Protecting Cognitive Radio Networks Against Poisson Distributed Eavesdroppers

Yueming Cai†, Xiaoming Xu†, Biao He‡, Weiwei Yang†, and Xiangyun Zhou‡
†College of Communications Engineering, PLA University of Science and Technology, Nanjing, China
‡Research School of Engineering, Australian National University, Canberra, Australia
Email: caiym@vip.sina.com, xiaomingxu.plaust@gmail.com, biao.he@anu.edu.au,
wwyang1981@163.com, xiangyun.zhou@anu.edu.au,

***Abstract*—In this paper, we study secure transmission designs for underlay cognitive radio networks in the present of randomly distributed eavesdroppers. We consider the scenario where a secondary transmitter sends confidential messages to a secondary receiver subject to an interference constraint set by the primary user. We design two transmission protocols under different channel knowledge assumptions at the transmitter. For each protocol, we first give a comprehensive performance analysis to investigate the transmission delay, secrecy, and reliability performance. We then optimize the transmission design for maximizing the secrecy throughput subject to both secrecy and reliability constraints. Finally, we numerically compare the performance of the two transmission protocols.**

***Index Terms*—Physical layer security, cognitive radio networks, threshold-based transmission, secrecy guard zone.**

I. Introduction

Cognitive radio (CR) has been regarded as a promising technology to solve the problem of inefficient spectrum usage to address the conflict between spectrum scarcity and spectrum underutilization [1, 2]. In CR networks, unlicensed secondary users (SUs) are allowed to access the spectrum of licensed primary users (PUs) with the requirement of not interfering the PUs. Allowing the spectrum sharing in the CR network makes the CR networks intrinsically non-secure. The coexistence of licensed and unlicensed users in the same network makes the data transmissions more vulnerable to security attacks [3]. To address this concern, innovative security technologies have been proposed for CR networks [3]. As a complement to the traditional cryptographic techniques [4], physical layer security (PLS) has been widely studied [5, 6] to secure the wireless transmissions by exploiting the fading characteristics of wireless channels. The information-theoretic performance of PLS in CR networks has been analyzed in, e.g., [7–9]. The signal processing technique to improve PLS in CR networks has been investigated in, e.g., [10–12].

Although increasing amount of attention has been paid to the issue of PLS in CR networks, most of current studies are still based on some simplified and idealized assumptions. For example, all of the aforementioned work [7–12] assumed that either the eavesdropper's channel state information (CSI) is perfectly known at the legitimate side or the network consists of only a very small number of eavesdroppers with known locations. In practice, an external eavesdropper would not reveal its CSI or location information to the legitimate side, and hence such assumptions are not always valid [13].

Taking into account potentially a large number of eavesdroppers inside the network at random and possibly changing locations (due to mobility), a common analytical approach is to model the location set of eavesdroppers to be a stochastic process following some distributions [14–16]. To the best of the authors' knowledge, the consideration of randomly distributed eavesdroppers has been rarely discussed in CR networks with a few exceptions. In [17] and [18], Shu. *et al* considered that the message to the PU is confidential and derived the secrecy capacity in the presence of randomly distributed eavesdroppers whose location set is modeled as a homogeneous Poisson point process (HPPP). However, the work in [17] and [18] considered a simplified channel model consisting of only the pass loss effect, while the fading effect is not considered. It is important to note that the performance of secure communication is very different between a fading and a non-fading scenario. Furthermore, the presence of fading can be smartly utilized to achieve a better secrecy performance.

In this paper, we study the problem of achieving PLS in an underlay CR network where a secondary transmitter (SU-Tx) sends confidential information to a secondary receiver (SU-Rx) over a quasi-static Rayleigh fading channel in the present of multiple eavesdroppers. To satisfy the interference constraint, the transmit power at the SU-Tx is carefully adjusted, which is determined by the instantaneous channel condition from the SU-Tx to the primary receiver (PU-Rx). The location set of the eavesdroppers is modeled as a HPPP. We consider two transmission protocols to achieve the secure transmission in the CR network: the secrecy guard zone protocol and the threshold-based protocol. The secrecy guard zone protocol is applicable for the scenario where the SU-Tx can detect the existence of eavesdroppers in its vicinity. The threshold-based protocol is applicable for the scenario where the SU-Tx can obtain a one-bit feedback from the SU-Rx. For each transmission protocol, we comprehensively evaluate the performance of transmission delay, secrecy, and reliability. Moreover, we optimize the designs of transmission protocols based on the performance analysis. To this end, we study the optimization problem of maximizing secrecy throughput subject to secrecy

This work was supported by the Natural Science Foundation of China under Project 61371122, Project 61471393, and the Australian Research Council under Discovery Project Grant DP150103905.

and reliability constraints. Finally, we numerically compare the performance of the two transmission protocols. We find that the secrecy guard zone protocol is preferred when the secrecy constraint is stringent while the threshold-based protocol is preferred when the reliability constraint is stringent.

