This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2011 proceedings.

Impact of Interference on Secrecy Capacity in a Cognitive Radio Network

Zhihui Shu, Yaoqing (Lamar) Yang, Yi Qian
Department of Computer and Electronics Engineering
University of Nebraska-Lincoln
Omaha, Nebraska 68182
Email: zshu@unomaha.edu, yyang3@unl.edu, yqian2@unl.edu

Rose Qingyang Hu
Department of Electrical and Computer Engineering
Utah State University
Logan, Utah 84322
Email: rose.hu@usu.edu

***Abstract*—In this paper, we investigate secrecy capacity of a cognitive radio network based on stochastic geometry distributions. We consider the Poisson process of both the secondary users and the eavesdroppers, and analyze how the stochastic interference from the secondary users can influence the secrecy capacity of the primary users. First, we describe a network model with primary users, secondary users and eavesdroppers in a cognitive radio communication network environment, and derive the expression of secrecy capacity in an additive white Gaussian noise channel. Then, we study the outage probability of secrecy capacity of a primary node from a secure communication graph point of view. Furthermore, we present numerical results of the cumulative distribution function (c.d.f.) of the secrecy capacity between a primary transmitter and a primary receiver. Our analysis brings the insights on secure communications in terms of spatially Poisson distributions of primary users, secondary users and eavesdroppers.**

***Index Terms*—Cognitive radio network, radio channel, secrecy capacity, stochastic geometry distribution.**

I. Introduction

Cognitive radio (CR) shows a great promise for future wireless communications. The term "cognitive radio" was first proposed by Mitola [1], which refers to a reconfigurable wireless black-box that intelligently adjusts its communication variables in response to the overcrowded frequency spectrum. Current wireless networks are regulated by a fixed spectrum assignment policy, i.e. the spectrum is regulated by governmental agencies, such as Federal Communications Commission (FCC), and is assigned to licensed users (or primary users) or services on a long term basis for large geographical regions. Although the fixed spectrum assignment policy generally served well in the past, there is a dramatic increase in the demand on the limited spectrum for mobile services in the recent years. The limited available spectrum and the inefficiency in the spectrum usage necessitate a new communication paradigm to exploit the existing wireless spectrum opportunistically [2]. The new scheme is using spectrum sharing which allows the operation of a cognitive system as long as it does not harm the transmission of the primary users. In spectrum sharing mode, the transmitting power of the secondary users (or unlicensed users) is optimally controlled such that no extra interference power constraint can be applied to the primary users. Cognitive radio can efficiently utilize the unused spectrum for secondary usage without interfering a primary licensed user. At the same time, the cognitive radio paradigm has introduced entirely new classes of security threats and challenges, and providing strong security may prove to be the most difficult aspects of making cognitive radio a long-term commerically-viable concept [3].

In this paper we present a secrecy capacity study for a cognitive radio network model. The information-theoretic secrecy capacity was proposed in [4], which shows how one could obtain "perfect secrecy" when a receiver enjoys a better channel than the wire-tapping eavesdropper. The secrecy capacity is defined as the difference of the Shannon capacity of the channel between the source and destination (a.k.a. main channel) and the Shannon capacity of the channel between the source and eavesdropper (a.k.a. eavesdropper channel). The secrecy capacity of wireless channels was studied in [5]. The outage secrecy capacity was investigated in additive white Gaussian noise (AWGN) channels. The secrecy capacity of fading channels was investigated in [6], which studied the secure transmission of information over an ergodic fading channel in the presence of an eavesdropper. In [7] [8], Ma et al. presented secure approaches of null space-based noise signal generation and randomized eigenvector-based jamming signals without considering cognitive users. The secrecy capacity in wireless networks was investigated in [9], where Koyluoglu et al. studied a random extended network, with the legitimate and eavesdropper nodes are assumed to be placed according to Poisson point processes in a square region. The secrecy capacity of cognitive radio networks was studied in [10], where Anand et al. considered the cognitive radio model when the primary nodes are stationary, and the secondary nodes cannot be inside the primary exclusive region (PER), and only one eavesdropper was considered. In [11], Vu et al. derived expressions for the PER for a primary transmitter in a cognitive radio network without fading in terms of the secrecy capacity. Poisson spatial model is often used to study the characteristics of wireless networks [12]. Consequently, different methods based on stochastic geometry and the theory of random geometric graphs - including point process theory, percolation theory, and probabilistic combinatorics - have led to results on the connectivity [13], the capacity [14], the outage probability, and other fundamental limits of wireless networks.

