\exp\left\{-\pi(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{cp}^{\frac{2}{\alpha}}r_P^2\lambda_P\right\}, \quad (29)$$

and

$$p_{sp}^{(0)}=\exp\left\{-\frac{\lambda_E e^{-D^2\pi(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{sp}^{\frac{2}{\alpha}}\lambda_P}}{(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{sp}^{\frac{2}{\alpha}}\lambda_P}\right\}. \quad (30)$$

2) For the energy efficiency, since

$$\eta_P=\frac{C_P}{p_t\lambda_P P_P}, \quad \text{and } \eta_P^{(0)}=\frac{C_P^{(0)}}{\lambda_P P_P}, \quad (31)$$

where $p_t=e^{-\pi\lambda_E D^2}$, we obtain

$$\frac{\eta_P}{\eta_P^{(0)}}=\frac{C_P}{C_P^{(0)}}\frac{1}{p_t}. \quad (32)$$

Since $0<p_t<1$, $C_P\geq C_P^{(0)}$ leads to $\eta_P>\eta_P^{(0)}$, and conversely, $\eta_P>\eta_P^{(0)}$ may not result in $C_P\geq C_P^{(0)}$. Namely, the improvement of the secrecy throughput is a sufficient but not necessary condition for the enhancement of the energy efficiency. However, this paper aimes at achieving the improvements of both the secrecy throughput and the energy efficiency of the primary network by exploiting the secondary interference. Therefore, in the following analysis, we focus on the secrecy throughput in (28), and denote S_p as $p_{cp}p_{sp}$ for simplicity.

IV. OPTIMAL SECONDARY LINK SCHEDULING UNDER GUARANTEE CRITERION FOR PRIMARY NETWORK

Based on the analytical results in Section III, we find that the intensity of secondary transmitters λ_S and the transmit power of secondary transmitters P_S play pivot roles in the secrecy throughput of the primary network. As such, we design the secondary link scheduling schemes, which determine the intensity and transmit power of secondary transmitters, under the performance guarantee criterion for the primary network. As the basis of the optimal secondary link scheduling schemes, the feasible region of secondary link scheduling for satisfying the proposed criterion is investigated at first.

A. FEASIBLE REGION OF SECONDARY LINK SCHEDULING

Here the feasible region refers to the secondary parameters (i.e., λ_S and P_S) that satisfy the performance guarantee criterion for the primary network. For the convenience of analysis, we let

$$a=\pi(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{cp}^{\frac{2}{\alpha}}r_P^2\lambda_P, \quad (33)$$

$$b=\pi(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{sp}^{\frac{2}{\alpha}}\lambda_P, \quad (34)$$

$$x=e^{-\lambda_E\pi D^2}\left(1+\left(\frac{P_S}{P_P}\right)^{\frac{2}{\alpha}}\frac{\lambda_S}{\lambda_P'}\right), \quad (35)$$

where $a>0$, $b>0$, $x>0$, and the factor of $(\frac{P_S}{P_P})^{\frac{2}{\alpha}}\frac{\lambda_S}{\lambda_P'}$ results from the access of SUs. Then S_p is expressed as

$$S_p(x)=p_{cp}p_{sp}=\exp\left\{-\left(ax+\pi\lambda_E\frac{e^{-D^2bx}}{bx}\right)\right\}. \quad (36)$$

Accordingly, we obtain

$$S_p(1) = p_{cp}^{(0)} p_{sp}^{(0)} = \exp\Big\{ -\Big(a + \pi\lambda_E \frac{e^{-D^2 b}}{b}\Big)\Big\}. \quad (37)$$

By comparing (28) with (36), we find that the performance guarantee criterion in (28) is equivalent to

$$S_p(x) \geq S_p(1). \quad (38)$$

Since $e^{-f(x)}$ is a monotone decreasing function of $f(x)$, (38) is equivalent to

$$f(x) \leq f(1), \quad (39)$$

where

$$f(x) = ax + \pi\lambda_E \frac{e^{-D^2 bx}}{bx}. \quad (40)$$

In the following, we compute x (i.e., λ_S and P_S) that satisfies (39). The following lemma lays the foundation for the feasible region.

Lemma 1: $f(x)$ is convex for $x \in (0, \infty)$, and attains the global minimum at

$$x^* = \frac{2}{D^2 b} W\left(\frac{D^2 b}{2}\sqrt{\frac{\pi\lambda_E(D^2 b+1)}{ab}}\right) \quad (41)$$

for $x \in (0, \infty)$, where $W(\cdot)$ is the inverse function of $g(W) = We^W$, and is called the Lambert-W function [41].

Proof: First, we prove that $f(x)$ is convex for $x \in (0, \infty)$. Evidently, $f(x)$ is a continuous function for $x \in (0, \infty)$, hence we investigate the monotonicity of $f(x)$ to testify the convexity. The first derivative of $f(x)$ is expressed as

$$\frac{df(x)}{dx} = a - \frac{\pi\lambda_E(D^2 b+1)}{b}\frac{e^{-D^2 bx}}{x^2}. \quad (42)$$

The second derivative of $f(x)$ is expressed as

$$\frac{d^2 f(x)}{dx^2} = \frac{\pi\lambda_E(D^2 b+1)}{b}\frac{(D^2 bx+2)e^{-D^2 bx}}{x^3}. \quad (43)$$

Due to $a > 0$, $b > 0$, and $x > 0$, $\frac{d^2 f(x)}{dx^2} > 0$ holds. Therefore, $f(x)$ is a convex function for $x \in (0, \infty)$.