It is worth mentioning that the concept of secrecy guard zone protocol has been previously studied in, e.g., [14, 15, 19], and the concept of similar threshold-based protocol has been previously investigated in, e.g., [20, 21]. Different from the existing results in [14, 15, 19], our proposed secrecy guard zone protocol is applicable in the CR network where the SU-Tx has an adaptive transmit power. Most importantly, none of [14, 15, 19] has studied the optimal design of the secrecy guard zone. In contrast, we have derived the optimal radius of the guard zone that maximizes the secrecy throughput. Note that the optimal design of the radius is very important for the performance of the secrecy guard zone protocol. Different from the existing results in [20, 21], our proposed threshold-based protocol is specifically designed for the CR network where the SU-Tx has an adaptive transmit power. The consideration of adaptive transmit power at the SU-Tx protects the primary network from interference by ensuring a low interference power received at the primary user. We have derived the optimal design of the threshold value, which is dependent on the conditions of both the channel from SU-Tx to PU-Rx and the channel from SU-Tx to SU-Rx. Although the optimal SNR threshold has also been designed in [21], the result in [21] cannot be applied in the secure CR network.

II. System Model

A. Channel Model

We consider an underlay CR network that consists of a primary transmitter-receiver pair and a secondary transmitter-receiver pair. The SU-Tx sends confidential messages to the SU-Rx in the present of multiple movable eavesdroppers, which are denoted by $\{E_j | j = 1, 2, \cdots\}$. We assume that the eavesdroppers are randomly distributed in the network. The location set of the eavesdroppers, denoted by Φ_E, is modeled as a HPPP with density λ_E. The primary network allows the secondary network to share the spectrum by underlay method, and requires that the instantaneous interference power at the PU-Rx from the SU-Tx is lower than a threshold, denoted by I_0. We further assume that all communication nodes have a single antenna and the wireless communication channel is modeled as a path-loss plus quasi-static Rayleigh fading channel. Denote the transmitter power at SU-Tx as P. Then, the received signal to noise ratios (SNRs) at the SU-Rx and eavesdropper E_j are given by

$$\gamma_D = \frac{P}{\sigma_D^2} \left|h_{SD}\right|^2 d_{SD}^{-\alpha} \tag{1}$$

and

$$\gamma_{E_j} = \frac{P}{\sigma_{E_j}^2} \left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}, \tag{2}$$

respectively, where $\alpha \geq 2$ denotes the path loss exponent, d_{SD} and d_{SE_j} denote the distance from SU-Tx to SU-Rx and the distance from SU-Tx to E_j, respectively, σ_D^2 and $\sigma_{E_j}^2$ denote additive white Gaussian noise (AWGN) variances at SU-Rx and E_j, respectively, with $\sigma_D^2 = \sigma_{E_j}^2 = \sigma^2$. In addition, h_{SD} and h_{SE_j} denote the channel coefficients for the channel from SU-Tx to SU-Rx and the channel from SU-Tx to E_j, respectively, which are modeled as complex Gaussian variables with zero mean and unit variance, i.e., $\mathcal{CN}(0, 1)$. Following a widely-adopted assumption, we consider that the interference from the primary transmitter (PU-Tx) at the SU-Rx or the eavesdropper is neglectable [9, 11, 22–24]. A practical example that approximates this occurrence is the scenario where the PU-Tx is located far away from the SU nodes [23].

We assume that the receiver side (including the PU-Rx, the SU-Rx and the eavesdroppers) has the perfect CSI. We consider a scenario where the PU-Rx is a cellular base station which is capable of instantaneous CSI feedback to both the PU-Tx and the SU-Tx, while the SU-Rx is not capable of full CSI feedback. Specifically, the PU-Rx feeds back to the SU-Tx with the instantaneous channel gain, denoted by $h_{SP} \sim \mathcal{CN}(0, 1)$, to enable the SU-Tx to adjust its transmit power to satisfy the interference constraint. This can be achieved through a spectrum-band manager that mediates between the licensed and unlicensed users [25]. Although the SU-Rx is not capable of full CSI feedback, we consider the possibility of a low-complexity feedback scheme in which the SU-Rx uses one bit to inform SU-Tx about its channel condition. The external eavesdroppers are totally passive, and hence their CSI is not revealed to SU-Tx. To satisfy the instantaneous interference constraint, I_0, the SU-Tx adjusts the transmit power to

$$P = \frac{I_0}{\left|h_{SP}\right|^2 d_{SP}^{-\alpha}} \mathbf{1}_{(\text{condition})}, \tag{3}$$

where d_{SP} denotes the distance from SU-Tx to PU-Rx. The $\mathbf{1}_{(\text{condition})}$ in (3) denotes an indicator function for whether the transmission is "on" or "off" at SU-Tx, which is given by

$$\mathbf{1}_{(\text{condition})} = \begin{cases} 1, & \text{if the condition holds} \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

where the condition in (4) depends on the specifical transmission protocol. We highlight that having such an on-off transmission strategy can effectively improve the secrecy and/or the reliability performance, which will be shown later in Sections III and V.

