A Novel Framework for Achievable Secrecy Throughput of Distributed Cognitive Radio Wireless Networks

Hongyu Ma[1,2] and Kai Niu[1]
[1] Key Laboratory of Universal Wireless Communication, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] School of Electronic and Information Engineering, Liaoning University of Technology, Jinzhou 121001, China
Email: {mhy, niukai}@bupt.edu.cn

Abstract —The achievable secrecy throughput of the distributed cognitive radio wireless networks (DCRWNs) is investigated in this paper. The related works on the secrecy performance mainly focus on the average value depending on nodes spatial distribution. However, these results neglect the effect of nodes location on the performance discrepancies. To break this bottleneck, a new framework is developed to derive a closed-form expression of the achievable secrecy throughput for the secondary network under the outage constraint of the primary network. Moreover, the nearest routing protocols is considered. Through the stochastic geometry analysis, it is shown that the new framework highlights the performance discrepancy resulting from spatial distribution. Besides, we derive the optimal value of connection outage probability of the SR network maximizing the successful transmission probability for DCRWNs.

Index Terms—Physical layer security, stochastic geometry, cognitive radio wireless network, achievable secrecy throughput

I. INTRODUCTION

As an effective way to improve the utilization of the wireless spectrum, cognitive radio (CR) technique has attracted more and more attention. In cognitive radio networks (CRNs), secondary (SR) users are allowed to share the licensed spectrum with primary (PR) users as long as the data transmission of PR users is guaranteed [1]. In cognitive radio scenarios, the confidential data of PR networks is easy to be intercepted by some malicious eavesdroppers considering the broadcasting characteristic of a random wireless channel. So, the security of data transmission has become an increasingly important issue in CRNs.

Traditionally, the security of transmitting message has been achieved via cryptographic algorithms [2] at the network layer. But, complicated encryption algorithms can not be supported by wireless networks with limited resource, and the implementation of secrecy at high layers is liable to suffer potential attacks. As a powerful complement, the physical layer security has attracted a growing of attention since the seminal work of Wyner [3], where he proposed the wiretap channel model for the point-to-point communication. Subsequently, various wiretap channel models have been proposed to evaluate the secrecy performance [4]-[9]. However, the majority of these works has focused on the configurations in a system with a limited number of legitimate users and eavesdroppers.

In view of the spatial distribution of random nodes, stochastic geometry tools [10]-[11] have been a powerful tool to analyze the secrecy performance of large-scale wireless networks. The authors [12] introduced secrecy transmission capacity which quantified the achievable rate of successful transmission of secret message per unit area, but this result was only limited in a single network and the distance between transmitter and receiver was simply defined as a fixed value. H. Wang *et al*. [13] investigated the secrecy performance in large-scale cellular networks, and provided tractable results and approximations to characterize the secrecy rate. Bai and Tao *et al*. [14] presented the exact expression of secrecy outage probability for a stochastic network, but they didn't consider the impact of aggregate interference. Recently, it has been proposed that cognitive interference can benefit network secrecy [15].

The aforementioned works evaluating network security performance focus on the spatial averaging which can be attributed to the tractability using stochastic geometry tools. However, these spatial average schemes can only present some kinds of average metrics referring to overall nodes without capability of evaluating performance discrepancies caused by random distribution of nodes with different spatial locations.

In order to overcome the aforementioned limitation, a new framework is developed to provide a more comprehensive description for the networks secrecy performance accounting for nodes spatial distribution, instead of just spatial average. The main contributions of this paper are summarized as follows.

- A new model is presented to analyze secrecy transmission performance respected of the random channel characteristics, nearest neighbor routing protocol, nodes spatial distributions and aggregate interference.
- Compared with ergodic secrecy rate, achievable secrecy rate can be employed to characterize

Manuscript received March 9, 2015; revised June 24, 2015.
This work is supported by National Natural Science Foundation of China (61171099), National High Technology Research and Development Program of China (863 Program) (2015AA011303).
Corresponding author email: mhy@bupt.edu.cn.
doi:10.12720/jcm.10.6.403-409

performance discrepancy resulting from spatial distribution.

- Using this framework, the achievable secrecy throughput of a SR network is presented under constraints of the connection outage provability (COP) of the PR network and the secrecy outage probability (SOP) of the SR network.

The rest of this paper is organized as follows. System model and problem statement are described in Section 2. Then, we analyze COP of DCRWNs and the achievable secrecy throughput of SR networks in Section 3 and Section 4, respectively. Numerical results are presented in Section 5, and conclusions are given in Section 6. The notations used in this paper are summarized in Table I.