Second, we compute the point of the minimum $f(x)$. We denote the stationary point of $f(x)$ by x^*, and we have

$$\frac{df(x)}{dx}\Big|_{x=x^*} = 0. \quad (44)$$

Since $f(x)$ is a convex function for $x \in (0, \infty)$, x^* is the point of the minimum $f(x)$. Based on (44), we obtain

$$\frac{\ln\sqrt{\frac{ab}{\pi\lambda_E(D^2 b+1)}}x}{\sqrt{\frac{ab}{\pi\lambda_E(D^2 b+1)}}x} = -\frac{D^2 b}{2}\sqrt{\frac{\pi\lambda_E(D^2 b+1)}{ab}}. \quad (45)$$

According to the property of Lambert-W function [41],

$$\frac{\ln z}{z} = -\tau \Longrightarrow z = e^{-W(\tau)}, \quad (46)$$

where $\tau > 0$. By combining (45) with (46), we have

$$\sqrt{\frac{ab}{\pi\lambda_E(D^2 b+1)}}x = \exp\left\{-W\Big(\frac{D^2 b}{2}\sqrt{\frac{\pi\lambda_E(D^2 b+1)}{ab}}\Big)\right\}. \quad (47)$$

Moreover, since

$$e^{-W(\tau)} = \frac{W(\tau)}{\tau}, \quad (48)$$

by combining (47) with (48), we obtain

$$x^* = \frac{2}{D^2 b} W\left(\frac{D^2 b}{2}\sqrt{\frac{\pi\lambda_E(D^2 b+1)}{ab}}\right). \quad (49)$$

This completes the proof. ■

Lemma 1 provides the value of x^*, hence according to the relation between x^* and 1, three cases should be considered: $x^* = 1$, $x^* < 1$, and $x^* > 1$. First of all, by letting $x^* = 1$, we derive the relation between the intensity of primary transmitters λ_P and that of eavesdroppers λ_E as

$$W\left(\frac{D^2 b}{2}\sqrt{\frac{\pi\lambda_E(D^2 b+1)}{ab}}\right) = \frac{D^2 b}{2} \quad (50)$$

$$\Longrightarrow \frac{D^2 b}{2} e^{\frac{D^2 b}{2}} = \frac{D^2 b}{2}\sqrt{\frac{\pi\lambda_E(D^2 b+1)}{ab}} \quad (51)$$

$$\Longrightarrow \lambda_E = \frac{abe^{D^2 b}}{\pi(D^2 b+1)}, \quad (52)$$

where (50) is obtained based on Lemma 1 and $x^* = 1$. (51) follows from the definition of Lambert-W function.

Based on (52), the following theorem reveals the feasible region of secondary link scheduling under the performance guarantee criterion proposed for the primary network in (28).

Theorem 4: The feasible region $\mathcal{F}$ constrained by the performance guarantee criterion is listed as follows.

(i) If $\lambda_E = \frac{abe^{D^2 b}}{\pi(D^2 b+1)}$, the feasible region $\mathcal{F}$ is

$$\lambda_S P_S^{\frac{2}{\alpha}} = 0, \text{ and primary transmitters adopt CM.} \quad (53)$$

(ii) If $0 < \lambda_E < \frac{abe^{D^2 b}}{\pi(D^2 b+1)}$, the feasible region $\mathcal{F}$ is

$$\lambda_S P_S^{\frac{2}{\alpha}} \geq \Big[\max\Big\{1, e^{\lambda_E \pi D^2} x_1\Big\} - 1\Big] e^{\lambda_E \pi D^2} \lambda_P P_P^{\frac{2}{\alpha}}, \quad (54)$$

$$\lambda_S P_S^{\frac{2}{\alpha}} \leq \Big[e^{\lambda_E \pi D^2} - 1\Big] e^{\lambda_E \pi D^2} \lambda_P P_P^{\frac{2}{\alpha}}. \quad (55)$$

(iii) If $\lambda_E > \frac{abe^{D^2 b}}{\pi(D^2 b+1)}$, the feasible region $\mathcal{F}$ is

$$\lambda_S P_S^{\frac{2}{\alpha}} \geq \Big[e^{\lambda_E \pi D^2} - 1\Big] e^{\lambda_E \pi D^2} \lambda_P P_P^{\frac{2}{\alpha}}, \quad (56)$$

$$\lambda_S P_S^{\frac{2}{\alpha}} \leq \Big[e^{\lambda_E \pi D^2} x_1 - 1\Big] e^{\lambda_E \pi D^2} \lambda_P P_P^{\frac{2}{\alpha}}. \quad (57)$$

where x_1 is the solution to $g(x_1)=0$ with $x_1 \neq 1$, and

$$g(x_1)=\pi\lambda_E e^{-D^2 b x_1}+abx_1^2-abx_1-\pi\lambda_E e^{-D^2 b}x_1. \tag{58}$$

Proof: Based on the relation between λ_E and $\frac{abe^{D^2b}}{\pi(D^2b+1)}$, i.e., x^* and 1, the proof consists of three cases as follows.

Case (i): $\lambda_E = \frac{abe^{D^2b}}{\pi(D^2b+1)}$, i.e., $x^*=1$. Since $f(1)$ is the minimum of $f(x)$ ($S_P(1)$ is the maximum of $S_P(x)$) for $x\in(0,\infty)$, the access of SUs would harm the original primary performance. Therefore, the best solution to the secrecy throughput is that primary transmitters adopt the cooperative mode without the access of SUs.

