On the Secrecy Capacity of Fading Cognitive Wireless Networks

S. Anand and R. Chandramouli
Department of ECE, Stevens Institute of Technology
{asanthan,mouli}@stevens.edu

Abstract— **In this paper, we compute the primary exclusive region (PER) and the secrecy capacity at a primary receiver in a fading cognitive radio network. We consider Rayleigh fading and log-normal shadowing. We also study the effect of secrecy capacity on the PER. We show that log-normal shadowing and Rayleigh fading can degrade the PER by about 40% and the secrecy capacity by about 70%.**

Keywords – Cognitive Radio Networks, Secrecy capacity, Primary Exclusive Region.

I. Introduction

The developments in software defined radio (SDR) [1] and cognitive radio networks [2] is expected to result in the paradigm of users sharing spectrums on an opportunistic basis. Users belonging to one network sense spectrum opportunities in another network and contend for the unused spectrum in this second network. The users thereby become "secondary" or "cognitive" users in the second network. Users that originally subscribed to the second network are called "primary users." The combined interference from all secondary transmitters to a primary receiver degrades the maximum throughput that can be obtained by a primary receiver and vice-versa. Vu *et al* obtained expressions for the primary exclusive region (PER) for a primary transmitter in a cognitive radio network without fading[1] [3]. The PER was obtained for a channel with no fading. In [4], Vu *et al* also extended their solution in [3] to obtain upper and lower bounds on the maximum capacity that can be obtained by a cognitive receiver. In addition to capacity, secrecy is another key performance factor that characterizes a cognitive wireless network. The notion of information theoretic secrecy capacity unifies both these factors.

Secrecy capacity was studied for systems with key-less security. A system typically consists of a source (or a transmitter), a destination (or a receiver) and an eavesdropper. The source transmits information which is received both by the receiver and the eavesdropper. Secrecy capacity is roughly the maximum rate at which the source can transmit such that the bit error rate (BER) at the destination approaches zero while that at the eavesdropper approaches 1/2. For some cases, the secrecy capacity is the difference between the Shannon capacity of the channel between the source and destination and that between the source and eavesdropper [5]. Wyner [5] first showed that positive secrecy capacity can be achieved without having a secret key of larger entropy than that of the message. Gopala *et al* extended Wyner's [5] work for fading wireless channels [6]. Tekin and Yener [7] studied multiple source-destination pairs and co-operative jamming. Multiple source-destination pairs was considered and the sum secrecy capacity of the network was maximized.

This is the first attempt to compute the secrecy capacity of a cognitive network to the best of our knowledge. In this paper, we extend the approach by Vu *et al* in [3] to first obtain the PER of cognitive radio networks operating on a fading wireless channel. We then extend the expressions obtained in [4] to obtain the secrecy capacity of a fading cognitive wireless network. We show that for a cognitive network with Rayleigh fading and log-normal shadowing, the PER can degrade by about 40% and the secrecy capacity can degrade by about 70% when compared to a system without shadowing and fading.

The rest of the paper is organized as follows. In Section II, we present the system model. In Sections III-A and III-B, we present the analysis for the PER and the secrecy capacity, respectively. In Section IV, we present the numerical results and discussion. Section V presents the conclusions.

II. System Model

Consider a cognitive radio network with primary and secondary/cognitive users[2] as shown in Fig. 1. In Fig. 1, the radius R_0 is the transmission range of a primary transmitter, that defines the primary exclusive region or primary exclusive radius (PER) and ϵ_p is the radius of the protected band which defines the region where cognitive transmitters are not allowed. This system model was also considered in [3] and [4]. As in [3] and [4], we consider a network with fixed node densities and a circular network with radius, R. We make the following considerations and assumptions in our analysis (see Fig. 1)

- There are m primary and n cognitive/secondary users.
- The entire network is a circular region of radius R. We then present our results with $R \to \infty$.
- Each primary receiver is within a radius of R_0 from the corresponding primary transmitter.
- In a circular region of radius R_0 centered at any primary transmitter, there are no other primary transmitters.
- There is guard band ϵ_p such that for any primary transmitter, the nearest cognitive transmitter is at a distance at least $R_0 + \epsilon_p$.