TABLE I: LIST OF NOTATION

Notation	Description ('of network k ' is abbreviated, $k \in \{p,c,e\}$)
{p, c, e}	PR network, SR network, and Eaves network
Π_k	Set of network k
Φ_k	PPP of network k
λ_k	Spatial density
l_k	Distance between the transmitter and receiver
β_k	SIR threshold
β_{ep}	Eavesdropping SIR threshold of PR network
β_{ec}	Eavesdropping SIR threshold of SR network
P_{to}^k	Connection outage probability of network k
P_{st}^k	Successful transmission probability of network k
P_{so}^k	Secrecy outage probability of network k
$\bar{P}_{to}$	Ergodic connection outage probability of SR network
$\vec{P}_{st}$	Achievable STT of SR network
$\vec{P}_{so}$	Achievable secrecy outage probability of SR network
κ_k	Target threshold of COP for network k
ε_k	Target threshold of SOP for network k
P_{cov}	Secrecy outage coverage probability of SR network
δ	Target threshold of P_{cov}
η	Achievable secrecy throughput of SR network
P	Transmission power of every transmission link

II. SYSTEM MODEL AND PROBLEM STATEMENT

A. System Model

We consider a distributed cognitive scenario in the presence of eavesdroppers. A distributed cognitive radio wireless networks (DCRWNs) is divided into the primary (PR) network, the secondary (SR) network and the eavesdropping network. The PR network consists of legitimate users with priority of spectrum access for secure communication. The SR network is composed of cognitive users which are allowed to utilize spectrum resources for secure communication guaranteeing the quality of service (QoS) requirement of PR users. The eavesdropping network consists of malicious nodes which attempt to bug the confidential message sending to intended receivers of legitimate networks.

In DCRWNs, a legitimate transmitter (Alice) wants to send a confidential message to a legitimate receiver (Bob) in SR networks, 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 [3]. Then, the secrecy transmission rate of a legitimate link R_s is given by

$$R_s = R_t - R_e \tag{1}$$

where R_t denotes the transmission rate for the legitimate communication link from Alice to Bob, R_e represents the eavesdropping rate for the bugging link from Alice to Eaves.

The spectrum sharing network is denoted as a set Π_k, $k \in \{p,c,e\}$, where p, c and e represent the primary network, secondary network and eavesdropping network, respectively. The random nodes of DCRWNs are assumed to be distributed independently according to a Poisson point process (PPP) Φ_k with density λ_k, $k \in \{p,c,e\}$, where λ_p, λ_c and λ_e denote the density of PR networks, SR networks and eavesdropping networks, respectively. Every transmitter is assumed to have a single antenna and equal transmitting power P. According to Slivnyak's theory of stochastic geometry approaches [16], a typical receiver is placed at the origin in a two-dimensional plane. Moreover, a propagation channel with path loss and Rayleigh fading is considered in interference-limited DCRWNs. Thus, the thermal noise can be ignored. The received power at a typical receiver can be defined as $Phl_k^{-\alpha}$, where h has an exponential distribution with unit mean, i.e., $h \sim exp(1)$, l_k represents the link distance between the transmitter and intended receiver of network k, α denotes the path loss exponent. Furthermore, the signal to interference ratio (SIR) of Φ_k is

$$SIR_k = \frac{Phl_k^{-\alpha}}{I_p + I_c} \tag{2}$$

where I_p represents the cumulative interference of the PR network, and I_c denotes the cognitive interference from the SR network.

It is noted that the nearest neighbor routing protocol is considered in SR networks. Each SR transmitter selects the nearest node as its intended receiver. Then, the cumulative distribution function (CDF) of l_c denotes as

$$F_{l_c}(l) = 1 - e^{-\pi\lambda_c l^2} \tag{3}$$

B. Problem Statement

On the base of the encoding scheme [2], the transmission rate R_i, $i \in \{s,t,e\}$ is determined by the threshold value of SIR at the intended receiver.

$$R_i = log_2(1+\beta_k) \tag{4}$$

where β_k denotes the SIR threshold depending on the outage probability. Outage events in DCRWNs are declared as follows:

- Connection outage **(CO)**: The connection outage happens when the instantaneous SIR is below the SIR threshold value at intended receiver, which means the message from Alice can't be correctly decoded by Bob.
- Secrecy outage **(SO)**: The secrecy outage happens when the received SIR at least one eavesdropping node is greater than a threshold value, which means the message from Alice can be partially decoded by Eves.