Case (ii): $0<\lambda_E<\frac{abe^{D^2b}}{\pi(D^2b+1)}$, i.e., $x^*<1$. Since $f(x)$ is a convex function for $x\in(0,\infty)$, and $x^*<1$, there exists a $x_1\in(0,x^*)$ satisfying $f(x_1)=f(1)$. Then we derive x_1 as

$$\begin{aligned} f(x_1) &= f(1) \\ &\Longrightarrow ax_1+\pi\lambda_E\frac{e^{-D^2bx_1}}{bx_1}=a+\pi\lambda_E\frac{e^{-D^2b}}{b} \\ &\Longrightarrow g(x_1)=0 \end{aligned} \tag{59}$$

where

$$g(x_1)=\pi\lambda_E e^{-D^2 b x_1}+abx_1^2-abx_1-\pi\lambda_E e^{-D^2 b}x_1. \tag{60}$$

x_1 is the solution to (59). Accordingly, $x_1\le x\le 1$ is the solution to $f(x)\le f(1)$ in (39), i.e.,

$$\lambda_S P_S^{\frac{2}{\alpha}} \ge \left[e^{\lambda_E\pi D^2}x_1-1\right]e^{\lambda_E\pi D^2}\lambda_P P_P^{\frac{2}{\alpha}}, \tag{61}$$

$$\lambda_S P_S^{\frac{2}{\alpha}} \le \left[e^{\lambda_E\pi D^2}-1\right]e^{\lambda_E\pi D^2}\lambda_P P_P^{\frac{2}{\alpha}}. \tag{62}$$

We set $\Delta=(e^{\lambda_E\pi D^2}x_1-1)$, and according to the relation between Δ and 0, we divide Case (ii) into two subcases as follows.

Case (ii-1): $\Delta<0$, λ_E is less than a certain value λ'_E which is the solution to $e^{\lambda'_E\pi D^2}x_1=1$. The solution to $f(x)\le f(1)$ in (39) is

$$0\le\lambda_S P_S^{\frac{2}{\alpha}} \le \left[e^{\lambda_E\pi D^2}-1\right]e^{\lambda_E\pi D^2}\lambda_P P_P^{\frac{2}{\alpha}}. \tag{63}$$

Case (ii-2): $\Delta\ge 0$, i.e., $\lambda_E\ge\lambda'_E$ and $\lambda_E<\frac{abe^{D^2b}}{\pi(D^2b+1)}$. The solution to $f(x)\le f(1)$ in (39) is

$$\lambda_S P_S^{\frac{2}{\alpha}} \ge \left[e^{\lambda_E\pi D^2}x_1-1\right]e^{\lambda_E\pi D^2}\lambda_P P_P^{\frac{2}{\alpha}}, \tag{64}$$

$$\lambda_S P_S^{\frac{2}{\alpha}} \le \left[e^{\lambda_E\pi D^2}-1\right]e^{\lambda_E\pi D^2}\lambda_P P_P^{\frac{2}{\alpha}}. \tag{65}$$

Combining the result of *Case (ii-1)* with that of *Case (ii-2)*, we get (54) and (55).

Case (iii): $\lambda_E>\frac{abe^{D^2b}}{\pi(D^2b+1)}$, i.e., $x^*>1$. Since $f(x)$ is a convex function for $x\in(0,\infty)$, and $x^*>1$, there exits a $x_2\in(x^*,\infty)$ satisfying $f(x_2)=f(1)$. The computation process to derive x_2 is the same with (59), and we have $x_2=x_1$. Hence $1\le x\le x_1$ is the solution to $f(x)\le f(1)$ in (39), i.e.,

$$\lambda_S P_S^{\frac{2}{\alpha}} \ge \left[e^{\lambda_E\pi D^2}-1\right]e^{\lambda_E\pi D^2}\lambda_P P_P^{\frac{2}{\alpha}}, \tag{66}$$

$$\lambda_S P_S^{\frac{2}{\alpha}} \le \left[e^{\lambda_E\pi D^2}x_1-1\right]e^{\lambda_E\pi D^2}\lambda_P P_P^{\frac{2}{\alpha}}. \tag{67}$$

By uniting the results of the above three cases, we complete the proof. ■

Remark 3: From Theorem 4, we get indications as follows:

- When $\lambda_E=\frac{abe^{D^2b}}{\pi(D^2b+1)}$, the primary transmitters adopting the cooperative mode without the access of SUs is the best way for the secrecy throughput of primary network, and the access of secondary network would not be beneficial to the primary network.
- When the intensity of eavesdroppers is very small, i.e., $\lambda_E<\lambda'_E$, the artificial noise conducted by primary transmitters has a critical interfering effect on primary links. Hence instead of the artificial noise conducted by primary transmitters, as long as $\lambda_S P_S^{\frac{2}{\alpha}}$ is below a threshold in (55), the access of the secondary network is beneficial to the primary network in terms of the secrecy throughput and energy efficiency.
- When the intensity of eavesdroppers is moderate, i.e., $\lambda'_E\le\lambda_E<\frac{abe^{D^2b}}{\pi(D^2b+1)}$, the artificial noise conducted by primary transmitters also has a critical interfering effect on primary links. As long as $\lambda_S P_S^{\frac{2}{\alpha}}$ is greater than a lower bound in (54) and less than an upper bound in (55), the access of secondary network is good for the primary network. This is because, for secondary links, the lower bound ensures their jamming effect on eavesdropping links, and the upper bound guarantees that their interfering effect on primary links is acceptable.
- When the intensity of eavesdroppers is large, i.e., $\lambda_E>\frac{abe^{D^2b}}{\pi(D^2b+1)}$, the artificial noise conducted by primary transmitters has a slight jamming effect on eavesdropping links as well as a weak interfering effect on primary links. Hence it is necessary to increase the noise, but not infinite. Consequently, $\lambda_S P_S^{\frac{2}{\alpha}}$ must be greater than a lower bound in (56) and less than an upper bound in (57). The lower bound ensures their jamming effect on eavesdropping links, and the upper bound guarantees that their interfering effect on primary links is acceptable.