In all the previous work discussed above, however, only Poisson distribution of the secondary users or Poisson distribution of the eavesdroppers is considered. The impact of

978-1-4244-9268-8/11/$26.00 ©2011 IEEE

the combination of the Poisson process of both the secondary users and the eavesdroppers have not been revealed. In this paper, we combine the Poisson process of both the secondary users and the eavesdroppers and analyze the stochastic interference from the secondary users to both the primary users and eavesdroppers. We first describe a model of the spatial distribution of nodes. Then we characterize the spatial location of both the secondary users and eavesdroppers as Poisson point process. Furthermore, we analyze the stochastic interference of secondary users to the primary users and eavesdroppers. We calculate the probability density function of the secrecy capacity and obtain the probability of an outage in secrecy capacity. At the end, we provide numerical results to further discuss the insights of our analysis.

The major contributions of this paper are as follows. First, we considered the interference impact of the secondary users in a cognitive radio network model. We derived the total interference of the secondary users on the primary users and eavesdroppers. Then we obtained the expression of secrecy capacity when there exist secondary users, and we analyzed the probability density function of the interference powers on the primary users and the secondary users. Second, we investigated how the stochastic distribution of primary users, secondary users and eavesdroppers influence the secrecy capacity. By using the characteristics of the Poisson process, we analyzed the cumulative distribution function of secrecy capacity and outage probability of the secrecy capacity of primary users. We presented expressions for the probabilities of existence and outage probability of the secrecy capacity, in the presence of a Poisson field of primary users, secondary users and eavesdroppers.

The rest of this paper is organized as follows. In Section II we describe the cognitive radio network model. In section III, we analyze the connectivity in Poisson secure communication graph and the secrecy capacity of the primary nodes in the cognitive radio network. In Section IV we provide numerical results and further discussions. In Section V we conclude this paper.

II. The Cognitive Radio Network Model

In this paper, we consider a cognitive radio network model with primary users, secondary users and eavesdroppers as illustrated in Fig. 1. In this model, let $\Pi_P = \{p_i\} \subset \mathbb{R}^2$ denote the set of primary user nodes, $\Pi_S = \{s_i\} \subset \mathbb{R}^2$ denote the set of secondary user nodes and $\Pi_E = \{e_i\} \subset \mathbb{R}^2$ denote the set of eavesdroppers, where Π_P, Π_S, Π_E are mutually independent homogeneous Poisson process with densities λ_P, λ_S and λ_E, respectively. From Fig. 1, primary receiver 1 is the closest neighbor of primary transmitter 1 as its distance to the primary transmitter 1 is the shortest. Primary receiver 2 is the second closest neighbor of primary transmitter 1 as its distance to the primary transmitter 1 is the second shortest, and so on.

The Poisson secure communication graph (a.k.a. s-graph) is a convenient geometrical representation of the information-theoretic secure links that can be established over such a network. In ad-hoc scenarios, a statistical description of the

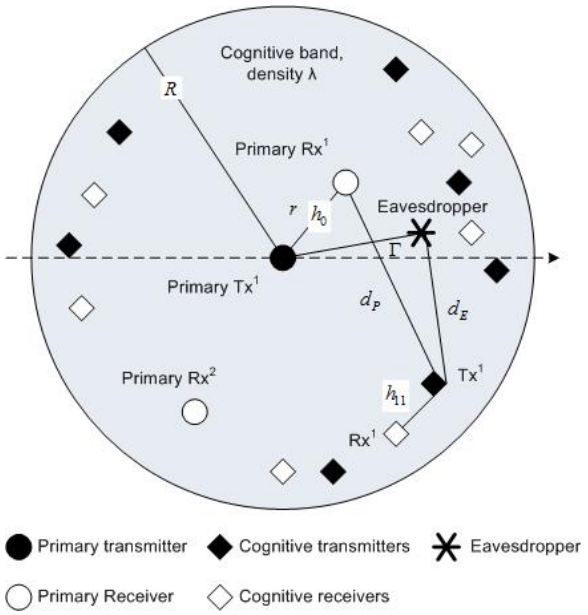

Fig. 1. A cognitive radio network model.