In DCRWNs, there are four kinds of outage probability: the COP of PR network (PR-COP), the SOP of PR network (PR-SOP), the COP of SR network (SR-COP) and the SOP of SR network (SR-SOP), which are represented as follows, respectively.

$$\textbf{\textit{PR-COP}}: P_{to}^{p} = P_r\{SIR_p < \beta_p\} \le \kappa_p \tag{5}$$

$$\textbf{\textit{PR-SOP}}: P_{so}^{p} = P_r\{max\{SIR_e\} > \beta_{ep}\} \le \varepsilon_p \tag{6}$$

$$\textbf{\textit{SR-COP}}: P_{to}^{c} = P_r\{SIR_c < \beta_c\} \le \kappa_c \tag{7}$$

$$\textbf{\textit{SR-SOP}}: P_{so} = P_r\{max\{SIR_e\} > \beta_{ec}\} \le \varepsilon_c \tag{8}$$

where κ_p denotes the target PR-COP, κ_c denotes the target SR-COP, ε_p represents the target SR-SOP, and ε_c represents the target SR-SOP.

Note that the COP describes QoS of the message transmission in the legitimate network related on the system reliability, and the SOP represents the security level in the presence of passive eavesdropping. Recalling the aforementioned analysis for achievable rate depended on the outage probability, we develop a new framework to highlight that the impact of user population with different spatial distributions on the achievable secrecy rate resulting from the achievable outage probability with respect to the spatial distribution instead of only spatial average.

For the convenience of the tractability, the successful transmission probability (STP) of SR networks can be denoted as

$$\begin{aligned} P_{st}^{c} &= \Pr\{SIR_c > \beta_c\} \\ &= 1 - P_{to}^{c} \end{aligned} \tag{9}$$

where P_{st}^{c} denotes the successful transmission probability of SR networks.

Note that the SR-COP is the complementary function of the STP of the SR networks from expression (9). It means SR-COP is equivalent to the STP from the point of outage performance analysis. According to the definition of the SR-COP, the STP of SR networks P_{st}^{c} is a random variable relating to the position distribution of random transmitters. Hence, the achievable outage coverage probability of a SR network P_{cov} can be obtained.

$$\begin{aligned} P_{\text{cov}} &= Pr\{P_{st}^{c} < \kappa_c\} \\ &= \Pr\{P_{st}^{c} > 1-\kappa_c\} \\ &< \delta \end{aligned} \tag{10}$$

where δ denotes target threshold of the secrecy outage coverage probability. Hence, the achievable successful transmission probability can be defined as

$$\vec{P}_{st} = (1-\kappa_c)\delta \tag{11}$$

It reveals that δ fraction of random nodes achieve to a successful transmission probability higher than $1-\kappa_c$ in DCRWNs. Employing the result of the achievable STP, we obtain the achievable secrecy rate $\overrightarrow{R_s}$ which is used to derive the achievable secrecy throughput of the SR network. Therefore, a new framework is presented to characterize the achievable secrecy throughput η of SR network. η is defined as the multiplication of the secrecy transmission probability, the spatial density and the achievable secrecy rate.

$$\eta = (1-\varepsilon_c)\lambda_c \overrightarrow{R_s} \tag{12}$$

where $\overrightarrow{R_s}$ is the achievable secrecy rate of an arbitrary link in the SR network.

III. Analysis of Connection Outage Probability

In this section, we first analyze the PR-COP and SR-COP of DCRWNs. In particular, a comparison between the achievable SR-COP and the ergodic SR-COP is presented considering the spatial distribution of random nodes.

Lemma 1: The successful transmission probability of the network Π_k is given by

$$P_{st}^{k} = \exp\left\{-\pi \nu_k l_k^2 (\lambda_p + \lambda_c)\right\} \tag{13}$$

where $\upsilon_k = C(\alpha)\beta_k^{2/\alpha}, k \in \{p,c\}$, $C(\alpha) = \frac{2\pi/a}{\sin(2\pi/a)}$.