B. OPTIMAL SECONDARY LINK SCHEDULING SCHEMES

The secondary link scheduling schemes consist of two parts: scheme S_1 and scheme S_2. Scheme S_1 maximizes the throughput of the secondary network under the optimal secrecy throughput of the primary network. Scheme S_2 maximizes the throughput of the secondary network under the performance guarantee criterion for the primary network. The throughput of the secondary network, denoted by C_S, is given by

$$C_S=Q_{ts}\lambda_S p_{cs}=Q_{ts}\lambda_S\exp\{-c\lambda_S\left(1+\left(\frac{P_P}{P_S}\right)^{\frac{2}{\alpha}}\frac{\lambda'_P}{\lambda_S}\right)\}, \tag{68}$$

where

$$c = \pi(\mathrm{sinc}^{-1}\frac{2}{\alpha})\beta_{cs}^{\frac{2}{\alpha}} r_S^2. \tag{69}$$

When $\lambda_E = \frac{abe^{D^2b}}{\pi(D^2b+1)}$, SUs are not allowed to access the spectrum. Thus we do not talk about this case.

In order to acquire scheme S_1, we first study how to achieve the maximum value of C_P, which is equivalent to the maximum value of $S_p(x)$, i.e., the minimum value of $f(x)$. The optimization problem of C_P is formulated as

$$\min f(\lambda_S, P_S), \quad \text{s.t.} \quad (\lambda_S, P_S) \in \mathcal{F}. \tag{70}$$

Lemma 1 shows that $f(x)$ is convex, and provides the point of the minimum $f(x)$. Then we obtain the following lemma.

Lemma 2: The optimal region $\mathcal{F}'$ to (70) is

$$\lambda_S P_S{}^{\frac{2}{\alpha}} = \left(\frac{2e^{\lambda_E\pi D^2}}{D^2b} W\Big(\frac{D^2b}{2}\sqrt{\frac{\pi\lambda_E(D^2b+1)}{ab}}\Big) - 1\right) e^{\lambda_E\pi D^2}\lambda_P P_P{}^{\frac{2}{\alpha}}. \tag{71}$$

Proof: According to Lemma 1, when $x = x^*$, $f(x)$ obtains the the minimum value. Theorem 4 shows that x^* in (41) is the optimal value to achieve the minimum $f(x)$ regardless of the relation between λ_E and λ_P. Besides, the relation among x, λ_S and P_S is given by (35). Combining (35) with (41), we have

$$\Big(1+\Big(\frac{P_S}{P_P}\Big)^{\frac{2}{\alpha}}\frac{\lambda_S}{\lambda'_P}\Big) = \frac{2e^{\lambda_E\pi D^2}}{D^2b} W\left(\frac{D^2b}{2}\sqrt{\frac{\pi\lambda_E(D^2b+1)}{ab}}\right).$$

By solving the above equality, (71) is established. ■

Lemma 2 indicates that there exists a series of (λ_S, P_S) achieving the maximum value of C_P. Then we investigate the value of λ_S and that of P_S among $\mathcal{F}'$ for the maximum value of C_S, i.e.,

$$\max\ C_S(\lambda_S, P_S), \quad \text{s.t.}\ (\lambda_S, P_S) \in \mathcal{F}'. \tag{72}$$

Here $\mathcal{F}'$ guarantees the optimal secrecy throughput of the primary network. The following theorem is provided to design scheme S_1 that maximizes C_S within the region $\mathcal{F}'$.

Theorem 5: Under the optimal secrecy throughput of the primary network, the optimal λ_S^* and P_S^* (i.e., scheme S_1) achieving the maximum value of C_S are

$$\lambda_S^* = \frac{\psi}{c(\psi+1)}, \tag{73}$$

$$P_S^* = (c(\psi+1)e^{-\lambda_E\pi D^2}\lambda_P)^{\frac{\alpha}{2}} P_P, \tag{74}$$

where

$$\psi = \frac{2e^{\lambda_E\pi D^2}}{D^2b} W\left(\frac{D^2b}{2}\sqrt{\frac{\pi\lambda_E(D^2b+1)}{ab}}\right) - 1. \tag{75}$$

Proof: According to (68), (69) and (71), C_S is

$$C_S = Q_{ts}\lambda_S \exp\big\{-c\big(1+\frac{1}{\psi}\big)\lambda_S\big\}. \tag{76}$$

Then the first derivative of C_S with respect to λ_S is given by

$$\frac{dC_S}{d\lambda_S} = Q_{ts}\big(1-c\big(1+\frac{1}{\psi}\big)\lambda_S\big)\exp\big\{-c\big(1+\frac{1}{\psi}\big)\lambda_S\big\}. \tag{77}$$

By letting $\frac{dC_S}{d\lambda_S} = 0$, we obtain the stationary point of C_S, which is $\frac{\psi}{c(\psi+1)}$. Based on (77), C_S monotonically increases in $\lambda_S \in [0, \frac{\psi}{c(\psi+1)})$ and monotonically decreases in $\lambda_S \in (\frac{\psi}{c(\psi+1)}, \infty)$, hence $\frac{\psi}{c(\psi+1)}$ is the point of minimum C_S, i.e., $\lambda_S^* = \frac{\psi}{c(\psi+1)}$. Besides, according to (71), we obtain (74). This completes the proof. ■

Theorem 5 provides the optimal throughput of the secondary network under the premise of the optimal secrecy throughput of the primary network. Then we focus on the following optimization problem of the secondary throughput, i.e.,

$$\max\ C_S(\lambda_S, P_S), \quad \text{s.t.}\ (\lambda_S, P_S) \in \mathcal{F}. \tag{78}$$

Compared to the optimization problem in (70), the constraint in (78) could be relaxed. Here $\mathcal{F}$ only guarantees that $C_P \geq C_P^{(0)}$ holds. The following theorem aims at scheme S_2 that maximizes C_S within the region $\mathcal{F}$.