node location is available, and thus a stochastic spatial model should be employed instead of a deterministic model. In particular, when there is no a *priori* information about the node positions, we can treat them randomly distributed according to a homogeneous Poisson point process [15]. The Poisson process has maximum entropy among all homogeneous processes [16], and corresponds to a simple and useful model for the location of nodes in a cognitive radio network.

Assume the entire network is a circular region of radius R [10], we analyze the features of this network and then extend our results to the entire network with $R \to \infty$. In a quasi-static wireless environment, the received power $P_{rx}(x_i, x_j) = \frac{P|h(x_i,x_j|^2}{d_{ij}^{\alpha}}$, where P is the transmit power of the primary nodes; $h(x_i, x_j)$ is the complex fading coefficient of the primary link $\overrightarrow{x_i x_j}$, which is assumed constant during the communication interval, $d_{ij} = ||x_i - x_j||$ is the distance between node x_i and node x_j, and α is the loss exponent of medium, which varies from 0.8 to 4 due to different communication environment [17]. In order to calculate the interference, we consider the case $\alpha > 2$ in our study. Thus, the Shannon capacity C_P between the primary transmitter and primary receiver with interference is given by

$$C_P = \log_2\left(1 + \frac{P_{rx}(x_i, x_j)}{W_P + I_P}\right) \quad \text{bps/Hz} \qquad (1)$$

where W_P is the noise powers introduced by the primary receivers and I_P is the interference powers of the primary receiver from the cognitive users. Similarly, the Shannon capacity C_E between the primary transmitter and the eavesdropper with interference is given by

$$C_E = \log_2\left(1 + \frac{P_{rx}(x_i, e)}{W_E + I_E}\right) \quad \text{bps/Hz} \qquad (2)$$

where W_E is the noise power introduced by the eavesdropper receivers and I_E is the interference power of the eavesdroppers from the cognitive users. For certain realization, the secrecy capacity of the primary link is given by

$$Cs(x_i,x_j)=\max\{\log_2\left(1+\frac{P_{rx}(x_i,x_j)}{W_P+I_P}\right) - \log_2\left(1+\frac{P_{rx}(x_i,e)}{W_E+I_E}\right),0\}. \quad (3)$$

where e is the eavesdropper with the strongest received signal from the transmitter x_i. Note that secrecy capacity cannot be negative.

We now consider a special case where the wireless environment introduces only path loss, that is $h(x_i,x_j)=1$ for all $i\neq j$ and the thermal noise powers at the primary users and eavesdroppers are assumed to be the same because these noise powers maintain the same even if the receiver of a secondary user changes position: $W_P=W_E=W$. The received powers of the primary users and eavesdroppers become

$$P_{rx}(x_i,x_j)=\frac{P}{||x_i-x_j||^\alpha}, \quad (4)$$

$$P_{rx}(x_i,e^*)=\frac{P}{||x_i-e^*||^\alpha}, \quad (5)$$

and secrecy capacity can be simplified as

$$C_s(x_i,x_j)=\max\left\{\log_2\left(1+\frac{P}{||x_i-x_j||^\alpha(W+I_P)}\right) - \log_2\left(1+\frac{P}{||x_i-e^*||^\alpha(W+I_E)}\right),0\right\} \quad (6)$$

where $\{r_i\}_{i=1}^{\infty}$ and $\{\Gamma_i\}_{i=1}^{\infty}$ denote the random distances to the origin of the nodes in Π and Π_E, respectively.

III. Analysis of Secrecy Capacity

Consider the main link (the link between the primary transmitter and its i^{th} closest neighbor, $i\geq 1$) and the eavesdropper, secrecy capacity satisfies $C_{s,i}=\max\{C_{P,i}-C_E,0\}$.