[1]Henceforth, throughout the paper, the term "fading" indicates Rayleigh fading and the term "shadowing" indicates log-normal shadowing unless explicitly mentioned otherwise.

[2]Henceforth, throughout the paper, the terms "secondary users" and "cognitive users" will be used interchangeably unless explicitly mentioned otherwise.

- The cognitive transmitters are uniformly distributed in the network with density λ_c users per unit area.
- The primary transmitters are uniformly distributed in the network with density λ_p users per unit area.
- Each cognitive receiver i is at a distance of at least ϵ_c from cognitive transmitter k ($k \neq i$).
- The signal from any transmitter to any receiver undergoes Rayleigh fading with mean Δ, log-normal shadowing and distance attenuation with path loss exponent, α.
- The positions of all the transmitters and receivers and the channel conditions between any pair of transmitters and receivers are statistically independent of each other.
- Primary transmitters transmit at a fixed power P_0 and cognitive transmitters at a fixed power P and $P < P_0$.
- The channel introduces additive white Gaussian noise with power spectral density (psd), N_0.

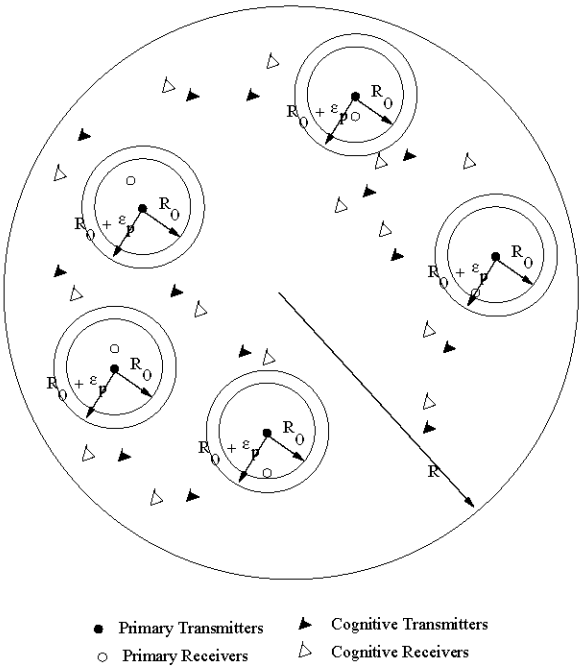

Fig. 1. A cognitive radio network with primary and secondary/cognitive transmitters and receivers.R_0 is the primary exclusive region (PER) and ϵ_p is the guard band between a primary receiver and a cognitive transmitter/receiver.

III. Evaluation of the PER and the Secrecy Capacity

We first present the analysis to evaluate the PER for a cognitive radio network with fading and shadowing in addition to distance attenuation in Section III-A. We then use the same to derive bounds on the secrecy capacity, in Section III-B.

The Shannon capacity, $C_p^{(i)}$, of the wireless channel between the i^{th} primary transmitter and i^{th} primary receiver can be obtained from the signal-to-interference ratio (SIR), $\gamma_p^{(i)}$, as

$$C_p^{(i)} = W \log_2 \left(1 + \gamma_p^{(i)}\right), \tag{1}$$

where W is the system bandwidth. The SIR, $\gamma_p^{(i)}$ is then given by

$$\gamma_p^{(i)} = \frac{S_{ii}}{N_0 W + I_p + I_c}, \tag{2}$$

where

$$S_{ii} = P_0 \left(\delta_p^{(ii)}\right)^2 \left(G_p^{(ii)}\right)^2 \left(d_p^{(ii)}\right)^{-\alpha}, \tag{3}$$

$$I_p = \sum_{\substack{k=1 \\ k \neq i}}^{m} P_0 \left(\delta_p^{(ki)}\right)^2 \left(G_p^{(ki)}\right)^2 \left(d_p^{(ki)}\right)^{-\alpha}, \tag{4}$$

and

$$I_c = \sum_{j=1}^{n} P \left(\delta_c^{(ji)}\right)^2 \left(G_c^{(ji)}\right)^2 \left(d_c^{(ji)}\right)^{-\alpha}, \tag{5}$$