Theorem 6: Under the performance guarantee criterion for the primary network, the optimal λ_S^* and P_S^* (i.e., scheme S_2) achieving the maximum value of C_S are listed as follows.

1) If $0 < \lambda_E < \frac{abe^{D^2b}}{\pi(D^2b+1)}$, scheme S_2 is

$$\lambda_S^* = \frac{e^{\lambda_E\pi D^2}-1}{ce^{\lambda_E\pi D^2}} \quad \text{and } P_S^* = (c\lambda_P)^{\frac{\alpha}{2}} P_P. \tag{79}$$

2) If $\lambda_E > \frac{abe^{D^2b}}{\pi(D^2b+1)}$, scheme S_2 is

$$\lambda_S^* = \frac{e^{\lambda_E\pi D^2}x_1-1}{ce^{\lambda_E\pi D^2}x_1} \quad \text{and } P_S^* = (cx_1\lambda_P)^{\frac{\alpha}{2}} P_P. \tag{80}$$

Proof:
Let $\lambda_S P_S{}^{\frac{2}{\alpha}} = \phi\lambda'_P P_P{}^{\frac{2}{\alpha}}$. According to (68), we have

$$C_S = Q_{ts}\lambda_S \exp\big\{-c\lambda_S\big(1+\frac{1}{\phi}\big)\big\}. \tag{81}$$

By employing the same method of Theorem 5, we obtain that C_S achieves the maximum value at $\lambda_S = \frac{\phi}{c(\phi+1)}$ and $P_S = (c(\phi+1)e^{-\lambda_E\pi D^2}\lambda_P)^{\frac{\alpha}{2}} P_P$. By applying $\lambda_S = \frac{\phi}{c(\phi+1)}$ into (81), the maximum C_S can be expressed as

$$C_S^{max} = Q_{ts}\frac{e^{-1}\phi}{c(\phi+1)}. \tag{82}$$

It is easy to see that C_S^{max} monotonically increases in $\phi \in (0, \infty)$, hence ϕ should be as large as possible.

From Theorem 4, we observe that if $\lambda_E < \frac{abe^{D^2b}}{\pi(D^2b+1)}$, the maximum ϕ is $(e^{\lambda_E\pi D^2}-1)$, hence $C_S^{max} = Q_{ts}c^{-1}e^{-1}(1-e^{-\lambda_E\pi D^2})$; If $\lambda_E > \frac{abe^{D^2b}}{\pi(D^2b+1)}$, the maximum ϕ is $(e^{\lambda_E\pi D^2}x_1 - 1)$, hence $C_S^{max} = Q_{ts}c^{-1}e^{-1}(1-e^{-\lambda_E\pi D^2}x_1^{-1})$. This completes the proof. ■

Both C_P and C_S of scheme S_1 depend on ψ in (75), and it is difficult to calculate the specific value of ψ. Consequently, it is also difficult to compare C_P/C_S of scheme S_1 with C_P/C_S of scheme S_2 in a straightforward way. In the next section, we provide numerical results for performance comparison of these two schemes.

V. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we first provide simulation results to verify the analytical results of the derived probabilities p_{cp}, p_{sp} and p_{cs}, and then provide numerical results of secondary network scheduling schemes. Without loss of generality, we set $P_P = 5$, $\alpha = 3$ [9], $D = 2$ and $r_P = 1$ due to the reason that the secrecy guard zone is better to be larger than the transmission region of primary transmitters [13], [15]. Since r_S is considered to be fixed, it is reasonable to set $r_S = 1$. Besides, according to the relationship $Q_{tp} > Q_{mp}$ [37], we set $Q_{tp} = 0.9$, $Q_{mp} = 0.6$, $Q_{ts} = 0.2$. All the parameters are set as described above unless otherwise specified.

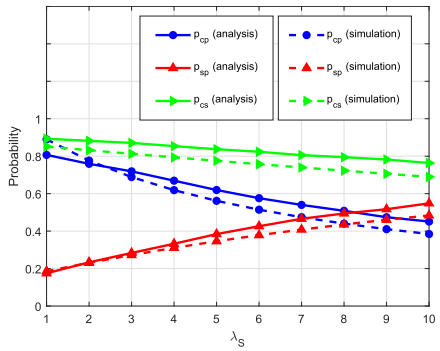

FIGURE 2. Verification of the analytical results of the derived probabilities p_{cp}, p_{sp} and p_{cs}.

The analytical results of the probabilities (i.e., p_{cp}, p_{sp} and p_{cs}) obtained in Section III are the bases of the following secondary network scheduling schemes, hence we verify the analytical results of the probabilities by simulation. The simulation adopts the PPP model with parameters $P_S = 1$, $\lambda_P = 2$, $\lambda_E = 0.5$, $\beta_{cp} = 0.1$, $\beta_{sp} = 0.1$, and $\beta_{cs} = 0.05$. Fig. 2 presents both analytical and simulation results of p_{cp}, p_{sp}, and p_{cs} versus λ_S. As we observe from Fig. 2, the analytical results in Theorems 1-3 are in good agreement with the simulation results. This observation shows that the proposed framework closely agrees with the practical underlay CRNs with eavesdroppers.