First, we evaluate the probability density function of the interference from all of the secondary users to the primary receiver. For instance, I_P can be obtained as follows

$$I_P=\sum_{i=1}^{n}\frac{P_s}{d_{P,i}^\alpha} \quad (7)$$

where the summation is over all secondary nodes in the network, $d_{P,i}$ denotes the distance between the i^{th} secondary user and the primary receiver, n denotes the number of the secondary nodes in the network, P_s is the transmitting power of secondary nodes. In this paper, we set $P_s=1\ Watt$.

As the secondary nodes satisfy a Poisson process in the two-dimensional plane with the average number of points per unit area equals to λ_s, due to the nature of the Poisson process, the distribution of the locations $d_{P,i}$ of the secondary nodes is that of independent and identically distributed points with uniform distribution [18]. Then, the characteristic function of random variable Z can be obtained as the following.

Let $\phi_Z(\omega)$ be the characteristic function of random variable Z, i.e., $\phi_Z(\omega)=E(e^{i\omega Z})$. Since the characteristic function of the sum of a number of independent random variables is the product of the individual characteristic functions, the characteristic function of interference satisfies [18]:

$$\phi_Z(\omega)=\exp\left(-\pi\lambda_s\Gamma(1-\frac{2}{\alpha})e^{-\frac{\pi}{\alpha}}\omega^{\frac{2}{\alpha}}\right) \quad (8)$$

where $\phi_Z(\omega)$ is the characteristic function, $\omega\in R$ is the argument of the characteristic function, Γ is the gamma function and α is the path loss exponent. By taking the inverse Fourier transform [18], we have

$$f_Z(z)=\frac{1}{\pi z}\sum_{k=1}^{\infty}\frac{\Gamma(\frac{2k}{\alpha}+1)}{k!}(\frac{\rho}{z^{\frac{2}{\alpha}}})\sin k\pi(1-\frac{2}{\alpha}) \quad (9)$$

where $\rho=\pi\lambda_s\Gamma(1-\frac{2}{\alpha})$.

When $\alpha=4$, the probability density function of interference satisfies

$$f_Z(z)=\frac{\pi}{2}\lambda_s z^{-3/2}e^{-\pi^3\lambda_s^2/4z} \quad (10)$$

Then, we derive the probability density function of $C_{P,i}$. When $\alpha=4$, from equation (1) and (4), we know that $C_{P,i}=\log_2(1+\frac{P}{r_i^4(W+I_P)})$, where r_i denotes the distance between the primary transmitter and its i^{th} closest neighbor. In order to find the probability density function of $\log_2(1+\frac{P}{r_i^4(W+I_P)})$, we assume that $Z=I_P$, $Y=r_i^4$, $X=r_i^2$, $V=W+Z$ and $U=Y\cdot V$.

So the probability density function of $V=W+Z$ is:

$$f_V(v)=\frac{\pi}{2}\lambda_s(v-W)^{-3/2}e^{-\pi^3\lambda_s^2/4(v-W)}\quad (v>W) \quad (11)$$

The cumulative distribution function of $U=Y\cdot V=Y\cdot(W+Z)$ is:

$$F_U(u)=Pr\{U\leq u\}=Pr\{Y\cdot V\leq u\}=Pr\{V\leq\frac{u}{Y}\}$$
$$=\int_W^{+\infty}\frac{\pi}{2}\lambda_s(v-W)^{-3/2}e^{-\pi^3\lambda_s^2/4(v-W)}dv\int_0^{\frac{u}{v}}f_Y(y)dy \quad (12)$$

So the probability density function of U is:

$$f_U(u)=(F_U(u))_u^{'}=$$
$$\int_W^{+\infty}\frac{\pi}{2}\lambda_s(v-W)^{-3/2}e^{-\pi^3\lambda_s^2/4(v-W)}f_Y(\frac{u}{v})\cdot\frac{1}{v}dv \quad (13)$$

Next, we determine the p.d.f of $Y=r_i^4$.