For a robust analysis, we consider that all eavesdroppers can collude and exchange information. Thus, the multiple eavesdroppers can be regarded as a single eavesdropper, E_{joint}, with multiple distributed antennas. The equivalent receive SNR at the E_{joint} is given by

$$\gamma_E = \frac{P}{\sigma^2} \sum\nolimits_{E_j \in \Phi_E} \left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}. \tag{5}$$

From (1) and (5), we note that γ_D and γ_E have the same power variable P, which makes them correlated with each other. For convenience, we define $Z_{\Phi_E} = \sum_{E_j \in \Phi_E} \left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}$.

B. Secure Encoding

The SU-Tx uses the widely-adopted wiretap code [26] to encode the confidential messages. Let $\mathbb{C}(R_B, R_S)$ denote the set of all possible Wyner codes, where R_B is the codeword transmission rate and R_S is the confidential information rate with $R_B > R_S$. The rate difference $R_B - R_S$ reflects the cost of securing the message against eavesdropping. We assume that the encoding rates have already been designed, and hence R_B and R_S are fixed. Such a fixed-rate transmission scheme is suitable for practical applications requiring low complexity, e.g., video streams in multimedia.

C. Outage Probability Metrics

In the following, we detail the outage definitions for characterizing the transmission delay, the secrecy performance and the reliability performance of the network. Moreover, we propose a new probability metric to comprehensively evaluate the joint performance of secrecy and reliability.

1) TP: Since the transmission may not always happen at SU-Tx depending on the transmission protocol, there exists a probability of transmission referred to as TP, which is given by

$$p_{\text{tx}} = \mathbb{P}\left(\mathbf{1}_{(\text{condition})} = 1\right), \tag{6}$$

where $\mathbb{P}(\cdot)$ denotes the probability measure. We adopt the probability of transmission as the metric of the delay performance.

2) SOP and COP: With the fixed-rate wiretap code, there are two kinds of outage events [21, 27]: secrecy outage event and connection outage event. The secrecy outage happens when the perfect secrecy of transmission is not achieved, and the probability of the secrecy outage referred to as SOP is given by [21]

$$p_{\text{so}} = \mathbb{P}\left(C_E > R_B - R_S | \, \mathbf{1}_{(\text{condition})} = 1\right), \tag{7}$$

where $C_E = \log(1+\gamma_E)$ denotes the channel capacity of E_{joint}. The connection outage happens when the received message cannot be decoded at the intended receiver without error, and the probability of the connection outage referred to as COP is given by

$$p_{\text{co}} = \mathbb{P}\left(C_B < R_B | \, \mathbf{1}_{(\text{condition})} = 1\right), \tag{8}$$

where $C_B = \log(1+\gamma_D)$ denotes the channel capacity of the secondary link. We adopt the SOP as the metric of the secrecy performance and the COP as the metric of the reliability performance.

3) TSOP: From (7) and (8), we note that the secrecy and reliability become correlated in the considered CR network due to the correlation between γ_D and γ_E. Therefore, it is necessary to comprehensively study the joint performance of the secrecy and the reliability. To this end, we propose a new outage performance metric, namely transmission secrecy outage probability (TSOP). The TSOP characterizes the probability that either secrecy outage or connection outage happens, which is given by

$$p_{\text{tso}} = 1 - \mathbb{P}\left(C_E \le R_B - R_S, C_B \ge R_B | \, \mathbf{1}_{(\text{condition})} = 1\right). \tag{9}$$

We highlight that the TSOP takes the mutual correlation between the SOP and the COP into account. A similar concept of jointly measuring secrecy and reliability performance can be found in another widely-adopted outage probability definition, i.e., $p_{\text{out}} = \mathbb{P}(C_S < R_S)$ [28], where C_S denotes the secrecy capacity. Compared with p_{tso} in (9), the p_{out} in [28] has not taken into account the transmission rate of codewords and the condition under which message transmission happens.

D. Secrecy Throughput

The overall performance of the system is measured by the secrecy throughput taking into account the transmission delay, the secrecy performance and the reliability performance together. The secrecy throughput is given by

$$\eta = p_{\text{tx}}(1 - p_{\text{tso}}) R_S, \tag{10}$$

where p_{tx} is the TP in (6) and p_{tso} is the TSOP in (9). As such, the secrecy throughput in (10) quantizes the average secrecy rate at which the messages are securely and reliably transmitted to SU-Rx.

III. Secure Transmission Protocols

We study two secure transmission protocols which are secrecy guard zone protocol and threshold-based protocol. The secrecy guard zone protocol is applicable for the scenario where the SU-Tx can detect the existence of eavesdroppers in its vicinity and the threshold-based protocol is applicable for the scenario where the SU-Tx can obtain a one-bit feedback from SU-Rx.

A. Secrecy Guard Zone Protocol

For the secrecy guard protocol, we consider the scenario where the SU-Tx is able to detect the existence of eavesdroppers within a finite range. As per the mechanism of secrecy guard zone [19, 29], we model the finite range around the SU-Tx as a secrecy guard circle $\mathcal{B}$ with radius r. The SU-Tx transmits messages only when there is no eavesdropper detected inside the guard circle. Thus, the condition in (4) for the secrecy guard zone protocol is that no eavesdropper is detected inside the secrecy guard zone, i.e., $\left\{C_1 : \forall E_j \in \Phi_E, d_{SE_j} > r\right\}$.