In the following, we provide some numerical results of the secondary network scheduling schemes. Fig. 3 presents the result of the comparison between C_P and $C_P^{(0)}$ versus $\lambda_S P_S^{\frac{2}{\alpha}}$ for the case (iii), i.e., $\lambda_E > \frac{abe^{D^2 b}}{\pi(D^2 b+1)}$. Without loss of generality, we set $\lambda_P = 0.1$ and $\lambda_E = 0.5$ to satisfy the condition of the case (iii). The horizontal axis represents x in (35), and x has a positive relationship with $\lambda_S P_S^{\frac{2}{\alpha}}$, which determines the intensity of secondary interference. $C_P^{(0)}$ represents the

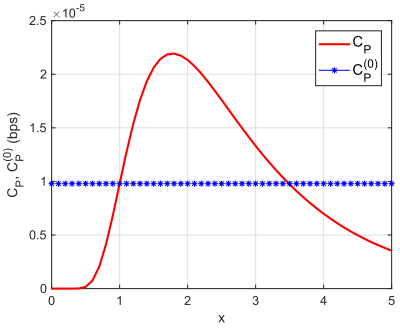

FIGURE 3. The comparison between C_P and $C_P^{(0)}$ versus x, i.e., $\lambda_S P_S^{\frac{2}{\alpha}}$, for $\lambda_E > \frac{abe^{D^2 b}}{\pi(D^2 b+1)}$.

secrecy throughput of the primary network with cooperative mode, which is the basis of comparison. As shown in Fig. 3, C_P is a concave function of x, i.e., the secondary interference. C_P and $C_P^{(0)}$ have two intersection points, where the left one is 1 and the right one is x_1 in (58), and C_P is greater than $C_P^{(0)}$ in $x \in (1, x_1)$. This verifies the feasible region of the case (iii). In addition, we see from this figure that C_P is smaller than $C_P^{(0)}$ in $x \in (0, 1)$ since the secondary interference has a slight jamming effect on eavesdropping links, and C_P is also smaller than $C_P^{(0)}$ in $x \in (x_1, +\infty)$ due to the reason that the secondary interference has a unacceptable interfering effect on primary links. The analysis method of the numerical result of the case (ii) is similar to that of case (iii).

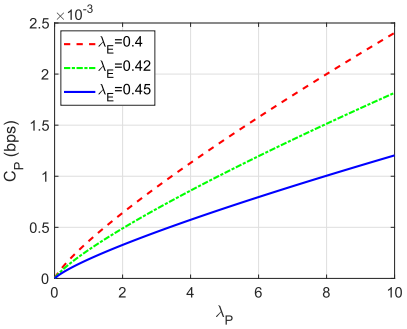

FIGURE 4. C_P of scheme S_1 versus λ_P with different λ_E.

Fig. 4 plots C_P of scheme S_1 versus λ_P with different λ_E. We observe that C_P increases with λ_P. Besides, the C_P with larger λ_E is smaller than that with smaller λ_E, for the reason that the increasing intensity of eavesdroppers reduces the secrecy probability of primary links. Intuitively, the increase of the intensity of eavesdroppers decreases the average distance of eavesdropping links.

Fig. 5 illustrates C_S of scheme S_1 versus λ_P with different λ_E. We observe that C_S decreases with λ_P. In contrast with C_P, the C_S with larger λ_E is larger than that with smaller λ_E. This is because with the increasing of the intensity of eavesdroppers, a larger artificial noise conduced by the secondary network, i.e., larger transmit power and intensity of the secondary network, is required to guarantee the performance of

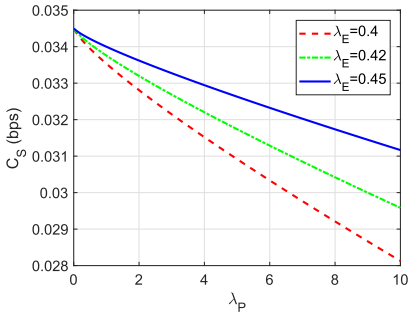

FIGURE 5. C_S of scheme S_1 versus λ_P with different λ_E.

the primary network, and meanwhile the secondary network has more opportunities to access the licensed spectrum.

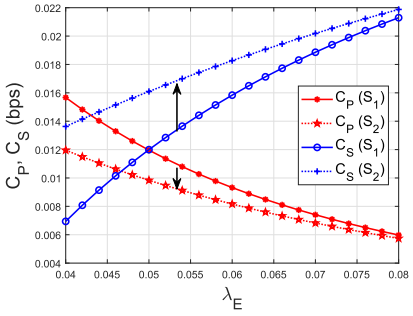

FIGURE 6. C_P/C_S of scheme S_1 and scheme S_2 for $0 < \lambda_E < \frac{abe^{D^2b}}{\pi(D^2b+1)}$.

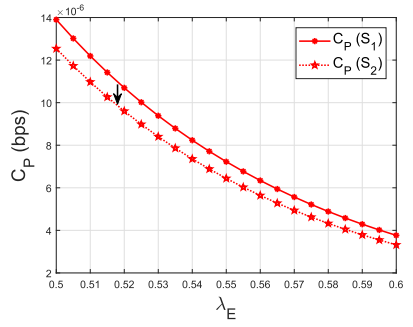

FIGURE 7. C_P of scheme S_1 and scheme S_2 for $\lambda_E > \frac{abe^{D^2b}}{\pi(D^2b+1)}$.

We then compare C_P/C_S of scheme S_1 with those of scheme S_2. Here we choose $\lambda_P = 0.1$, and obtain the threshold $\frac{abe^{D^2b}}{\pi(D^2b+1)} = 0.092$. Fig. 6 plots C_P/C_S of scheme S_1 and scheme S_2 versus λ_E in the case that $0 < \lambda_E < 0.092$. In this case, λ_S and P_S are equal to those in (79), respectively. In Fig. 6, C_P of scheme S_2 is smaller than that of scheme S_1, while C_S of scheme S_2 is larger than that of scheme S_1. Fig. 7 plots C_P of scheme S_1 and scheme S_2 versus λ_E in the case that $\lambda_E > 0.092$, and Fig. 8 plots C_S of scheme S_1 and scheme S_2 versus λ_E in the case that $\lambda_E > 0.092$. In this case, λ_S and P_S are equal to those in (80), respectively. In Fig. 7, C_P of scheme S_2 is still smaller than that of scheme S_1.