Proof: According to Slivnyak's theory [16], the SIR at the typical receiver in (2) is

$$SIR_k = \frac{Phl_k^{-\alpha}}{\sum_{i\in\Pi_p} Ph\left|x_i\right|^{-\alpha} + \sum_{j\in\Pi_c} Ph\left|x_j\right|^{-\alpha}} \tag{14}$$

where x_i and x_j represent the distance from the node i and j to the origin in the PR network and the SR network, respectively. Hence, the successful transmission probability P_{st}^{k} of the network k is derived as

$$\begin{aligned} P_{st}^{k} = \Pr\{SIR_k > \beta_k\} &\overset{(a)}{=} \Pr\left\{h_k > l_k^{\alpha}\beta_k\left(I_p + I_c\right)\right\} \\ &\overset{(b)}{=} \Phi_{I_p}\left(l_k^{\alpha}\beta_k\right)\Phi_{I_c}\left(l_k^{\alpha}\beta_k\right) \end{aligned} \tag{15}$$

where (a) considers exponential distribution of a random variable h_k, (b) follows the Campbell's Theorem [16], i.e.,

$$\phi_{I_p}(s)=\exp\left[-\lambda_p s^{2/\alpha}\pi C(\alpha)\right] \quad (16)$$

$$\phi_{I_c}(s)=\exp\left[-\lambda_c s^{2/\alpha}\pi C(\alpha)\right] \quad (17)$$

A. SR-COP

In this section, we derive the achievable successful transmission probability which is equivalent to the achievable SR-COP respecting of the aforementioned expression of (9).

Lemma 2: The achievable STP of SR networks is given by

$$\vec{P}_{st}=(1-\kappa_c)\left\{1-\exp\left[-\frac{\lambda_c \ln\frac{1}{1-\kappa_c}}{\nu_c(\lambda_p+\lambda_c)}\right]\right\} \quad (18)$$

where $\nu_c=C(\alpha)\beta_c^{2/\alpha}$.

Proof: According to Lemma 1 (13), the successful transmission probability of the SR network denotes as

$$P_{st}^c=\exp\left\{-\pi\nu_c l_c^2(\lambda_p+\lambda_c)\right\} \quad (19)$$

Applying (19) into (10), the achievable outage coverage probability is given by

$$\begin{aligned}P_{\text{cov}}&=\Pr\left\{P_{st}^c>1-\kappa_c\right\}\\&=\Pr\left\{\exp\left[-\pi\nu_c l_c^2(\lambda_p+\lambda_c)\right]>1-\kappa_c\right\}\\&\overset{(a)}{=}\Pr\left\{l_c^2<\frac{-\ln(1-\kappa_c)}{\pi\nu_c(\lambda_p+\lambda_c)}\right\}\\&=1-\exp\left[-\frac{\lambda_c\ln\frac{1}{1-\kappa_c}}{\nu_c(\lambda_p+\lambda_c)}\right]\end{aligned} \quad (20)$$

where (a) follows the distribution of l_c in (3).

It can be seen that the achievable STP is determined by network parameters, such as the density of PR networks, the density of SR networks, the SR-COP and the target SIR threshold of SR networks. The achievable STP of the SR network decrease as the PR density increase, which reflects the fact that the chance of spectrum access for the SR nodes reduces when the density of PR users increases in cognitive radio wireless networks.

In addition, considering the relationship $P_{\text{cov}}<\delta$, it is easy to derive the achievable SIR threshold of the SR network.

$$\beta_c\le\left[\frac{\lambda_c\ln\frac{1}{1-\kappa_c}}{(\lambda_p+\lambda_c)\ln\frac{1}{1-\delta}C(\alpha)}\right]^{\frac{\alpha}{2}} \quad (21)$$

Corollary 1: The optimal SR-COP that maximize the achievable STP is given by

$$\kappa_c^{opt}=1-(1+m)^{-\frac{1}{m}} \quad (22)$$

where $m=\frac{\lambda_c}{(\lambda_p+\lambda_c)\nu_c}$.

Proof: It is assume that the objective function is $f(\kappa_c)=\vec{P}_{st}$. The objective function $f(\kappa_c)$ has the characteristics of $f(\kappa_c)'=0$ when $\kappa_c=\kappa_c^{opt}$ and $f(\kappa_c)''<0$, where $f(\cdot)'$ and $f(\cdot)''$ are the first derivative and the second derivative of the function, respectively. We can observe that the achievable STP is a concave function about κ_c.