From [19], we know that $X=r_i^2$ represents Poisson arrival times on the line with the constant arrival rate $\pi\lambda$ and X has an Erlang distribution of order i and rate $\pi\lambda$ with probability density function:

$$f_X(x)=\begin{cases}\frac{(\pi\lambda)^i x^{i-1}e^{-\pi\lambda x}}{(i-1)!}, & x\geq 0,\\ 0, & x<0.\end{cases} \quad (14)$$

Let $Y=X^2$, we have [20]

$$f_Y(y)=\frac{1}{2\sqrt{y}}f_X(\sqrt{y}) \quad (15)$$

Combining (14) and (15), the probability density function of $Y = r_i^4$ can be obtained as the following:

$$f_Y(y) = \frac{1}{2\sqrt{y}} \frac{(\pi\lambda)^i (\sqrt{y})^{i-1} e^{-\pi\lambda\sqrt{y}}}{(i-1)!} \tag{16}$$

The Shannon capacity of primary user satisfies:

$$C_{P,i} = \log_2\left(1 + \frac{P}{Y(W+I_P)}\right) = \log_2\left(1 + \frac{P}{Y(W+Z)}\right), \tag{17}$$

Then, the cumulative distribution function of $C_{P,i}$ is:

$$\begin{aligned} F_{C_{P,i}}(c) &= Pr\{C_{P,i} \le c\} = Pr\{\log_2(1+\frac{P}{U}) \le c\} \\ &= Pr\{U \ge \frac{P}{2^c-1}\} = 1 - Pr\{U < \frac{P}{2^c-1}\} \\ &= 1 - F_U(\frac{P}{2^c-1}) \quad (c>0) \end{aligned} \tag{18}$$

So the probability density function of $C_{P,i}$ is:

$$\begin{aligned} f_{C_{P,i}}(c) &= F_{C_{P,i}}(c)'_c = -f_U(\frac{P}{2^c-1}) \cdot \frac{\partial}{\partial c}\left(\frac{P}{2^c-1}\right) \\ &= f_U(\frac{P}{2^c-1}) \cdot \frac{P}{(2^c-1)^2} \cdot 2^c \cdot \ln 2 \quad (c>0) \end{aligned} \tag{19}$$

Similarly, the probability density function of C_E can be obtained from (19) by replacing λ by λ_E and setting $i = 1$. As the sequences $\{r_i\}_{i=1}^{\infty}$ and $\{\Gamma_i\}_{i=1}^{\infty}$ are mutually independent, then $C_{P,i}$ and C_E are also independent. So we can determine the p.d.f of $C_{s,i} = \max\{C_{P,i} - C_E, 0\}$ by the convolution of $f_{C_{P,i}}$ and f_{C_E} [19].

The p.d.f. of $C_{s,i}$ is

$$f_{C_{s,i}}(c) = \begin{cases} f_{C_{P,i}}(c) * f_{C_E}(-c), & c > 0, \\ Pr_{0,i}\delta(c), & c = 0, \\ 0, & c < 0. \end{cases} \tag{20}$$

where $\delta(c)$ is the Dirac delta function; $Pr_{0,i} = Pr\{C_{s,i} = 0\}$ is the probability of zero secrecy capacity, given by

$$Pr_{0,i} = Pr\left\{\frac{P_{rx}(x_i, x_j)}{W + I_P} - \frac{P_{rx}(x_i, e)}{W + I_E} < 0\right\}, \tag{21}$$

As we know, $P_{rx}(x_i, x_j)$, $P_{rx}(x_i, e)$, I_P and I_E are only related to the position of the primary receivers and secondary receivers and they are all independent. However, W is the noise power which is not related to the position of the nodes. Thus, we have

$$Pr_{0,i} = \int_0^{\infty} f_{C_E}(y)dy \int_0^{y} f_{C_P}(x)dx, \tag{22}$$

The above analysis can be used to determine the probabilities of existence and outage of the secrecy capacity between a node and its i^{th} closest neighbor.

