Research Article

Secrecy Cognitive Gain of Cognitive Radio Sensor Networks with Primary Outage Constraint

Hongyu Ma,1,2 Kai Niu,1 Weiling Wu,1 Shengyu Li,1 and Guangqian Chu1

1Key Laboratory of Universal Wireless Communications, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China
2School of Electronic and Information Engineering, Liaoning University of Technology, Jinzhou 121001, China

Correspondence should be addressed to Hongyu Ma; mhy@bupt.edu.cn

Received 19 December 2014; Accepted 1 June 2015

Academic Editor: Antonio Lazaro

Copyright © 2015 Hongyu Ma et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper studies the physical layer security issue for cognitive radio sensor networks (CRSNs) with primary outage constraint, for which a tractable framework is developed to analyze the secrecy performance for CRSNs related to the random channel characteristics, the spatial distributions of nodes, the nearest neighbour routing protocol, and the aggregate interference. Based on stochastic geometry technique, a novel random analysis method is proposed to derive the closed-form expression of secrecy transmission capacity and analyze the connection outage probability (COP) and secrecy outage probability (SOP) for both secondary (SR) and primary (PR) systems. Then, the concept of secrecy cognitive gain is produced to highlight the effect of SR systems with secrecy on the whole networks security. Comparing with a single PR system, the SR system is beneficial to enhance the secrecy level for overlaid CRSNs. In addition, the maximum achievable secrecy capacity is achieved through optimizing the density of SR systems satisfying outage constraints of PR and SR systems. Analytical results provide insights into regimes in which the SR system with secrecy is beneficial for the overlaid network secrecy.

1. Introduction

Wireless sensor networks (WSNs) are now widely used in many contexts of military and civilian applications [1], such as battlefield surveillance, environment monitoring, target detection, and tracking, especially in unattended and possibly hostile areas. All of these applications have resulted in a shortage of spectrum bands with respect to a tremendous demand for radio spectrums. Fortunately, the cognitive radio (CR) technology emerges, which is revealed to be a promising solution to this problem [2]. In cognitive radio networks (CRNs), secondary (SR) users could share the spectrum with primary (PR) users as long as the quality of service (QoS) of the PR network was not disturbed [3].

As a smart integration of WSNs and CRNs, cognitive radio sensor networks (CRSNs) have received a great deal of interest for the characteristic of large-scale and overlaid deployments [4]. In general, a wireless cognitive sensor network consists of sensor nodes equipped with cognitive radio. The transmission performance could be improved by sharing spectrum between primary sensor nodes and secondary sensor nodes, while ensuring that SR nodes can avoid interference with PR users. However, spectrum sharing leads to the security problem of data transmissions since broadcasting messages sent to intended receivers often face the risk of interception by some malicious eavesdroppers. Thus, the secrecy transmission in CRSNs becomes a critical issue.

Traditionally, the security of data transmission has been performed via cryptographic techniques [5] at the network layer. However, complicated encryption algorithms cannot be supported by wireless sensor nodes with limited computing power and storage space. As a powerful complement, the physical layer security has been proposed to achieve perfect secrecy without requiring key distribution and complex encryption/decryption algorithms. The fundamental principle of physical layer security is to exploit intrinsic properties of communication channels to restrict the amount of confidential messages that is possibly intercepted by unauthorized receivers.
In the past few years, physical layer security or information-theoretic security has become a very active area of research. In the seminal work on physical layer security [6], Wyner proposed the wiretap channel model for the point-to-point communication, where Alice transmitted confidential message to Bob and Eve tried to wiretap the message. Subsequently, various wiretap models have been proposed to evaluate the secrecy capacity for different applying scenarios. Csiszar and Kornner and Liang et al. generalized it to broadcast channels and fading channels, respectively, in [7] and [8]. The secure MIMO channel was studied in [9, 10]. The secrecy capacity region of interference channel was presented in [11]. Motivated by emerging wireless applications, there is a growing interest in exploiting the benefits of relay channel to guarantee secure transmissions [12]. However, the majority of these works ignored the spatial distributions of network nodes but only focused on the configurations with a limited number of legitimate users and eavesdroppers.

With respect to the node spatial distribution, stochastic geometry techniques have been a powerful tool to analyze large-scale wireless networks [13]. Further, the Poisson point process (PPP) modeling [14, 15] has been shown to yield tractable results for secrecy performance of wireless networks. The secrecy graph was introduced to investigate the secure connectivity [16]. The work [17] established the secrecy outage probability with and without colluding eavesdroppers in cellular networks. Zhou et al. [18] proposed the concept of secrecy transmission capacity of a single wireless network, and they exploited secrecy guard zone to improve the network throughput. Zhang et al. [19] presented asymptotic analysis of secrecy capacity in large-scale networks and obtained order sense results for the secrecy capacity. Recently, Win et al. [20] show that cognitive interference was beneficial for the security of cognitive networks, while proposing corresponding interference engineering strategies. However, to the best of our knowledge, the exact expression of secrecy capacity has not been obtained for overlaid networks like CRSNs.