In order to investigate the impact of spatial distribution of random nodes on the secrecy transmission rate, the ergodic SR-COP is also presented in DCRWNs. The ergodic SR-COP is defined as the expected value of distance weighted COP of an arbitrary communication link in this section.

$$\bar{P}_{to}=E_l[P_{to}]=\int_0^{+\infty}f_{l_c}(l)P_{to/l}dl \quad (23)$$

Lemma 3: The ergodic SR-COP is given by

$$\bar{P}_{to}=\frac{\upsilon_c(\lambda_p+\lambda_c)}{\lambda_c+\upsilon_c(\lambda_p+\lambda_c)} \quad (24)$$

Proof: The STP of SR network is expressed as $P_{st}^c=exp\left[-\pi\upsilon_c l_c^2(\lambda_p+\lambda_c)\right]$ using the result in (13). Hence, the ergodic SR-COP is evaluated as

$$\begin{aligned}\bar{P}_{to}&=1-E[\Pr\{SIR_c>\beta_c/l\}]\\&=1-\int_0^{+\infty}f_{l_c}(l)P_{st/l}^c dl\\&=1-\int_0^{+\infty}2\pi\lambda_c l e^{-\pi\lambda_c l^2}\exp\left[-\pi\upsilon_c l^2(\lambda_p+\lambda_c)\right]dl\\&=1-\frac{\lambda_c}{\lambda_c+(\lambda_c+\lambda_p)\upsilon_c}\end{aligned} \quad (25)$$

where $f_{l_c}(l)$ is the probability density function (PDF) of the TX-RX distance l_c. In addition, $f_{l_c}(l)=F_{l_c}(l)'$.

Applying (24) in (4), we obtain the ergodic transmission rate of SR networks as follows.

$$\bar{R}_t=\log_2\left\{1+\left[\frac{\lambda_c\left(\frac{1}{\kappa_c}-1\right)}{(\lambda_p+\lambda_c)C(\alpha)}\right]^{\frac{\alpha}{2}}\right\} \quad (26)$$

B. PR-COP

It is essential to present the PR-COP for the reason that the transmission performance of SR networks is limited by the PR-COP. For the convenience of tractability, we assume that the transmitting distance between the PR transmitter and the intended receiver is fixed as $l_p=1$.

Lemma 4: The PR-COP in DCRWNs is given by

$$P_{to}^p=1-\exp\left\{-\pi\nu_p(\lambda_p+\lambda_c)\right\} \quad (27)$$

Proof: With respect to the result in (13) and (9), it is easy to derive the expression of PR-COP under a given distance $l_p=1$.

Using (27) in (5), we find that the SR density is limited by the PR-COP.

$$\lambda_c \le \frac{\ln\left(\frac{1}{1-\kappa_p}\right)}{\pi C(\alpha)\beta_p^{2/\alpha}} - \lambda_p \tag{28}$$

IV. Achievable Secrecy Throughput of SR Networks

At first, the achievable secrecy outage probability is derived for SR networks with no-colluding eavesdroppers. Then, we analyze the secrecy transmission rate including achievable secrecy rate and average secrecy rate. Finally, the achievable secrecy throughput of the SR network is evaluated based on the achievable secrecy rate under outage constraints of the PR-COP and SR-SOP.

A. SR-SOP

Lemma 5: The achievable SR-SOP in DCRWNs is given by

$$\vec{P}_{so} = 1 - \exp\left[-\frac{\lambda_e}{(\lambda_p+\lambda_c)\beta_e^{2/\alpha}C(\alpha)}\right] \tag{29}$$

Proof: All eavesdropping nodes in the DCRWN are randomly and independently distributed, 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

$$\Pr\{SIR_e > \beta_e\} = \exp\left\{-\pi C(\alpha) l^2 \beta_e^{2/\alpha}\left(\lambda_p+\lambda_c\right)\right\} \tag{30}$$

The eavesdropping event occurs when the maximum of received SIR_e for all eavesdroppers is greater than the threshold β_e. Hence, the achievable SR-SOP is derived as

$$\begin{aligned}
\vec{P}_{so} &= 1 - \Pr\{\max_{e\in\Phi_e}\{SIR_e\} < \beta_e\} \\
&\overset{(a)}{=} 1 - \mathbb{E}_{\Phi_e}\left\{\prod\nolimits_{e\in\Phi_e}\Pr\{SIR_e < \beta_e\}\right\} \\
&\overset{(b)}{=} 1 - \exp\left\{-\lambda_e\int_{\mathbb{R}^2}\Pr\{SIR_e > \beta_e\}\,dl\right\} \\
&= 1 - \exp\left\{-\lambda_e 2\pi\int_0^\infty \Pr\{SIR_e > \beta_e\}\,ldl\right\}
\end{aligned} \tag{31}$$

where (a) follows the independent distribution of eavesdroppers, (b) follows the probability generating functional (PGFL) of the Poisson point process [17]. The closed-form expression of the achievable SR-SOP is obtained by substituting (30) into (31).