Considering the link between a node and its i^{th} closest neighbor, $i \ge 1$, the probability of existence of a non-zero secrecy capacity, $Pr_{\text{exist},i} = Pr\{C_{s,i} > 0\}$, is given by

$$Pr_{\text{exist},i} = 1 - \int_0^{\infty} f_{C_E}(y)dy \int_0^{y} f_{C_P}(x)dx \tag{23}$$

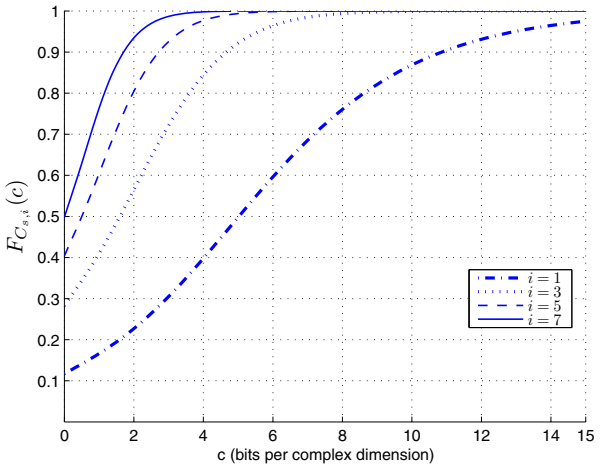

Fig. 2. C.d.f. $F_{C_{s,i}(c)}$ of the secrecy capacity $C_{s,i}(c)$ between a node and its i^{th} closest neighbor, for various i ($\lambda = 1$, $\lambda_E = \lambda_S = 0.1$, $P = 10$ $Watts$, $P_s = 1$ $Watt$, $W = 1$ $Watt$).

and the probability of an outage in secrecy capacity, $Pr_{\text{outage},i}(R_s) = Pr\{C_{s,i} < R_s\}$ for $R_s > 0$, is given by:

$$\begin{aligned} Pr_{\text{outage},i}(R_s) = 1 - \int_{R_s}^{\infty}\int_{c}^{\infty} f_P(\frac{P}{2^{\tau}-1})\frac{P}{(2^{\tau}-1)^2}2^{\tau}\ln 2 \\ f_E(\frac{P}{2^{\tau-c}-1})\frac{P}{(2^{\tau-c}-1)^2}2^{\tau-c}\ln 2 d\tau dc \end{aligned} \tag{24}$$

Using (22), we can write $Pr_{\text{exist},i} = Pr\{C_{s,i} > 0\} = 1 - Pr_{0,i} = 1 - \int_0^{\infty} f_{C_E}(y)dy \int_0^{y} f_{C_P}(x)dx$ and leads to equation (23). Note that $Pr_{\text{outage},i}(R_s)$ is just the c.d.f. of the r.v. $C_{s,i}$ evaluated at R_s. Thus, it can be obtained by integration of the corresponding p.d.f. given in (20). From $Pr_{\text{outage},i}(R_s) = \int_{-\infty}^{R_s} f_{C_{s,i}}(c)dc$, it results equation (24). Comparing this result with the work in [19], $Pr_{\text{outage},i}(R_s)$ is obtained by a double integral, while $Pr_{\text{outage},i}(R_s)$ in [19] is a single integral without considering the secondary users. It shows that the interference power from the secondary users is accounted.

IV. Numerical Results

In this section, we show numerical results of our analysis above, and discuss the insights of secrecy capacity analysis in some specific cognitive radio network scenarios.

In the numerical results, we set density and power parameters such that the density of primary users $\lambda = 1$, the density of secondary users and eavesdroppers $\lambda_E = \lambda_S = 0.1$, the transmit power of primary transmitter $P = 10$ $Watts$, secondary transmitter $P_s = 1$ $Watt$ and noise power $W = 1$ $Watt$.

Fig. 2 shows the cumulative density function (c.d.f.) $F_{C_{s,i}}(c)$ of the secrecy capacity $C_{s,i}$ between a node and its i^{th} closest neighbor according to (20). It shows that when i is small, the $F_{C_{s,i}}(0)$ is small and the outage probability in this case is relatively small. It also tells that as the