The primary goal of this work is to derive the exactly closed-form expression of the secrecy transmission capacity in CRSNs. Related works are [18, 21–25]. Shu et al. [21] characterized the secrecy capacity of PR networks considering a cognitive radio network but only focused on the effect of small-scale fading on the secrecy performance ignoring that of large-scale fading. In [22], the capacity and delay scaling laws were investigated for cognitive radio networks, which only gave an asymptotic prediction on the capacity without an exact expression. Elkashlan et al. [23] studied multiple antennas securing the transmission of the secondary network and presented new closed-form expressions for asymptotic secrecy outage probability. Chae et al. [24] investigated the optimal utilization of artificial noise for secrecy communication with a secrecy protected zone and derived the secrecy transmission rate without CSI of eavesdroppers. Liu et al. proposed four relay and jammer selection policies and derived new closed-form expressions for secrecy outage probability of cognitive DF relay networks [25]. Although Zhou et al. [18] introduced secrecy transmission capacity which quantified the achievable rate of successful transmission of secret message per unit area, this result was only limited in a single network and the distance between transmitter and receiver was simply defined as a fixed value.

The main contributions of this paper can be summarized as follows.

(i) This paper develops a framework for the analysis and design of CRSNs with secrecy in respect of the random channel characteristics, the nearest neighbour routing protocol, the spatial distributions of PR, SR and eavesdropping nodes, and the aggregate interference from intersystem and intrasystem.

(ii) A novel method is proposed to derive closed-form expressions of secrecy transmission capacity of CRSNs under constraints of the connection outage provability (COP) and the secrecy outage probability (SOP), and the maximum achievable secrecy transmission capacity is obtained by optimizing transmission density. The result reveals an insight into the tradeoff between the security of SR system and reliability of PR system.

(iii) The concept of secrecy cognitive gain is first introduced to evaluate the advantageous effect of SR system with secrecy on the secrecy capacity of the whole CRSNs. Compared with a single PR system, the SR system is beneficial to enhance the secrecy level for overlaid CRSNs. In summary, we quantify secrecy cognitive gain and characterize relationship between the secrecy performance and various system parameters.

The rest of this paper is organized as follows. System model and problem formulation are described in Section 2. Outage performance of CRSNs is analyzed in Section 3. The secrecy transmission capacity and secrecy cognitive gain are derived in Section 4. Some numerical results are presented in Section 5. Finally, conclusions are given in Section 6. The notations used in this paper are summarized as follows.

Notations and Description (“of System k” Is Abbreviated, \(k \in \{p, c\}\))

- \(\{p, c\}\): PR system, SR system,
- \(\Phi_k\): PPP of potential transmitters of network \(k\),
- \(P_k^c\): connection outage probability,
- \(P_{so}\): secrecy outage probability,
- \(\lambda_k\): spatial density,
- \(l_k\): transmission distance,
- \(\kappa_k\): target threshold of COP,
- \(\epsilon_k\): target threshold of SOP,
- \(\beta_k\): SIR threshold,
- \(P\): transmission power,
- \(\Phi_{ew}\): PPP of Eaves networks,
- \(\lambda_{ew}\): spatial density of Eaves networks,
- \(\beta_{ew}\): SIR threshold of Eaves networks,
- \(Pr[\cdot]\): probability of an event,
- \(E[\cdot]\): expectation of a random variable.
2. System Model and Problem Formulation

Cognitive radio sensor networks in the presence of eavesdroppers, composed of a number of sensor nodes with cognitive radio function, are divided into PR systems, SR systems, and eavesdropping systems. Network model is depicted in Figure 1 with descriptions as follows.

(i) A PR system consists of legitimate sensor nodes with priority of spectrum access for secure communication.

(ii) A SR system consists of legitimate sensor nodes which are allowed to utilize spectrum resources for secure communication guaranteeing the QoS requirement of PR system.

(iii) An eavesdropping system consists of malicious nodes which attempt to bug the confidential data sent to intended receivers in the PR and SR system.

In CRSNs, a legitimate transmitter (Alice) wants to send a confidential message to a legitimate receiver (Bob), and multiple passive eavesdroppers (Eves) overhear the secret message. Because Alice does not know the channel state information (CSI) before transmission, she sets a constant secrecy transmission rate $R_s$ according to Wyner’s encoding scheme [6], and then the secrecy transmission rate $R_s$ is given by

$$R_s = R_t - R_{e},$$  \hspace{1cm} (1)

where $R_t$ is the transmission rate for the legitimate communication link from Alice to Bob and $R_e$ is the eavesdropping rate for the bugging link from Alice to Eaves.

Spectrum sharing networks are denoted as sets $\Pi_k$, $k \in \{p, c\}$, where $p, c$ represent the primary system and the secondary system, respectively. The legitimate nodes in PR and SR systems are assumed to be randomly distributed according to a Poisson point process (PPP) $\Phi_k$ with density $\lambda_k$, where $\lambda_p$ denotes the density of PR systems and $\lambda_c$ denotes the density of eavesdropping systems.