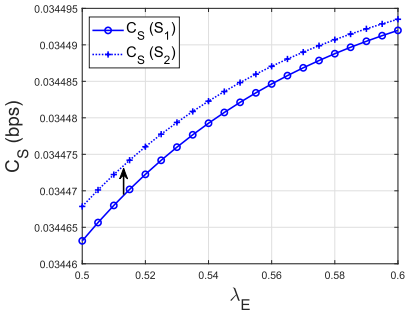

FIGURE 8. C_S of scheme S_1 and scheme S_2 for $\lambda_E > \frac{abe^{D^2b}}{\pi(D^2b+1)}$.

From Fig. 8, we see that C_S of scheme S_2 is still larger than that of scheme S_1. The numerical results verify that scheme S_1 achieves the optimal performance for the primary network, while scheme S_2 provides a higher throughput performance level for the secondary network.

VI. CONCLUSION

In this paper, we focused on a large-scale underlay CRN in the presence of eavesdroppers overhearing the primary transmission. We applied a secrecy guard zone around each primary transmitter to boost the security of the primary network, and adopted the non-cooperative mode to save the energy of the primary network. We modeled such a random CRN through stochastic geometry, and then derived the general closed-form expressions for the connection/secrecy probability of primary links, as well as the connection probability of secondary links. We proposed the performance guarantee criterion for the primary network due to the access of SUs. Based on this criterion, we investigated the feasible region of secondary links. Besides, we designed the optimal secondary link scheduling schemes within the feasible region to maximize the secrecy throughput of the primary network and the throughput of the secondary network, respectively. According to analytical and numerical results, we found that the interference caused by SUs can be exploited to improve the secrecy throughput and energy efficiency of the primary network, and at the meanwhile provide SUs with extra transmission opportunities.

This paper analyzed the energy efficiency of the primary network qualitatively. As one of the future research directions, we will further study the energy efficiency quantitatively. Another direction is to investigate the fairness-aware resource (e.g., power and channel) allocation among secondary users [42]. We also think it is an interesting direction to study energy-efficient communications in wireless sensor networks [43].

REFERENCES

[1] J. Mitola, "Cognitive radio—An integrated agent architecture for software defined radio," PhD. dissertation, Kungliga Tekniska Hogskolan, Royal Inst. Technol., Stockholm, Sweden, 2000.

[2] R. Menon, R. M. Buehrer, and J. H. Reed, "Outage probability based comparison of underlay and overlay spectrum sharing techniques," in *Proc. IEEE DySPAN*, Baltimore, MD, USA, Nov. 2005, pp. 101–109.

[3] L. Gao, Y. Xu, and X. Wang, "MAP: Multiauctioneer progressive auction for dynamic spectrum access," *IEEE Trans. Mobile Comput.*, vol. 10, no. 8, pp. 1144–1161, Aug. 2011.

[4] H. Wen, S. Li, X. Zhu, and L. Zhou, "A framework of the PHY-layer approach to defense against security threats in cognitive radio networks," *IEEE Netw.*, vol. 27, no. 3, pp. 34–39, May 2013.

[5] M. J. Saber and S. M. S. Sadough, "Optimisation of cooperative spectrum sensing for cognitive radio networks in the presence of smart primary user emulation attack," *Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 1, p. e2885, Jan. 2017.

[6] J.-F. Huang, G.-Y. Chang, and J.-X. Huang, "Anti-jamming rendezvous scheme for cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 3, pp. 648–661, Mar. 2017.

[7] C. Wang and H.-M. Wang, "On the secrecy throughput maximization for MISO cognitive radio network in slow fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 11, pp. 1814–1827, Nov. 2014.

[8] K. Zheng *et al.*, "Secrecy capacity scaling of large-scale networks with social relationships," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2688–2702, Mar. 2017.

[9] H. Zhang, T. Wang, L. Song, and Z. Han, "Interference improves PHY security for cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 3, pp. 609–620, Mar. 2016.

[10] L. Xiao, J. Liu, Q. Li, N. B. Mandayam, and H. V. Poor, "User-centric view of jamming games in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2578–2590, Dec. 2015.

[11] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103–5113, Dec. 2013.

[12] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.

[13] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[14] X. Xu, B. He, W. Yang, X. Zhou, and Y. Cai, "Secure transmission design for cognitive radio networks with poisson distributed eavesdroppers," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 373–387, Feb. 2016.

[15] X. Xu, W. Yang, Y. Cai, and S. Jin, "On the secure spectral-energy efficiency tradeoff in random cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 10, pp. 2706–2722, Oct. 2016.

[16] D. Wang, B. Bai, W. Chen, and Z. Han, "Achieving high energy efficiency and physical-layer security in AF relaying," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 740–752, Jan. 2016.

[17] M. El-Halabi, T. Liu, and C. N. Georghiades, "Secrecy capacity per unit cost," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1909–1920, Sep. 2013.

[18] F. Gabry, N. Li, N. Schrammar, M. Girnyk, L. K. Rasmussen, and M. Skoglund, "On the optimization of the secondary transmitter's strategy in cognitive radio channels with secrecy," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 451–463, Mar. 2014.

[19] Y. Wu and X. Chen, "Robust beamforming and power splitting for secrecy wireless information and power transfer in cognitive relay networks," *IEEE Commun. Lett.*, vol. 20, no. 6, pp. 1152–1155, Jun. 2016.