We denote the location of the SU-Tx as the origin o. Then, the secrecy guard zone around the SU-Tx with radius r is denoted by $\mathcal{B}(o, r)$. Note that the number of eavesdroppers inside $\mathcal{B}(o, r)$, denoted by N, is a Poisson random variable with mean $\pi r^2 \lambda_E$. Thus, its probability mass function (PMF) is given by

$$\mathbb{P}(N = n) = \exp\left(-\pi r^2 \lambda_E\right) \frac{\left(\pi r^2 \lambda_E\right)^n}{n!}. \tag{11}$$

Then, the TP is derived as

$$p_{\text{tx}} = \mathbb{P}(N = 0) = \exp\left(-\pi \lambda_E r^2\right). \tag{12}$$

Substituting (1) into (8) with condition C_1, the COP for the secrecy guard zone protocol is given by

$$p_{\text{co}} = \mathbb{P}\left(|h_{SD}|^2 < \frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}|h_{SP}|^2\right) = \frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}. \quad (13)$$

Denote $\widetilde{\Phi}_E$ as the new location set of the eavesdroppers for the scenario where the transmission happens, i.e., no eavesdropper is inside the secrecy guard zone. Then, the received SNR at the eavesdropper E_{joint} for the scenario where the transmission happens is given by $\gamma_E = \frac{P}{\sigma^2}\sum_{E_j\in\widetilde{\Phi}_E}\left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}$. Here, we define $Z_{\widetilde{\Phi}_E} = \sum_{E_j\in\widetilde{\Phi}_E}\left|h_{SE_j}\right|^2 d_{SE_j}^{-\alpha}$. Thus, the SOP for the secrecy guard zone protocol is derived as

$$p_{\text{so}} = \mathbb{P}\left(\log_2\left(1+\frac{I_0 Z_{\widetilde{\Phi}_E}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}}\right) > R_B - R_S\right) = 1 - L_{Z_{\widetilde{\Phi}_E}}\left(\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \quad (14)$$

We can further derive the Laplace transform of $Z_{\widetilde{\Phi}_E}$ as

$$L_{Z_{\widetilde{\Phi}_E}}(s) = \exp\left[-\frac{2}{\alpha}\pi\lambda_E s^{2/\alpha}\mathrm{B}_{\left(r^{\alpha}s^{-1}+1\right)^{-1}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)\right], \quad (15)$$

where $\mathrm{B}_x(p,q) = \int_0^x t^{p-1}(1-t)^{q-1}\,dt$ is the incomplete Beta function. For brevity, the detailed derivation is omitted here. Then, the closed-form expression for the SOP can be obtained by substituting (15) into (14). Based on (1), (5) and (9), the TSOP for the secrecy guard zone protocol is derived as

$$p_{\text{tso}} = 1 - \frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}} \cdot L_{Z_{\widetilde{\Phi}_E}}\left(\frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \quad (16)$$

B. Threshold-Based Protocol

In the threshold-based protocol, we assume that the SU-Tx can obtain a one-bit feedback from the SU-Rx to enable a threshold-based transmission. Specifically, the SU-Tx transmits only when the received SNR at SU-Rx is larger than a predetermined threshold μ. Otherwise, the SU-Tx suspends the transmission. To this end, the SU-Rx sends an instantaneous one-bit feedback to the SU-Tx for indicating whether the received SNR is larger the threshold μ. Thus, the condition in (4) for the threshold-based protocol is that the SNR at the SU-Rx is larger than μ, i.e., $\left\{C_2 : \frac{I_0|h_{SD}|^2 d_{SD}^{-\alpha}}{\sigma^2|h_{SP}|^2 d_{SP}^{-\alpha}} > \mu\right\}$.

The SU-Tx transmits only when γ_D is larger than the predetermined threshold $\mu \in [0,\infty)$. Thus, the TP is given by

$$p_{\text{tx}} = \mathbb{P}\left(C_2 : \gamma_D > \mu\right) = \frac{I_0 d_{SP}^{\alpha}}{\mu\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}. \quad (17)$$

Note that only when $\mu \in \left[0, 2^{R_B}-1\right)$, the connection outage exists. Substituting (1) into (8), the COP for $\mu \in \left[0, 2^{R_B}-1\right)$ is derived as

$$p_{\text{co}} = \frac{\mathbb{P}\left(\frac{\mu\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}|h_{SP}|^2 < |h_{SD}|^2 < \frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}|h_{SP}|^2\right)}{\mathbb{P}\left(\frac{\mu\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}|h_{SP}|^2 < |h_{SD}|^2\right)} = 1 - \frac{\mu\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}. \quad (18)$$

Then, the COP for $\mu \geq 0$ is given by

$$p_{\text{co}} = 1 - \frac{\mu\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\max\left(\mu, 2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}. \quad (19)$$