It is assumed that Eves are not colluded with each other and follow another independent PPP distribution $\Phi_e$ with density $\lambda_e$. All nodes are assumed to have a single antenna and equal transmitting power $P$. Accounting for stochastic geometry techniques, a typical receiver is put at the origin in a two-dimensional plane. Moreover, the large-scale attenuation and the small-scale Rayleigh fading are considered in interference-limited CRSNs, where the thermal noise can be ignored. Hence, the received power can be represented as $Ph_l^{\alpha}$, where $l_k$ denotes the communication distance, $\alpha$ denotes the path loss exponent, and $h$ denotes an exponentially distributed random variable with unit mean. Furthermore, the signal to interference ratio (SIR) of $\Phi_k$ is defined as

$$\text{SIR}_k = \frac{Ph_l^{\alpha}}{I_p + I_c},$$ \hspace{1cm} (2)

where $I_p$ represents the cumulative interference of the PR system and $I_c$ denotes the cognitive interference from the SR system, which leads to a degradation of data transmission for both legitimate links and eavesdropping links.

It is noted that the nearest neighbour routing protocol is considered in SR systems, each SR transmitter selects the nearest node as its intended receiver, and then the communication distance $l_c$ is a random variable with probability density function (PDF)

$$f_{l_c}(l) = 2\pi \lambda_c le^{-\lambda_c l^2}.\hspace{1cm} (3)$$

According to the instantaneous value of SIR at receivers, the capacity of either a legitimate or eavesdropping system is determined based on the encoding scheme [6]. Hence, the outage event in CRSNs can be declared as follows.

(i) Connection outage (CO): the channel capacity of intended communication link is lower than the transmission rate $R_t$, which means that the message from Alice cannot be correctly decoded by Bob.

(ii) Secrecy outage (SO): the channel capacity of at least one Eve is higher than eavesdropping rate $R_e$, which means that the message from Alice can be partially decoded by Eves.

Accounting for the QoS requirement of legitimate link, the data transmission is interrupted when the instantaneous SIR is below the SIR threshold value $\beta_k$ at intended receiver, which leads to a connection outage. In addition, the confidential information will be grabbed by Eves when the received SIR at least one eavesdropping node is greater than a threshold value $\beta_e$, which results in a secrecy outage. Therefore,
the connection outage probability \( P_{to}^k \) and secrecy outage probability \( P_{so}^k \) will be represented as follows, respectively:

\[
\text{COP:} \quad P_r \left[ \text{SIR}_{Bob} < \beta_k \right] \leq \kappa_k, \quad (4)
\]

\[
\text{SOP:} \quad P_s \left[ \max \left| \text{SIR}_{Eve} \right| > \beta_s \right] \leq \epsilon_k, \quad (5)
\]

where \( \kappa_k \) denotes the target COP of system \( k \) and \( \epsilon_k \) represents target SOP of system \( k \). In CRSNs, there are four kinds of outage probability, the COP of PR system (PR-COP), the SOP of PR system (PR-SOP), the COP of SR system (SR-COP), and the SOP of SR system (SR-SOP). Note that the COP describes QoS of message transmission of the legitimate network related on the system reliability, and the SOP represents the security level in the presence of passive eavesdropping.

Furthermore, it is assumed that \( \beta_p \) and \( \beta_s \) are known to Alice because she can arbitrarily select the rates \( R_p \) and \( R_s \) such that \( R_p \leq R_t - R_c \). Thus, the relationship between the SIR threshold and the transmission rate can be represented as follows, respectively:

\[
\beta_p = 2R_t - 1, \quad (6)
\]

\[
\beta_s = 2R_s - 1. \quad (7)
\]

As an overlaid wireless network, the CRSN is considerably complicated due to variety of interference. Exploiting the transmission framework [26], a random analysis method is proposed to analyze the secrecy transmission capacity of CRSNs. In this section, the secrecy transmission capacity is defined as the achievable secrecy rate of successful transmission of secret messages under outage constraints, which is expressed as

\[
\eta = \lambda \left( 1 - \kappa \right) \mathbb{E} \left[ R_i \right], \quad (8)
\]

where \( \lambda \) is the average number of legitimate transmitters per unit area and \( \mathbb{E} \left[ R_i \right] \) denotes the achievable secrecy rate, which is the expected value of secrecy transmission rate over transmission distance. Hence, the unit of \( \eta \) is bit/s/m²/Hz. The achievable secrecy rate will be computed based on the expected value of secrecy communication rate considering the distribution of link transmission distance \( L \). Therefore, the achievable secrecy rate is given as

\[
\mathbb{E} \left[ R_i \right] = \int_0^{+\infty} f_L \left( l \right) R_s, \beta dl, \quad (9)
\]

where \( R_s/l \) is the secrecy transmission rate, which is the function of the TX-RX distance \( L \).

### 3. Outage Performance Analysis

It is essential to evaluate COP and SOP of CRSNs to perform the security capacity analysis. Therefore, connection outage probabilities of the PR and SR system are derived in this section, and then secrecy outage probabilities are achieved for CRSNs. Details of outage performance analysis are given in the following lemmas.

#### 3.1. Connection Outage Probability

**Lemma 1.** The COPs of the PR and CR system are given by

\[
P_{to}^k = 1 - \exp \left\{ -\eta_k^2 \left( \lambda_p + \lambda_s \right) \right\}, \quad (10)
\]

where \( \eta_k = C(\alpha)p_k^{2/\alpha}, \quad k \in \{ p, c \}, \) and \( C(\alpha) = \frac{(2\pi/a)}{\sin(2\pi/a)} \).