From (8) and (29), the SR density is limited by the SR-SOP.

$$\lambda_c \ge \frac{\lambda_e}{\ln\left(\frac{1}{1-\varepsilon_c}\right)\beta_e^{2/\alpha}C(\alpha)} - \lambda_p \tag{32}$$

B. Achievable Secrecy Rate of SR Networks

Theorem 1: The achievable secrecy rate of SR networks is given by

$$\vec{R}_s = \log_2\left\{\frac{\lambda_c \ln\frac{1}{1-\kappa_c}\ln\frac{1}{1-\varepsilon_c}}{\lambda_e \ln\frac{1}{1-\delta}}\right\}^{\frac{\alpha}{2}} \tag{33}$$

Proof: Applying (21) in (4), the achievable transmission rate $\vec{R}_t$ of SR networks can be given by

$$R_t \overset{\rightarrow}{=} \log_2\{1+A\} \tag{34}$$

Plugging (29) and (8) into (4), the achievable eavesdropping rate is given as follows.

$$R_e \overset{\rightarrow}{=} \log_2\{1+B\} \tag{35}$$

where $A = \left[\frac{\mu\ln\frac{1}{1-\kappa_c}}{\ln\frac{1}{1-\delta}}\right]^{\frac{\alpha}{2}}$, $B = \left[\frac{\mu}{\ln\frac{1}{1-\varepsilon_c}}\right]^{\frac{\alpha}{2}}$, $\mu = \frac{\lambda_c}{(\lambda_p+\lambda_c)C(\alpha)}$

Using (34) and (35) in (1), we obtain the expression of $\overrightarrow{R_s} = \overrightarrow{R_t} - \overrightarrow{R_e}$. It is worth to noting that the result in (33) is valid in high SIR regime, i.e., $A \gg 1$ and $B \gg 1$.

Theorem 2: The ergodic secrecy rate of SR networks is given by

$$\bar{R}_s = \log_2\left\{\frac{\lambda_c\left(\frac{1}{\kappa_c}-1\right)\ln\frac{1}{1-\varepsilon_c}}{\lambda_e}\right\}^{\frac{\alpha}{2}} \tag{36}$$

Proof: It is easy to complete the proof of Theorem 2 using the similar proofing approach as Theorem 1 respecting of (26) and (29).

C. Achievable Secrecy Throughput of SR Networks

In this section, we derive the achievable secrecy throughput of SR networks, and analyze the impaction of the connection outage probability of PR networks and secrecy outage probability of SR networks on the achievable secrecy throughput of SR networks.

Theorem 3: The achievable secrecy throughput of SR systems is given by

$$\eta = (1-\varepsilon_c)\lambda_c \log_2\left\{\frac{\lambda_c \ln\frac{1}{1-\kappa_c}\ln\frac{1}{1-\varepsilon_c}}{\lambda_e \ln\frac{1}{1-\delta}}\right\}^{\frac{\alpha}{2}} \tag{37}$$

Proof: Respecting of the definition of achievable secrecy throughput (12), η is defined as the multiplication of the secrecy transmission probability, the spatial density and the achievable secrecy rate. Then, the expression of the achievable secrecy rate $\vec{R}_s$ is obtained as (33). Substituting (33) into (12), the achievable secrecy throughput of SR networks η can be obtained as (37).

From Theorem 3, the achievable secrecy throughput is determined by system parameters, such as SR density, the PR-COP and the SR-SOP. The feasible range of the SR density is given by

$$\lambda_c \in [\lambda_{c1}, \lambda_{c2}] \tag{38}$$

where λ_{c1} is derived by guaranteeing the constraint of PR-COP (32), and λ_{c2} is obtained by meeting the SR-SOP in (28). Furthermore, the condition of positive achievable secrecy throughput of SR networks can be evaluated as follows.

Corollary 2: The condition of positive secrecy transmission capacity of SR networks is given by

$$\lambda_e < \frac{\ln\frac{1}{1-\kappa_c}\ln\frac{1}{1-\varepsilon_c}}{\ln\frac{1}{1-\delta}}\lambda_c \tag{39}$$

Proof: The above result is achieved by solving $\eta > 0$.

V. Numerical Results

In this section, we present numerical results to evaluate the achievable successful transmission probability, secrecy transmission rate and achievable secrecy throughput of SR networks.