Substituting (5) into (7), the SOP for the threshold-based protocol is derived as

$$p_{\text{so}} = \frac{\mathbb{E}_{\Phi_E}\left\{\int_0^{\frac{I_0 d_{SP}^{\alpha} Z_{\Phi_E}}{\left(2^{R_B-R_S}-1\right)N_0}} \exp\left(-\left(\frac{\mu\sigma^2 d_{SD}^{\alpha}}{I_0 d_{SP}^{\alpha}}+1\right)y\right)dy\right\}}{I_0 d_{SP}^{\alpha}/\left(\mu\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}\right)} = 1 - L_{Z_{\Phi_E}}\left(\frac{\mu\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \quad (20)$$

where $L_{Z_{\Phi_E}}(s) = \exp\left(-2\pi\lambda_E s^{2/\alpha}/\alpha\Gamma\left(1-\frac{2}{\alpha}\right)\Gamma\left(\frac{2}{\alpha}\right)\right)$ is the Laplace transform of Z_{Φ_E}. Substituting (1) and (5) into (9), the TSOP for this protocol is derived as (21), which is shown at the top of next page.

IV. Optimal Designs for Secrecy Throughput Maximization

In the section, we optimize the design of each transmission protocol for maximizing the secrecy throughput subject to the secrecy outage probability constraint and the connection outage probability constraint. For each transmission protocol, we first investigate the feasible constraints under which a non-zero secrecy throughput is achievable. We then obtain the optimal solution of the designable parameter, i.e., r for the secrecy guard zone protocol or μ for the threshold-based protocol.

A. Secrecy Guard Zone

For the secrecy guard zone protocol, the designable parameter is the radius of the guard zone, r. Then, we formulate the optimization problem as

$$\textbf{P1:}\ \max_{r}\quad \eta(r) = p_{\text{tx}}(r)\left(1-p_{\text{tso}}(r)\right)R_S, \quad \text{s.t.}\quad p_{\text{so}} \leq \varepsilon, p_{\text{co}} \leq \delta, r \geq 0. \quad (22)$$

1) Feasibility of Constraints: We find that the SOP in (14) is a decreasing function of r, and $\lim_{r\to\infty} p_{so} = 0$. We also find that the COP in (13) is independent with r. Thus, the feasible constraint range for the secrecy guard zone protocol is given by

$$\left\{(\varepsilon,\delta) : 0 < \varepsilon \leq 1, \delta_1 \leq \delta \leq 1\right\}. \quad (23)$$

where δ_1 is the COP of secrecy guard zone in (13).

$$p_{\text{tso}} = 1 - \mathbb{P}\left(\log_2\left(1+\gamma_E\right) < R_B - R_S \;\&\; \log_2\left(1+\gamma_D\right) > R_B \middle| \mathbf{1}_{(C_2)} = 1\right)$$
$$= 1 - \frac{\mu\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\max\left(\mu, 2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}} L_{Z_{\Phi_E}}\left(\frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \quad (21)$$

2) Optimal Design: The optimal design parameter r^* of the P1 is given by

$$r^* = \begin{cases} 0, & \text{if } \varepsilon_1 < \varepsilon \le 1 \\ r_{\text{LB}}, & \text{if } 0 \le \varepsilon \le \varepsilon_1, \end{cases} \quad (24)$$

where

$$r_{\text{LB}} = \phi^{1/\alpha}\left(\left(\text{B}^{-1}_{\frac{-\alpha\ln(1-\varepsilon)}{2\pi\lambda_E\phi^{1/\alpha}}}\left(1-\frac{2}{\alpha},\frac{2}{\alpha}\right)\right)^{-1} - 1\right)^{1/\alpha} \quad (25)$$

with $\phi = \frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}$ and $\text{B}_x^{-1}(p,q)$ representing the inverse function of $\text{B}_x(p,q)$.

Proof: Substituting (12) and (16) into (10), the secrecy throughput η for the secrecy guard zone can be derived as a closed-form expression. Taking first-order derivative of η with respect to r, we can obtain $\frac{\partial\eta(r,\mu)}{\partial r} < 0$. This implies that the secrecy throughput is a decreasing function of radius, r. Therefore, it is wise to set r to the minimum value considering the secrecy constraint. For brevity, the detailed proof is omitted here. ■

B. Threshold-Based Protocol

For the threshold-based protocol, the designable parameter is the SNR threshold, μ. Then, we formulate the optimization problem as

$$\textbf{P2:} \max_{\mu} \quad \eta(\mu) = p_{\text{tx}}(\mu)\left(1 - p_{\text{tso}}(\mu)\right)R_S, \quad \text{s.t.} \quad p_{\text{so}} \le \varepsilon, p_{\text{co}} \le \delta, \mu \ge 0. \quad (26)$$

1) Feasibility of Constraints: We find that the COP in (19) is a decreasing function of μ and when $\mu \ge 2^{R_B}-1$, p_{co} is equal to zero. We also find the SOP in (20) is an increasing function of μ. To be specific, when $\delta \ge \delta_1$, the minimum value of ε can be achieved by setting μ to zero, which is given by

$$\varepsilon_1 = 1 - L_{Z_{\Phi_E}}\left(\frac{I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \quad (27)$$