**Proof.** According to Slivnyak’s theory [27], the SIR (2) at the typical receiver of system \( k \) can be rewritten as follows:

\[
\text{SIR}_k = \frac{P_{h_1}(l_k)^{-\alpha}}{\sum_{i \in \Phi_p} P_{h_1}|x_i|^{-\alpha} + \sum_{j \in \Phi_c} P_{h_1}|x_j|^{-\alpha}}, \quad (11)
\]

where \( |x_i| \) and \( |x_j| \) represent the distance from nodes \( i \) and \( j \) to the origin in the PR system and SR system, respectively. Hence, the connection outage probability of system \( k \) is

\[
P_{to}^k = 1 - \Pr \left\{ \text{SIR}_k > \beta_k \right\} = 1 - \Pr \left\{ h > l_k^{-\alpha} \beta_k \left( I_p + I_s \right) \right\} = 1 - \Phi_{t_p} \left( l_k^{-\alpha} \beta_k \right) \Phi_{t_s} \left( l_k^{-\alpha} \beta_k \right), \quad (12)
\]

where

\[
I_p = \sum_{i \in \Phi_p} h_t |x_i|^{-\alpha}, \quad (13)
\]

and \( \Phi_{t_p}(s) \) and \( \Phi_{t_s}(s) \) denote the Laplace transform of the probability density function (PDF) for the interference of the PR system and SR system, respectively. Applying Campbell’s theorem [27], the following expressions are obtained:

\[
\phi_{t_p}(s) = \exp \left( -\lambda_p s^{2/\alpha} \pi C(\alpha) \right), \quad \phi_{t_s}(s) = \exp \left( -\lambda_s s^{2/\alpha} \pi C(\alpha) \right). \quad (14)
\]

From a cognitive point of view, since the PR system has higher priority to access the spectrum, the SR system will control its density to guarantee the QoS of the primary system. In other words, the density of SR systems \( \lambda_s \) is limited by the COP of PR systems. Accounting for the outage constraint (4), the following expression can be achieved from (10) in PR systems:

\[
\lambda_c \leq \frac{\ln \left( 1/(1 - \kappa_p) \right)}{C(\alpha) \beta_p^{2/\alpha} - \lambda_p}. \quad (15)
\]

Note that the outage probability \( P_{to}^k \) of CRSNs is a function of the random variable \( l_k \). In practical network design, the outage probability is determined by the spatial distribution of transmission distance \( l_k \). □
3.2. Secrecy Outage Probability

Lemma 2. The SOP of legitimate nodes in CRSNs is given by

\[ P_{so} = 1 - \exp \left( -\frac{\lambda_c}{(\lambda_p + \lambda_c)\beta_c^{2\alpha}C(\alpha)} \right) \].  \hspace{1cm} (16)

**Proof.** All eavesdropping nodes in the CRSN are randomly and independently distributed, and the SOP can be evaluated by inspecting a typical wiretap link. Using the similar analysis adopted in Lemma 1, the eavesdropping probability of arbitrary wiretap link is found as

\[ \Pr \{ \text{SIR}_c > \beta_c \} = \exp \left( -\pi C(\alpha) I_t^{2/\alpha} \left( \lambda_p + \lambda_c \right) \right). \]  \hspace{1cm} (17)

The eavesdropping event occurs when the maximum of received SIRs for all eavesdroppers is greater than the threshold \( \beta_c \). Hence, the SR-SOP is derived as follows:

\[
P_{so} = 1 - \Pr \left\{ \max_{e \in \Phi_c} \{ \text{SIR}_c < \beta_c \} \right\} \\
= (a) \quad 1 - \mathbb{E}_{\Phi_c} \left\{ \prod_{e \in \Phi_c} \Pr \{ \text{SIR}_c < \beta_c \} \right\} \\
= 1 - \mathbb{E}_{\Phi_c} \left\{ \prod_{e \in \Phi_c} \left\{ 1 - \Pr \{ \text{SIR}_c > \beta_c \} \right\} \right\} \\
= (b) \quad 1 - \exp \left\{ -\lambda_c \int_{\beta_c}^{\infty} \Pr \{ \text{SIR}_c > \beta_c \} \, dr \right\} \\
= 1 - \exp \left\{ -\lambda_c \beta_c^{2\alpha} \int_{0}^{\infty} \Pr \{ \text{SIR}_c > \beta_c \} \, r \, dr \right\} ,
\]

where (a) follows the independent distribution of eavesdroppers and (b) follows the probability generating functional (PGFL) of the Poisson point process [28]. Substituting (17) into (18), the closed-form expression of the SOP is obtained easily. From Lemma 2, it can be observed that the secrecy outage performance of legitimate nodes depends on system parameters such as the densities of PR, SR, and eavesdropping nodes, the threshold value of eavesdropping SIR, and path loss exponent.

Integrating (5) with (16), it is easy to obtain that the SR density \( \lambda_c \) is limited by the following condition for SR system:

\[ \lambda_c \geq \frac{\lambda_c}{\ln(1/(1 - \epsilon_c))\beta_c^{2\alpha}C(\alpha) - \lambda_p}. \]  \hspace{1cm} (19)

4. Secrecy Transmission Capacity and Secrecy Cognitive Gain

In this section, the secrecy transmission rate is first analyzed for both PR and SR systems in the presence of eavesdroppers, and then the closed-form secrecy transmission capacity of CRSNs is derived. It has been focused on the evaluation of secrecy transmission capacity of SR systems, in which the nearest neighbour routing protocol is adopted. For the convenient analysis of secrecy cognitive gain, secrecy transmission capacity of PR systems at a given transmission distance is also evaluated. Finally, the secrecy cognitive gain is proposed to evaluate the beneficial effect of SR system with secrecy on the CRSN.