Fig. 1 shows the achievable successful transmission probability $\vec{P}_{st}$ given in (18) versus target connection outage probability κ_c in SR networks for various values of density ratio λ_p / λ_c and SIR threshold β_c. It can be seen that the achievable STP decreases as SIR threshold increases. On the other hand, the achievable STP increases when density ratio decreases. It shows that $\vec{P}_{st}$ is determined by the PR density, the SR density and the SIR threshold of the SR user. When the requirement of STP in SR networks is high, the density ratio between the PR network and the SR network needs to be reduced, which also reflects the impact of PR density on the SR-COP. In addition, we can find an optimal target COP maximizing the achievable STP, and the optimal value κ_c can be verified from Corollary 1.

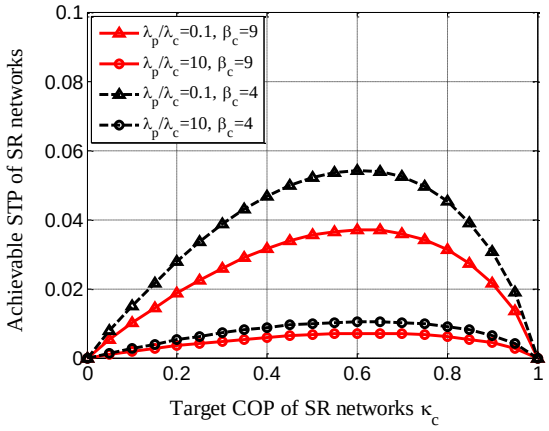

Fig. 1 Achievable successful transmission probability $\vec{P}_{st}$ versus target COP for different values of SR density and outage coverage probability. The system parameters are set as $\alpha = 4$.

Fig. 2 compares the secrecy transmission rate of SR networks between two cases: the achievable secrecy rate $\vec{R}_s$ and the average secrecy rate $\overline{R}_s$. For the first case, $\vec{R}_s$ increases as δ decreases, and $\vec{R}_s$ increases as ε_c increases. It reveals the tradeoff between the achievable outage coverage probability and the secrecy outage probability. Comparing among the three solid lines which have same $\varepsilon_c = 0.8$, we observe that the gap of secrecy rate between the solid lines with circle and square is relatively small. It means that the average secrecy rate is just a particular case of achievable secrecy rates. This can be attributed to the fact that the spatial distribution of random nodes has a significantly impact on the secrecy rate. It can be see that the secrecy rate for two cases of $\vec{R}_s$ and $\overline{R}_s$ increases as λ_c / λ_e. Hence, the SR density should be carefully controlled for the target of a given secrecy level in transmission service.

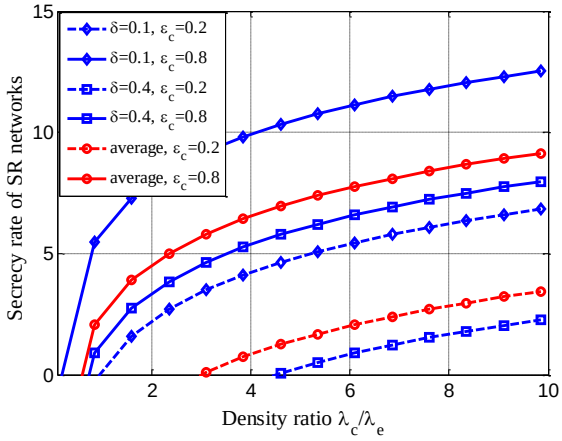

Fig. 2 Comparison of the secrecy rate between achievable case and ergodic case versus density ratio λ_c / λ_e for different values of ε_c. The blue lines and the red lines represent the achievable secrecy rate and the ergodic secrecy rate, respectively. The system parameters are set as $\alpha = 4$, $\beta_c = 1$, $\kappa_c = 0.4$

Fig. 3 presents the achievable secrecy throughput of SR networks versus the target secrecy outage probability ε_c with different values of SR density λ_c and secrecy outage coverage probability δ. We can first observe that there exists an optimal value of target SOP ε_c maximizing the achievable secrecy throughput. As shown in this figure, the achievable secrecy throughput η increases as the SR density λ_c under the constraints of the PR-COP and the SR-SOP, this coincides with the result in (38). For a given λ_c, η increases when δ decreases. It means that secrecy throughput can be improved significantly by sacrificing the outage coverage probability of SR networks.