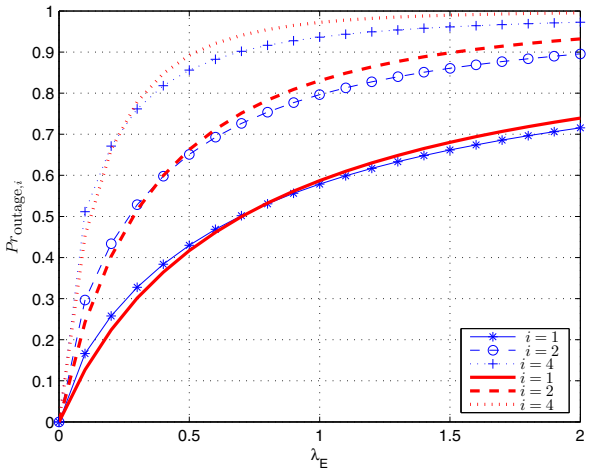

Fig. 3. Outage probability of secrecy capacity $C_{s,i}$ between the primary node and its i^{th} closest neighbor with and without secondary users (the lines with markers and without markers correspond to the cases with and without secondary users), for various values of i ($\lambda = 1$, $\lambda_S = 0.1$ (with secondary users), $P = 10\ Watts$, $P_s = 1\ Watt$, $W = 1\ Watt$, $R_s = 1$).

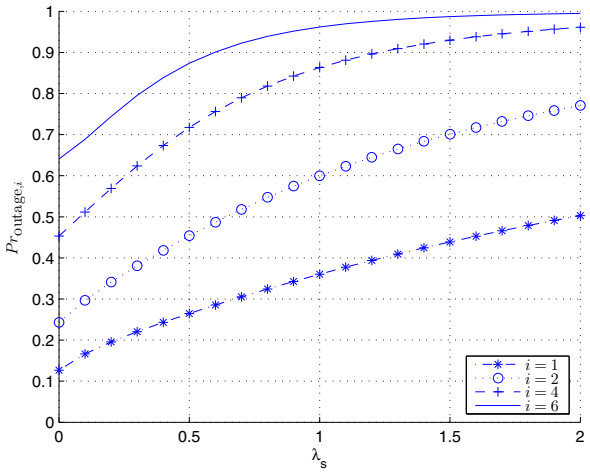

Fig. 4. Outage probability of secrecy capacity $C_{s,i}$ between the primary node and its i^{th} closest neighbor with secondary users, for various values of i ($\lambda = 1$, $\lambda_E = 0.1$, $P = 10\ Watts$, $P_s = 1\ Watt$, $W = 1\ Watt$, $R_s = 1$).

distance to the i^{th} closest neighbor increases with i, the secrecy capacity increases slowly. This implies that when i is small, the secrecy capacity has a greater likelihood of high secrecy capacity. When i increases, the secrecy capacity becomes smaller because the distance between the primary transmitter and receiver becomes larger.

Fig. 3 compares the secrecy outage probability versus the eavesdropper density λ_E with secondary users and without secondary users. It is found that when i increases, the outage probability of secrecy capacity is higher. This result is due to the fact that when the primary receiver is farther away from the primary transmitter, the capacity between the primary transmitter and receiver will be smaller. Thus, the secrecy capacity becomes larger. Moreover, when the density of eavesdroppers λ_E increases, the outage probability of secrecy capacity will also increase. Comparing the case with secondary users to the case without secondary users, it is noticed that when λ_E is smaller than a certain threshold, the outage probability with secondary users is higher than that without secondary users. When λ_E exceeds a certain threshold, the outage probability with secondary users is smaller than that without secondary users. This result is because that the interference of the eavesdroppers from the secondary users is larger when the density of eavesdroppers becomes larger. Thus, the secrecy capacity can be larger in the network with secondary users than that of without secondary users.

Fig. 4 compares the secrecy outage probability versus the secondary user density λ_S with secondary users. Similar to Fig. 3, when i increases, the outage probability of secrecy capacity becomes larger. Moreover, when the density of secondary users λ_S increases, the outage probability of secrecy capacity will also increase. This means when the secondary users are denser, they will deteriorate the quality of the primary link more than that of the eavesdropper link.

V. Conclusion

In this paper, we considered the Poisson process of both the secondary users and the eavesdroppers and analyzed the impact of the stochastic interference on the fundamental limits of secure communications in a cognitive radio network. We discussed a network model with primary users, secondary users and eavesdroppers and investigated the secure communication graph from an information-theoretic perspective. Then, we analyzed the interference from the secondary users to the primary users and eavesdroppers. By taking account of interference we derived the secrecy capacity between a primary transmitter and receivers. From the theory of stochastic geometry, we showed how the spatial Poisson process of primary and eavesdropper nodes influence the secrecy capacity and outage probability between a node and its neighbors.