**Theorem 3.** The secrecy transmission rate of network \( k \) in CRSNs is given by

\[ R_{k}^t = \frac{\alpha}{2} \log_2 \left[ A_k \beta_c^{-2} \right] . \]  \hspace{1cm} (20)

**Proof.** Exploiting (4) and (6), it can be observed that the transmission rate \( R_t \) is determined by the target threshold value of COP \( \kappa \). The 

**Theorem 4.** The secrecy transmission capacity of the PR system in CRSNs is given by

\[ C_{p} = \frac{\alpha \lambda_p}{2} \log_2 A_p, \]  \hspace{1cm} (23)

**Proof.** Taking the distance between the primary transmitter and intended receiver as \( l_p = 1 \), we obtain the achievable secrecy rate of the PR network by combining (20) with (9):

\[ \mathbb{E}[R_1] = \frac{\alpha}{2} \log_2 A_p. \]  \hspace{1cm} (24)

From (8), it is easy to obtain the secrecy transmission capacity of the PR system.
In PR systems, the successful transmission of confidential data for an intended receiver is limited by two constraints, PR-COP and PR-SOP. The limitations on density of PR systems can be deduced from outage constraints of (4) and (5), respectively. Combining (4) with (10), the density of PR systems $\lambda_p$ is limited as follows:

$$\lambda_p \leq \frac{\ln \left(1/(1 - \kappa_p)\right)}{C(\alpha) \beta_p^{2\alpha}} - \lambda_c. \quad (25)$$

Integrating (5) with (16), another density limitation for PR systems $\lambda_p$ is written as follows:

$$\lambda_p \geq \frac{\lambda_c}{\ln \left(1/(1 - \epsilon_p)\right) \beta_p^{2\alpha} C(\alpha)} - \lambda_c. \quad (26)$$

**Corollary 5.** The condition of positive secrecy transmission capacity for PR systems is given by

$$\pi \lambda_c < \ln \left(1 - \kappa_p\right) \ln \left(1 - \epsilon_p\right). \quad (27)$$

**Proof.** It is easy to obtain the condition under which positive secrecy transmission capacity exists by solving $\eta_p > 0$, which coincides with the result in [18] in respect of a fixed transmission distance. It reveals that positive secrecy transmission capacity is achieved when the number of eavesdroppers within unit distance $l_p = 1$ is less than $\ln(1 - \kappa_p) \ln(1 - \epsilon_p)$. $\square$

### 4.2 Secrecy Transmission Capacity of SR Systems

The secrecy transmission capacity of SR systems is derived on the base of the result of the secrecy rate, and the effect of the PR-COP and the SR-SOP on the secrecy transmission capacity is illustrated in this section. Note that the nearest neighbour routing protocol is considered in SR networks. Furthermore, the SR density $\lambda_c$ is optimized to maximize the secrecy transmission capacity of SR systems.

**Theorem 6.** The secrecy transmission capacity for the SR system in CRSNs is given by

$$\eta_c = \frac{\alpha \lambda_c}{2} \left(1 - \kappa_c\right) \left[e^{-\pi \lambda_c \log_2 A_c} + \frac{1}{\ln 2} E_i(-\pi \lambda_c)\right], \quad (28)$$

where $A_c = \ln(1 - \kappa_c) \ln(1 - \epsilon_c) / \pi \lambda_c$.

**Proof.** Plugging (3) and (20) into (9), the achievable secrecy rate of SR system in CRSNs is derived as

$$E[R_i] = \int_0^\infty 2\pi \lambda_c e^{-\pi \lambda_c l^2/2} \alpha \log_2 [A(l^2)] dl$$

$$\overset{(a)}{=} \alpha \pi \lambda_c \left[\int_1^\infty le^{-\pi \lambda_c l^2} \log_2 A_c dl\right]$$

where (a) meets the distance limitation $l > 1$. Here, a closed-form expression of the secrecy transport throughput is presented under the case of $l > 1$, which is achievable in practical applications, and (b) follows a kind of variable substitution; that is, $s = \pi \lambda_c l^2$. Considering the definition of exponential integral function [29], that is, $E_i(-x) = \int_x^\infty e^{-t/t} dt$, the secrecy transmission capacity (28) is achieved by integrating (29) with (8).

It is shown that the secrecy transmission capacity is primarily determined by the SR transmission density $\lambda_c$, the COP $\kappa_c$, and the SOP $\epsilon_c$. Moreover, the condition under which positive secrecy transmission capacity exists can be found.

**Corollary 7.** The condition of positive secrecy transmission capacity of SR systems is given by

$$\pi \lambda_c < \ln \left(1 - \kappa_p\right) \ln \left(1 - \epsilon_p\right). \quad (30)$$

where $Z = -E_i(-\pi \lambda_c) / (\ln 2 \cdot e^{-\pi \lambda_c})$.