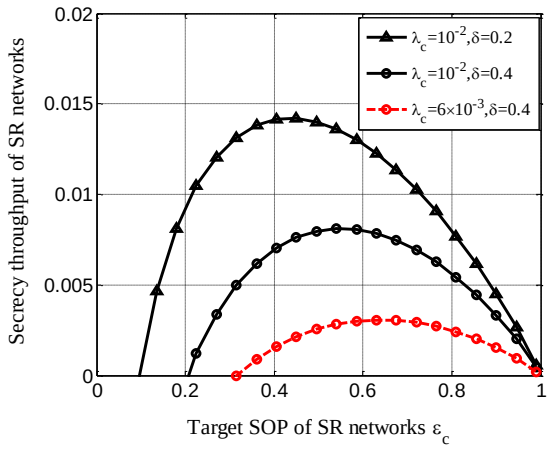

Fig. 3 Achievable secrecy throughput η versus target SOP ε_c for different values of SR density λ_c and secrecy outage coverage probability δ. The system parameters are set as $\alpha = 4$, $\kappa_c = 0.2$.

VI. Conclusions

In this paper, a novel framework is introduced to analyze achievable secrecy throughput of the SR network in DCRWNs. Through stochastic geometry analysis, we derive the exact expressions of the connection outage probability, secrecy outage probability, and achievable secrecy rate respecting of many determinant such as the nearest neighbor routing protocol, general spatial node distribution and aggregate interference. Compared with the ergodic secrecy rate, the achievable secrecy rate is provided to indicate the performance discrepancy resulting from spatial distribution of random nodes. In particular, the optimal value of SR-COP maximizing the achievable STP of SR networks is derived. Future work can be extended to a more general wireless network with multiple antennas, cooperative relays or colluding eavesdroppers.

Acknowledgment

The authors would like to thank the editor and anonymous reviewers for their valuable comments and suggestions that improved the quality of the paper.

References

[1] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive raios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no, 5, pp. 894-914, May. 2009.

[2] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533-549, May 1988.

[3] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1367, Oct. 1975.

[4] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, June 2008.

[5] 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.

[6] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005-4019, Sept. 2008.

[7] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547-2553, Jun. 2009.

[8] A. Khisti and G. Wornell, "Secure transmission with multiple antennas—part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol.56, no. 11, pp. 5515-5532, Nov. 2010.

[9] C. Fan, W. Y. Raymond, and W. S. Kenneth, "Imperfect secrecy in wiretap channel II," *IEEE Trans. Inf. Theory*, vol. 61, no. 1, pp. 628-636, Jan. 2015.

[10] H. EISawy, E. Hossain, and M. Haenggi, "Stochastic geometry for modeling, analysis, and design of multi-tier and cognitive cellular wireless networks: A survey," *IEEE Commun. Surveys & Tutorials*, vol. 15, no. 3 pp. 996-1019, Apr. 2013.

[11] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: Survey," *IEEE Commun. Surveys & Tutorials*, vol. 16, no. 3 pp. 1550-1537, Apr. 2014.

[12] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Netw*., vol. 10, pp. 2764-2775, Jan. 2010.

[13] H. Wang, X. Y. Zhou, and M. C. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun*., vol. 12, no. 6, Jun. 2013.

[14] J. Bai, X. F. Tao, J. Xun, and Q. M. Cui, "The secrecy outage probability for theith closest legitimate user in stochastic networks," *IEEE Commun. Lett.*, vol. 18, no. 7, pp. 1230-1233, Jul. 2014.

[15] M. Z. Win, A. Rabbachin, J. Lee, and A. Conti, "Cognitive network secrecy with interference engineering" *IEEE Trans. Netw.*, vol. 28, no. 5, pp. 86-90, Oct. 2014.

[16] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and it`s Applications*, Chichester: John Wiley & Sons, 1995.

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

Hongyu Ma received the B.E. degree from Liaoning University of Technology, Jinzhou, China, in 2003. She is currently working towards the Ph.D. degree in signal and information processing of Beijing University of Posts and Telecommunications (BUPT). Her current research interests include wireless communications, cognitive radio wireless networks and cooperative communication.

Kai Niu received a B.S. degree in information engineering and a Ph.D. in signal and information processing from BUPT, Beijing, China, in 1998 in 2003, respectively. Currently he is a professor in the School of Information and Communication Engineering of BUPT. His research interests are in the area of channel coding and broadband wireless communication, particularly on the practical design of polar codes and study of polar decoding algorithms.