When $\delta < \delta_1$, by setting $p_{\text{co}} = \delta$, we can obtain the minimum value of the ε as

$$\varepsilon_2 = 1 - L_{Z_{\Phi_E}}\left((1-\delta)\frac{\left(2^{R_B}-1\right)\sigma^2 d_{SD}^{\alpha} + I_0 d_{SP}^{\alpha}}{\left(2^{R_B-R_S}-1\right)\sigma^2}\right). \quad (28)$$

Therefore, the feasible constraint range for the threshold-based protocol is given by

$$\left\{(\varepsilon,\delta) : \max\left(\varepsilon_1,\varepsilon_2\right) \le \varepsilon \le 1, 0 \le \delta \le 1\right\}. \quad (29)$$

2) Optimal Design: The optimal design parameters μ^* of the P2 is given by

$$\mu^* = \begin{cases} [\,0, \mu_{\text{UB}}\,], & \text{if } \delta_1 < \delta \le 1 \\ [\,\mu_{\text{LB}}, \mu_{\text{UB}}\,], & \text{if } 0 \le \delta \le \delta_1, \end{cases} \quad (30)$$

where

$$\mu_{\text{LB}} = (1-\delta)\left(2^{R_B}-1\right) - \frac{I_0 d_{SP}^{\alpha}}{\sigma^2 d_{SD}^{\alpha}}\delta, \quad (31)$$

$$\mu_{\text{UB}} = \min\left(2^{R_B}-1, \left(\frac{-\alpha\ln(1-\varepsilon)}{2\pi\lambda_E\Gamma(1-\alpha/2)\Gamma(\alpha/2)}\right)^{\alpha/2} \cdot\frac{2^{R_B-R_S}-1}{d_{SD}^{\alpha}} - \frac{I_0 d_{SP}^{\alpha}}{\sigma^2 d_{SD}^{\alpha}}\right). \quad (32)$$

Proof: Substituting (17) and (21) into (10), the secrecy throughput η for the secrecy guard zone can be derived as a closed-form expression. We find that when $\mu > 2^{R_B}-1$, η is a decreasing function of μ. When $\mu \le 2^{R_B}-1$, η remains constant. Therefore, it is wise to have $\mu \le 2^{R_B}-1$. To satisfy the secrecy constraint, there is an upper bound of μ. By solving $p_{\text{so}} = \varepsilon$ and according to $\mu \le 2^{R_B}-1$, we derive the upper bound as (32). In addition, to satisfy the reliability constraint, there is a lower bound of μ. By solving $p_{\text{co}} = \delta$, we derive the lower bound as (31). For brevity, the detailed proof is omitted here. ■

V. Numerical Results and Discussion

In this section, we first illustrate the impact of design parameters on the studied transmission protocols. We then compare the achievable performance of the two transmission protocols based on the proposed optimal designs. The results shown in this section are all for the network with $\alpha = 4$, $I_0/\sigma^2 = 10$ dB, $R_B = 3$, $R_S = 1$, $d_{SD} = 5$ and $d_{SP} = 5$.

We first demonstrate the impact of the secrecy guard zone radius r on the performance of secrecy guard zone protocol. Figure 1 plots p_{tx}, p_{co}, p_{so}, and p_{tso} versus r. As shown in the figure, both of p_{so} and p_{tx} are decreasing functions of r. This implies that a high secrecy level is achieved at the cost of a large transmission delay. Thus, a large radius of the secrecy guard zone is not always beneficial for real CR networks. In addition, we find that COP remains constraint with the increase of the radius, since the COP is not related to the radius of secrecy guard zone.

We then exam the impact of the SNR threshold μ on the performance of threshold-based protocol. Figure 2 plots p_{tx}, p_{co}, p_{so}, and p_{tso} versus μ for threshold-based protocol. As the figure shows, p_{co} is a decreasing function of μ, and it is equal to zero when $\mu \ge 2^{R_B}-1$. The p_{so} is an increasing function of μ and p_{tx} is a decreasing function of μ. These observations

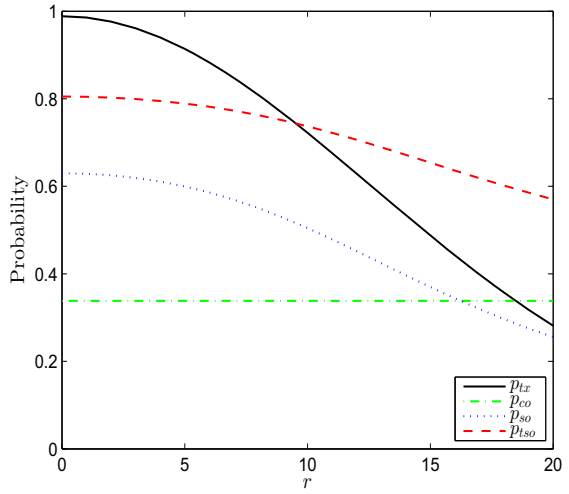

Fig. 1. TP, COP, SOP and TSOP for the secrecy guard zone protocol versus secrecy guard radius r with eavesdropper density $\lambda_E = 10^{-3}$.