**Proof.** This result is obtained by solving $\eta_k > 0$.

The above condition gives a tradeoff between the QoS and the security level for a given $\lambda_c$. And the feasible range of $\kappa_c$ can be found from (30) as

$$\kappa_c \in \left(1 - \exp\left[\frac{\pi \lambda_c Z^2}{\ln(1 - \epsilon_c)}\right], 1\right). \quad (31)$$

From (28), the secrecy transmission capacity of the SR system mainly depends on the SR density. Now, the problem of finding the optimal secondary density $\lambda^*_c$ maximizing the achievable secrecy capacity can be given under constraints of the PR-COP and the SR-SOP as

$$\arg \max_{\lambda_c} \eta_c,$$

s.t. $p^P_{in} < \kappa_p$, \hspace{1cm} (32)

$p^P_{so} < \epsilon_c$.

Subject to the aforementioned outage constraints, the feasible range of the SR density is given as

$$\lambda_c \in [\lambda_{c1}, \lambda_{c2}], \quad (33)$$
where \( \lambda_{c1} \) is the optimal \( \lambda_c \) satisfying the PR-COP given in (19) and \( \lambda_{c2} \) is the greatest \( \lambda_c \) meeting the SR-SOP in (15). Moreover, it is easy to see that the following inequality is valid when \( \lambda_{c1} < \lambda_{c2} \):

\[
\lambda_c < \frac{\ln (1 - \kappa_p) \ln (1 - \varepsilon_c)}{(\beta_p/\beta_s)^{n/2}}. \tag{34}
\]

**Corollary 8.** The optimal value of \( \lambda_c \) that maximizes \( \eta_c \) under constraints of PR-COP and SR-SOP is given by

\[
\lambda_c^* = \frac{1}{\pi \ln 2 \log_2 A_c}. \tag{35}
\]

**Proof.** The objective function \( f(\lambda_c) = \eta_c \) shows the tradeoff between the spatial density and the outage probability. In particular, the objective function has the characteristics of \( f(\lambda_c)' = 0 \) when \( \lambda_c = \lambda_c^* \) and \( f(\lambda_c)'' < 0 \) when \( n \lambda_c < \ln (1 - \kappa_c) \ln (1 - \varepsilon_c) \) which is achievable considering the limitation of the positive secrecy capacity (30), where \( f(\cdot)' \) and \( f(\cdot)'' \) are the first derivative and the second derivative of the function. \( \square \)

**Remark 9.** Using the optimal spatial density of SR systems, the maximum achievable secrecy transmission capacity of the SR systems is defined as \( \eta^* = (\alpha \lambda_p^*/2)(1 - \kappa_p)[e^{-\pi \lambda_c^* \log_2 A_c} + (1/\ln 2)E_i(\pi \lambda_c^*)] \).

**Corollary 10.** The achievable density of \( \lambda_c \) meeting constraints of positive secrecy transmission, PR-COP, and SR-SOP, is given by

\[
\lambda_c^* = \min \{ \lambda_{c1}, \lambda_{c2} \}, \tag{36}
\]

where \( \lambda_{c1} = \ln (1 - \kappa_c) \ln (1 - \varepsilon_c)/(\pi \cdot 2^2) \) and \( \lambda_{c2} = \ln (1 - \kappa_p) \ln (1 - \varepsilon_c)/(\beta_p/\beta_s)^{n/2} \).

**Proof.** From (30) and (34), we can easily see that \( \lambda_{c1} \) is the greatest value of \( \lambda_c \) meeting the condition of a positive secrecy capacity, and \( \lambda_{c2} \) is the peak of \( \lambda_c \) subject to the PR-COP and SR-SOP. Hence, \( \lambda_c^* = \lambda_{c1} \) if \( \lambda_{c1} < \lambda_{c2} \), and \( \lambda_c^* = \lambda_{c2} \) if \( \lambda_{c2} < \lambda_{c1} \).

**Remark 11.** Now, we provide a new perspective on the constraint of security level based on the density of eavesdroppers. Obviously, the secrecy transmission will be disrupted if \( \lambda_c > \lambda_c^* \). From the unimodality of (28), \( \eta_c \) decreases monotonously with \( \lambda_c \). Therefore, \( \lambda_c^* \) is the maximum value of \( \lambda_c \) minimizing the secrecy transmission capacity when other system parameters are given.

4.3. Secrecy Cognitive Gain. In this section, the concept of secrecy cognitive gain is proposed to quantify the improvement of security level generated from SR systems. And it is defined as the secrecy capacity ratio between the sum of capacities for CRSNs with secrecy and the secrecy capacity of a single PR system, which is given by

\[
\theta = \frac{\eta_{sum}}{\eta_{sp}} \tag{37}
\]

where \( \eta_{sum} \) denotes the sum of secrecy capacities and \( \eta_{sp} \) denotes the secrecy capacity of a single PR system.

Based on the analysis of secrecy transmission capacity in above sections, the sum of capacities for CRSNs is denoted as the sum of secrecy capacity between PR systems and SR systems, which is given as

\[
\eta_{sum} = \eta_p + \eta_c. \tag{38}
\]

To simplify analysis, we study a special case of \( \varepsilon_p = \varepsilon_c \) and \( \kappa_p = \kappa_s \) and derive the closed-form expression of the secrecy cognitive gain.