[20] X. Liu, K. Zheng, L. Fu, X.-Y. Liu, X. Wang, and G. Dai, "Energy efficiency of secure cognitive radio networks with cooperative spectrum sharing," *IEEE Trans. Mobile Comput.*, to be published, doi: 10.1109/TMC.2018.2836902.

[21] C. Yang, J. Li, Q. Ni, A. Anpalagan, and M. Guizani, "Interference-aware energy efficiency maximization in 5G ultra-dense networks," *IEEE Trans. Commun.*, vol. 65, no. 2, pp. 728–739, Feb. 2017.

[22] C. C. Zarakovitis, Q. Ni, and J. Spiliotis, "Energy-efficient green wireless communication systems with imperfect CSI and data outage," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 12, pp. 3108–3126, Dec. 2016.

[23] K. Lee, C.-B. Chae, and J. Kang, "Spectrum leasing via cooperation for enhanced physical-layer secrecy," *IEEE Trans. Veh. Technol.*, vol. 62, no. 9, pp. 4672–4678, Jun. 2013.

[24] N. Mokari, S. Parsaeefard, H. Saeedi, and P. Azmi, "Cooperative secure resource allocation in cognitive radio networks with guaranteed secrecy rate for primary users," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 1058–1073, Feb. 2014.

[25] X. Wang, W. Huang, S. Wang, J. Zhang, and C. Hu, "Delay and capacity tradeoff analysis for motioncast," *IEEE/ACM Trans. Netw.*, vol. 19, no. 5, pp. 1354–1367, Oct. 2011.

[26] X. Liu *et al.*, "Network connectivity with inhomogeneous correlated mobility," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4307–4320, Jun. 2016.

[27] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[28] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.

[29] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer, 2016.

[30] A. Rabbachin, T. Q. S. Quek, H. Shin, and M. Z. Win, "Cognitive network interference," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 2, pp. 480–493, Feb. 2011.

[31] J. Lee, A. Conti, A. Rabbachin, and M. Z. Win, "Distributed network secrecy," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1889–1900, Sep. 2013.

[32] C.-H. Lee and M. Haenggi, "Interference and outage in Poisson cognitive networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 4, pp. 1392–1401, Apr. 2012.

[33] J. Lee, J. G. Andrews, and D. Hong, "Spectrum-sharing transmission capacity with interference cancellation," *IEEE J. Sel. Areas Commun.*, vol. 63, no. 1, pp. 76–86, Jan. 2013.

[34] S. A. R. Zaidi, M. Ghogho, D. C. McLernon, and A. Swami, "Achievable spatial throughput in multi-antenna cognitive underlay networks with multi-hop relaying," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1543–1558, Aug. 2013.

[35] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.

[36] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996.

[37] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[38] A. Hasan and J. G. Andrews, "The guard zone in wireless ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 3, pp. 897–906, Mar. 2007.

[39] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[40] M. Haenggi, *Wireless Security and Cryptography: Specifications and Implementations*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[41] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth, "On the lambert *W* function," *IEEE Trans. Wireless Commun.*, vol. 5, no. 1, pp. 329–359, Dec. 1996.

[42] Q. Ni and C. Zarakovitis, "Nash bargaining game theoretic scheduling for joint channel and power allocation in cognitive radio systems," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 1, pp. 70–81, Jan. 2012.

[43] X. Liu *et al.*, "CDC: Compressive data collection for wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 8, pp. 2188–2197, Aug. 2015.

XIAOYING LIU received the B.E. degree in electronic engineering from the Nanjing University of Science and Technology, Nanjing, China, in 2013, and the Ph.D. degree in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 2018. She is currently with the School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, China. Her research interests include scaling laws analysis in wireless networks, network security, and green communications.

KECHEN ZHENG received the B.E. and Ph.D. degrees in electronic engineering from Shanghai Jiao Tong University, Shanghai, China, in 2013 and 2018, respectively. He is currently with the School of Computer Science and Technology, Zhejiang University of Technology, Hangzhou, China. His research interests include scaling laws analysis in wireless networks, performance evaluation in cognitive networks and social networks, and energy harvesting wireless communication networks.

XIAO-YANG LIU (M'15) received the B.E. degree in computer science and technology from the Huazhong University of Science and Technology, Wuhan, in 2010. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, Columbia University, and the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include tensor theory and deep learning, big data analysis, data privacy and homomorphic encryption, and green communication networks.

XINBING WANG (SM'12) received the B.S. degree (Hons.) from the Department of Automation, Shanghai Jiaotong University, Shanghai, China, in 1998, the M.S. degree from the Department of Computer Science and Technology, Tsinghua University, Beijing, China, in 2001, and the Ph.D. degree major from the Department of Electrical and Computer Engineering, minor from the Department of Mathematics, North Carolina State University, Raleigh, in 2006. He is currently a Professor with the Department of Electronic Engineering, Shanghai Jiaotong University. He was a member of the Technical Program Committee of several conferences, including the ACM MobiCom 2012, the ACM MobiHoc 2012–2014, and the IEEE INFOCOM 2009–2017. He has been an Associate Editor of the IEEE/ACM TRANSACTIONS ON NETWORKING and the IEEE TRANSACTIONS ON MOBILE COMPUTING.

GUOJUN DAI (M'00) received the Ph.D. degree from Zhejiang University in 1998. He is currently a Professor with the School of Computer Science and Technology, and the Director of the Institute of Applied Computing, Hangzhou Dianzi University. He is also the Director of the International Cooperation Base of Human–Machine interaction of Zhejiang province. He authored over 40 research papers in top-quality international conferences and journals, particularly, INFOCOM, the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and the IEEE TRANSACTIONS ON MOBILE COMPUTING. He also published two books and has over 20 granted patents. His research interests include cyber-physical system, wireless sensor network, and big data application. He is a member of the ACM.