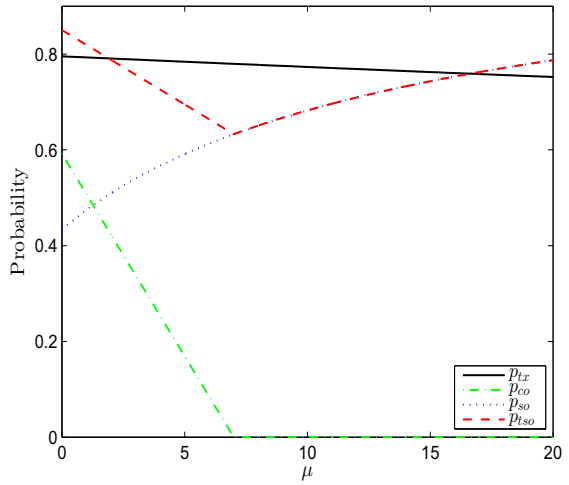

Fig. 2. TP, COP, SOP and TSOP for threshold-based protocol versus the SNR threshold μ with eavesdropper density $\lambda_E = 10^{-3}$.

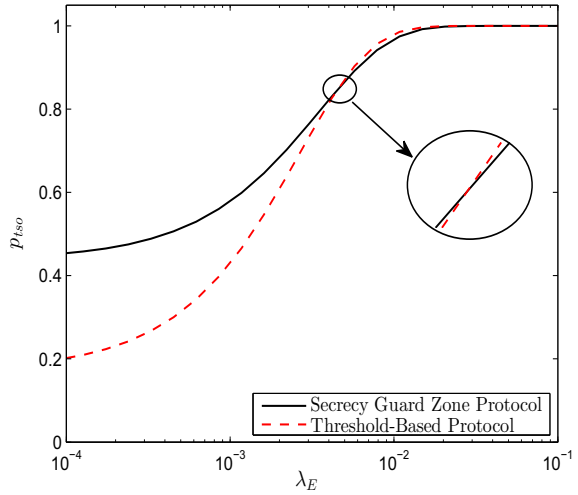

Fig. 3. The TSOP for both of secrecy guard zone and threshold-based transmission protocols versus the eavesdropper density.

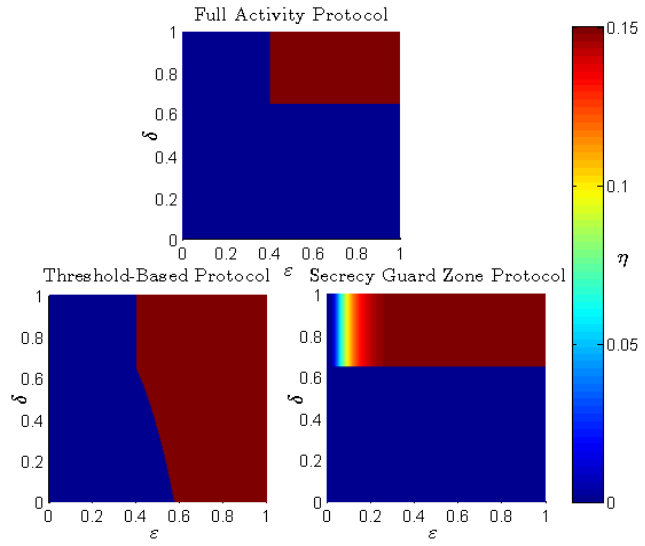

Fig. 4. The optimized secrecy throughput η (bits/s/Hz) for different transmission protocols as a function of the secrecy constraint ε and the reliability constraint δ with eavesdropper density $\lambda_E = 10^{-3}$.

imply that a larger SNR-threshold can enhance the reliability performance while harm the secrecy performance and the transmission delay performance. Consequently, p_{tso}, which characterizes the joint performance of secrecy and reliability, is not a monotonous function of μ. The p_{tso} firstly decreases and then increases as μ increases, and p_{tso} is minimized at $\mu = 2^{R_B} - 1$. According to these observations, the designers of real CR networks can wisely set up the SNR threshold to balance the tradeoff among the delay, secrecy, and reliability performance of the network.

Next, we compare the joint secrecy and reliability performance of the two transmission protocols. Figure 3 plots p_{tso} versus the eavesdropper density λ_E. As depicted in the figure, p_{tso} is an increasing function of λ_E for both protocols. We note that, when the eavesdropper density is low, the threshold-based protocol outperforms the secrecy guard zone protocol. On the contrary, when the eavesdropper density is high, the secrecy guard zone protocol outperforms the threshold-based protocol. These observations can be explained as follows. When λ_E is small, the reliability performance dominates the overall performance of the transmission. When λ_E is high, the secrecy performance dominates the overall performance.

Finally, we compare the achievable secrecy throughput for different transmission protocols by Figure 4. We present the result achieved by simple transmission without any technique, namely full activity protocol, for comparison. That is, the full activity protocol simply transmit messages all the time without either the threshold-based protocol or the secrecy guard zone. We plot the achievable secrecy throughput versus the secrecy constraint ε and the reliability constraint δ. As shown in the figure, the secrecy guard zone protocol can achieve the non-zero secrecy throughput under more stringent secrecy constraint, compared with the full activity protocol.