**Theorem 12.** The secrecy cognitive gain of CRSNs is given by

\[
\theta = 1 + \frac{\lambda_c}{\lambda_p} \left[ e^{-(1+\kappa_p)} \ln(1 - \kappa_p) + E_i(\pi \lambda_c) \right]. \tag{39}
\]

**Proof.** Taking into account a single PR system in the absence of the SR system, the secrecy capacity \( \eta_{sp} \) can be found from the result of [18], which is given by

\[
\eta_{sp} = \frac{\alpha \lambda_p}{2} (1 - \kappa_p) \ln^2 A_{sp}, \tag{40}
\]

where \( A_{sp} = \ln (1 - \kappa_p) \ln (1 - \varepsilon_p)/\pi \lambda_c \).

Substituting (23) and (28) into (38), we achieve the following expressions:

\[
\eta_{sum} = \frac{\alpha \lambda_c}{2} (1 - \kappa_p) \left[ e^{-(1+\kappa_p)} \ln^2 A_{c} + \frac{1}{\ln 2} E_i(\pi \lambda_c) \right] \tag{41}
\]

Assuming that the SOP and COP between PR and SR networks are equal, \( \varepsilon_p = \varepsilon_c \), \( \kappa_p = \kappa_s \), we obtain the secrecy cognitive gain (39) by plugging (40) and (41) into (37).

From Theorem 12, it can be reflected that the presence of SR system is beneficial for the improvement of secrecy capacity of CRSNs compared with the secrecy capacity of a single PR system.

In practice network design, these system parameters including the COP, the SOP, and spatial transmission density could be under the control of the system designer. The derived closed-form expressions of secrecy transmission capacity and secrecy cognitive gain are helpful for design and optimization for CRSNs respecting security. \( \square \)

5. Numerical Results and Analysis

In this section, numerical results are presented to characterize the secrecy transmission performance, such as the secrecy
transmission capacity, the secrecy outage probability, and the secrecy cognitive gain. The path loss exponent $\alpha$ is set as 4 and the transmission power is set as 1.

Figure 2 quantifies the secrecy transmission capacity of SR systems versus the SR density $\lambda_c$ for various secrecy outage probabilities. The secrecy capacity of SR systems is shown as a function of the density $\lambda_c$. And clearly, there exists an optimal $\lambda_c$ maximizing the secrecy transmission capacity. These figures verify analytical results in Corollary 7. Comparing between the four curves, it can be seen that the gap in $\eta_c$ between $\varepsilon_c = 0.2$ and $\varepsilon_c = 0.3$ becomes relatively small than that between $\varepsilon_c = 0.01$ and $\varepsilon_c = 0.02$. It reveals that the cost of secrecy capacity increases significantly as the security requirement becomes higher in the SR system.

Figure 3 presents the secrecy transmission capacity of SR systems versus the SR-COP $\kappa_c$ with different secrecy outage probabilities. It can be seen that there exists an optimal $\kappa_c$ maximizing the secrecy transmission capacity. At the same time, the feasible working range of $\kappa_c$ never comes to 0, which conforms with the result in (31). It also can be found that the minimum value of $\kappa_c$ achieving positive transmission capacity increases as $\varepsilon_c$ decreases. It reflects that there should be a tradeoff between the transmission reliability and the security. In addition, the optimal value of SR-COP $\kappa_c$, maximizing the secrecy transmission capacity, increases as the secrecy outage probability $\varepsilon_c$ decreases. It shows the reliability of SR networks is increased at the cost of sacrificing the secure performance. Therefore, when the design of secure SR systems targets a higher secrecy level, the QoS of SR systems needs to be reduced.

Figure 4 compares secrecy connection probability (SNP) versus the achievable eavesdropping density $\lambda^*_e$ with different values of $\lambda_{e1}$ and $\lambda_{e2}$, where SNP is the complementary function of SOP. The figure shows that SNP monotonically decreases as $\lambda^*_e$ increases. It indicates that the secrecy connection performance cuts down when the achievable density of eavesdroppers increases. We also observe that an interesting fact SNP always grows when $\kappa_p$ rises for both cases of $\lambda_{e1}$ and $\lambda_{e2}$. It reflects that the security performance of SR systems can be improved dramatically by degrading the QoS of PR systems. This result is benefit for the flexible adjustment of the security performance of CRNs.

Figure 5 characterizes secrecy cognitive gain $\theta$ versus the PR density $\lambda_p$ for different SR densities. As shown in this figure, secrecy cognitive gain $\theta$ decreases with $\lambda_p$ and finally
The authors declare that there is no conflict of interests for physical layer security.

expected to provide more accurate performance assessment when multiple antennas and eavesdroppers are colluding, which is a more general scenario where receivers are equipped with multiple antennas. Therefore, the security of SR systems. Future work could extend to there exists a tradeoff between the reliability of PR systems and the security of SR systems. COP and SR-SOP. In addition, the nearest neighbour routing protocol is considered in SR systems. Comparing with a single PR system, the SR system with secrecy is beneficial to enhance the secrecy level of whole CRSNs. Numerical results show that there exists a tradeoff between the reliability of PR systems and the security of SR systems. Future work can extend to a more general scenario where receivers are equipped with multiple antennas and eavesdroppers are colluding, which is expected to provide more accurate performance assessment for physical layer security.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

6. Conclusions

This paper investigates the physical layer security problem in cognitive radio scenario with wireless sensors. A novel random analysis method is presented to derive secrecy performance metrics, such as the connection outage provability (COP), the secrecy outage probability (SOP), the secrecy transmission capacity, and the secrecy cognitive gain. Specifically, the optimal density of SR systems, maximizing the secrecy transmission capacity via stochastic geometry analysis, is achieved whilst guaranteeing constraints of the PR-COP and SR-SOP. Hence, the densities of PR and SR systems should be carefully controlled for guaranteeing reliability and security of CRSNs.