References

[1] J. Mitola. III, "Cognitive Radio for Flexible Mobile Multimedia Communications," *IEEE 1999 Mobile Multimedia Conference (MoMuC)*, pp. 3-10, Nov. 1999.

[2] I. F. Akyildiz, Y. Altunbasak, and F. Fekri, R. Sivakumar, "AdaptNet: adaptive protocol suite for next generation wireless internet," *IEEE Communications Magazine*, vol. 42, pp. 128-138, Jan. 2004.

[3] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security," *Proceedings of CrownCom 2008*.

[4] A. D. Wyner, "The wire-tap channel," *the Bell Systems Tech, Jl.*, vol. 54,no. 8, pp. 1355-1367, Oct.1975.

[5] J. N Barros and M. R. D. Rodrigues, "Secrecy Capacity of Wireless Channels," *International Symp. Information Theory (ISIT)*, pp. 356-360, Seattle, WA, Jul. 2006.

[6] P. K. Gopola, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels ," *IEEE Trans. on Information Theory*, vol. 54, no. 10, pp. 4687-4698, Sep. 2008.

[7] S. Ma, M. Hempel, Y. Yang, and H. Sharif, "A New Approach to Null Space-Based Noise Signal Generation for Secure Wireless Communications in Transmit-Receive Diversity Systems," *Proc. of IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS'10)*, pp. 406-410, Beijing, China, Jun. 2010.

[8] S. Ma, M. Hempel, Y. Yang, and H. Sharif, "A Novel Approach to Secure Wireless Communications Using Randomized Eigenvector-Based Jamming Signals," *Proc. of the 6th International Wireless Communications & Mobile Computing Conference (IWCMC'10)*, pp. 1172-1176, Caen,France, Jun. 2010.

[9] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *Information Theory and Application Workshop*, pp. 1-4, San Diego, CA, Jan. 2010.

[10] S. Anand, and R. Chandramouli, "On the Secrecy Capacity of Fading Cognitive Wireless Networks," *Cognitive Radio Oriented Wireless Networks and Communications, 2008.*, pp. 1-5, Singalpore, May. 2008.

[11] M. Vu, N. Devroye, M. Sharif, and V. Tarokh, "Achievable Rates and Scaling Laws for Cognitive Radio Channels," *EURASIP Journal on Wireless Communications and Networking, Special Issue on Cognitive Radio and Dynamic Spectrum Sharing Systems*, vol. 2008, Jan. 2007.

[12] 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 Jounal on Selected Areas in Communications*, vol. 27, no. 7, pp. 1029-1046, Sep. 2009.

[13] O. Dousse, F. Baccelli, and P. Thiran, "Impact of Interferences on Connectivity in Ad Hoc Networks," *IEEE/ACM Transactions on Networking*, vol. 13, Issue. 2, pp. 425-436, Apr. 2005.

[14] S. P. Weber, X. Yang, J. G. Andrews, and G. Veciana, "Transmission Capacity of Wireless Ad Hoc Networks with Outage Constraints," *IEEE Transaction on Information Theory*, vol. 51, no. 12, pp. 4091-4102, Dec. 2005.

[15] J. Kingman, *Poisson Processes*, Oxford University Press, 1993.

[16] J. A. McFadden, "The entropy of a point process," *Jounal of the Society for Industrial and Applied Mathematics*, vol. 13, no. 4, pp. 998-994, Dec. 1965.

[17] A. Goldsmith, *Wireless Communications*, Cambridge Universtiy Press, 2005.

[18] E. S. Sousa and J. A. Silvester, "Optimum Transmission Ranges in a Direct-Sequence Spread-Spectrum Multihop Packet Radio Network," *IEEE Jounal on Selected Areas in Communications*, vol. 8, no. 5, pp. 762-771, Jun. 1990.

[19] P. C. Pinto, J. Barros, and M. Z. Win, "Physical-Layer Security in Stochastic Wireless Networks," *International Conference on Communication Systems*, pp. 974-979, Nov. 2008.

[20] A Papoulis and S. U. Pillai, *Probability, Random Variables and Stochastic Process*, McGraw-Hill Higher Education, Fourth Edition, 2002.