The threshold-based protocol can achieve the non-zero secrecy throughput under more stringent reliability constraint, compared with the full activity protocol. Therefore, we summarize the wise choices of different transmission protocols under different conditions as follows. When the secrecy constraint is stringent but the reliability constraint is loose, it is preferable to adopt the secrecy guard zone protocol. When the reliability constraint is stringent but the secrecy constraint is loose, it is preferable to adopt the threshold-based protocol.

VI. Conclusion

In this paper, we studied the secure communication in an underlay CR network with multiple movable eavesdroppers with a HPPP location entity at each snapshot of time. Importantly, the location set of eavesdroppers is assumed unknown at the legitimate side. We considered the scenario where the SU-Tx sends confidential messages to the SU-Rx with an instantaneous power constraint in order not to interfere the PU. To achieve PLS in such a CR network, we proposed two transmission protocols according to different assumptions on the channel knowledge at SU-Tx and the location knowledge about the eavesdroppers. We comprehensively analyzed the transmission delay, secrecy, reliability, and overall performance of each transmission protocol. Moreover, we optimized the design parameters (r or μ) to maximize the secrecy throughput for the proposed transmission protocols. Our results showed that the secrecy guard zone protocol is preferred when the secrecy constraint is stringent and the threshold-based protocol is preferred when the reliability constraint is stringent.

It is worth mentioning that a hybrid transmission protocol can be further developed when the SU-Tx is able to detect the existence of eavesdroppers within its vicinity and obtain the one-bit feedback from the SU-Rx. For the hybrid protocol, the SU-Tx adopts a joint secrecy guard zone and threshold-based transmission strategy. The performance analysis as well as the joint optimal design of such a hybrid protocol can be found in a full version of this work [30].

References

[1] J. Mitola and G. Q. Maguire, "Cognitve radio: Making software radios more personal," *IEEE Personal Commun.*, vol. 6, no. 4, pp. 13–18, Apr. 1999.

[2] Y. T. Hou, A. Wyglinski, M. Nekove, H. Zhang, R. Chandramouli, and F. Martin, "Guest editorial: Special issue on cognitive radio oriented wireless networks and communications," *Moble. Netw. Appl.*, vol. 13, no. 5, pp. 411–415, May 2008.

[3] H. Wen, 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, Mar. 2013.

[4] J. L. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.

[5] X. Zhou, L. Song, and Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, 2013.

[6] M. Bloch and J. Barros, *Physical Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[7] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Achieving cognitive and secure transmissions using multiple antennas," in *Proc. IEEE Int. Symp. Personal, Indoor and Mobile Radio Commun. (PIMRC)*, Singapore, Sep. 2009, pp. 1–5.

[8] ——, "Secure communication over MISO cognitive radio channels," *IEEE Trans. Wirel. Commun.*, vol. 9, no. 4, pp. 1494–1502, Apr. 2010.

[9] Y. Zou, X. Li, and Y.-C. Liang, "Secrecy outage and diversity analysis of cognitive radio systems," *IEEE J. Sel. Areas in Commun.*, vol. 32, no. 11, pp. 2222–2236, Nov. 2014.

[10] C. Wang and H. 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.

[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] H. Sakran, M. Shokair, O. Nasr, S. EI-Rabaie, and A. A. EI-Azm, "Proposed relay selection scheme for physical layer security in cognitive radio networks," *IET Commun.*, vol. 6, no. 16, pp. 2676–2687, 2012.

[13] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *ZTE Commun.*, vol. 11, no. 3, pp. 11–19, Sept. 2013.

[14] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks – Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[15] ——, "Secure communication in stochastic wireless networks – Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.

[16] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Austin, TX, June 2010, pp. 2627–2631.

[17] Z. Shu, Y. Qian, and S. Ci, "On physical layer security for cognitive radio networks," *IEEE Network*, vol. 27, no. 3, pp. 28–33, Mar. 2013.

[18] Y. Q. Z. Shu, Y. L. Yang and R. Q. Hu, "Impact of interference on secrecy capacity in a cognitive radio network," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Houston, TX, USA, Dec. 2011, pp. 1–6.

[19] 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.

[20] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[21] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[22] J. Lee, H. Wang, J. G. Andrews, and D. Hong, "Outage probability of cognitive relay networks with interference constraints," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 390–395, Feb. 2011.

[23] F. Rafael, V. Guimaraes, D. B. da Costa, T. A. Tsiftsis, C. C. Cavalcante, and G. K. Karagiannidis, "Multiuser and multirelay cognitive radio networks under spectrum sharing constraints," *IEEE Trans. Vel. Technol.*, vol. 63, no. 1, pp. 433–439, Jan. 2014.

[24] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE J. Sel. Areas Commun.*, vol. 25, no. 2, pp. 517–428, Apr. 2007.

[25] L. Musavian, S. Aïssa, and S. Lambotharan, "Effective capacity for interference and delay constrained cognitive-radio relay channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 5, pp. 1698–1707, May 2010.

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

[27] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[28] M. Bloch, J. Barros, M. Rodrigues, and S. Mclaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[29] 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. 2013.

[30] 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.