Acknowledgments

This work is supported by National Natural Science Foundation of China (61171099), National High Technology Research and Development Program of China (863 Program) (2015AA011303), and Huawei Technologies Co. Ltd. Project (YB2013120018).

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, 2002.
[2] S. Haykin, “Cognitive radio: brain-empowered wireless communications,” IEEE Journal on Selected Areas in Communications, vol. 23, no. 2, pp. 201–220, 2005.
[3] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, “Breaking spectrum gridlock with cognitive radios: an information theoretic perspective,” Proceedings of the IEEE, vol. 97, no. 5, pp. 894–914, 2009.
[4] O. B. Akan, O. B. Karli, and O. Ergul, “Cognitive radio sensor networks,” IEEE Network, vol. 23, no. 4, pp. 34–40, 2009.
[5] J. L. Massey, “An introduction to contemporary cryptography,” Proceedings of the IEEE, vol. 76, no. 5, pp. 533–549, 1988.
[6] A. D. Wyner, “The wire-tap channel,” The Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, 1975.
[7] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339–348, 1978.
[8] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2470–2492, 2008.
[9] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” IEEE Transactions on Information Theory, vol. 55, no. 6, pp. 2547–2553, 2009.
[10] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas—part II: the MIMOME wiretap channel,” IEEE Transactions on Information Theory, vol. 56, no. 11, pp. 5515–5532, 2010.
[11] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates, “Discrete memoryless inference and broadcast channels with confidential messages: secrecy rate regions,” IEEE Transactions on Information Theory, vol. 56, no. 6, pp. 2493–2507, 2008.
[12] L. Lai and H. El Gamal, “The relay-eavesdropper channel: cooperation for secrecy,” IEEE Transactions on Information Theory, vol. 54, no. 9, pp. 4005–4019, 2008.
[13] A. Rabbachin, T. Q. S. Quek, H. Shin, and M. Z. Win, “Cognitive network interference,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 2, pp. 480–493, 2011.
[14] P. C. Pinto and M. Z. Win, “Communication in a poisson field of interferers—part I: interference distribution and error probability,” IEEE Transactions on Wireless Communications, vol. 9, no. 7, pp. 2176–2186, 2010.
[15] P. C. Pinto and M. Z. Win, “Percolation and connectivity in the intrinsically secure communications graph,” IEEE Transactions on Information Theory, vol. 58, no. 3, pp. 1716–1730, 2012.
[16] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, “Stochastic geometry and random graphs for the analysis and design of wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 27, no. 7, pp. 1029–1046, 2009.
[17] J. Bai, X. F. Tao, J. Xun, and Q. M. Cui, “The secrecy outage probability for the ith closest legitimate user in stochastic networks,” *IEEE Communications Letters*, vol. 18, no. 7, pp. 1230–1233, 2014.

[18] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, “On the throughput cost of physical layer security in decentralized wireless networks,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 8, pp. 2764–2775, 2011.

[19] J. B. Zhang, L. Y. Fu, and X. B. Wang, “Asymptotic analysis on secrecy capacity in large-scale wireless networks,” *IEEE Transactions on Networking*, vol. 22, no. 1, pp. 66–79, 2014.

[20] M. Z. Win, A. Rabbachin, J. Lee, and A. Conti, “Cognitive network secrecy with interference engineering,” *IEEE Network*, vol. 28, no. 5, pp. 86–90, 2014.

[21] Z. Shu, Y. Yang, Y. Qian, and R. Q. Hu, “Impact of interference on secrecy capacity in a cognitive radio network,” in *Proceedings of the Global Telecommunications Conference*, Houston, Tex, USA, December 2011.

[22] Y. Li, X. Wang, X. Tian, and X. Liu, “Scaling laws for cognitive radio network with heterogeneous mobile secondary users,” in *Proceedings of the IEEE INFOCOM*, pp. 46–54, Orlando, Fla, USA, March 2012.

[23] M. Elkashlan, L. F. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, “On the security of cognitive radio networks,” *IEEE Transactions on Vehicular Technology*, 2014.

[24] 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 Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, 2014.

[25] Y. W. Liu, L. F. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, “Relay selection for security enhancement in cognitive relay networks,” *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 46–49, 2015.

[26] S. P. Weber, X. Y. Yang, J. G. Andrews, and G. de Veciana, “Transmission capacity of wireless ad hoc networks with outage constraints,” *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4091–4102, 2005.

[27] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*, John Wiley & Sons, Chichester, UK, 1995.

[28] M. Franceschetti and R. Meester, *Random Networks for Communication: From Statistical Physics to Information Systems*, Cambridge University Press, 2007.

[29] G. B. Arfken, H. J. Weber, and F. E. Harris, *Mathematical Methods for Physicists: A Comprehensive Guide*, Academic Press, New York, NY, USA, 2011.