In (3), (4) and (5), $\left(\delta_p^{(ki)}\right)^2$ is the Rayleigh fading term from the k^{th} primary transmitter to the i^{th} primary receiver, $\left(\delta_c^{(ji)}\right)^2$ is the Rayleigh fading term from the j^{th} cognitive transmitter to the i^{th} primary receiver, $\left(G_p^{(ki)}\right)^2$ is the log-normal shadowing term from the k^{th} primary transmitter to the i^{th} primary receiver, $\left(G_c^{(ji)}\right)^2$ is the log-normal shadowing term from the j^{th} cognitive transmitter to the i^{th} primary receiver, $d_p^{(ki)}$ is the distance between the k^{th} primary transmitter and the i^{th} primary receiver and $d_c^{(ji)}$ is the distance between the j^{th} cognitive transmitter and the i^{th} primary receiver. $\left(G_p^{(ki)}\right)^2$ and $\left(G_c^{(ji)}\right)^2$ are of the form $10^{-\frac{\xi}{10}}$ $\forall$ k, j, where $\xi \sim \mathcal{N}(0, \sigma^2)$ [8]. For analytical simplicity and convenience in following the analysis, we consider the interference to a primary receiver 1 without loss of generality.

A. Evaluation of the Primary Exclusive Region

As in [3], the outage is defined as the event that the capacity of the channel between primary transmitter 1 and primary receiver 1 is below a specified threshold, C_p^{th}. It is desired that the probability of outage be less than a pre-specified quantity, β. Hence, it is essential to evaluate the value of R_0 and ϵ_p such that

$$\Pr\{C_p < C_p^{th}\} < \beta, \tag{6}$$

where $C_p = C_p^{(1)}$ and the super-script (1) is dropped for convenience. The maximum value of R_0 satisfying (6) is called the PER.

In order to evaluate the outage probability in (6), it is essential to obtain the average interference $E[I_p]$ and $E[I_c]$. As in [3], the positions of the cognitive transmitters are uniformly distributed in in the annular region $(R_0 + \epsilon_p, R)$. In order to obtain the expression for $E[I_c]$, we model I_c as a log-normal random variable of the form $10^{-\frac{\Omega_n}{10}}$, where $\Omega_n \sim \mathcal{N}(\mu_{nc}, \sigma_{nc}^2)$. Each term in the summation in the right hand side of (5) is a log-normally distributed random variable when conditioned on the position of the cognitive transmitter

and the Rayleigh fading term. Thus, each term in the summation on the right hand side of (5) is of the form $10^{-\frac{\xi_j}{10}}$ where $\xi_j \sim \mathcal{N}(\mu_j, \sigma^2)$, where μ_j is given by

$$\mu_j = 10\log_{10}\left[\left(d_c^{(j)}\right)^{-\alpha}\right] + 10\log_{10}\left[\left(\delta_c^{(j)}\right)^2\right], \quad (7)$$

where $\delta_c^{(j)} = \delta_c^{(ji)}$ and $d_c^{(j)} = d_c^{(ji)}$, with the super-script i omitted since the interference is calculated for primary user 1. The sum of log-normal random variables can be approximated to be a log-normal random variable using Fenton's method [9]. The mean μ_{nc} and variance σ_{nc}^2 by applying the approximation in [9] can then be obtained as

$$\sigma_{nc}^2 = \frac{1}{a^2}\ln\left(1 + \frac{e^{a^2\sigma^2} - 1}{n}\right), \quad (8)$$

and

$$\mu_{nc} = \mu_j + \frac{a\left(\sigma_n^2 - \sigma^2\right)}{2} - \frac{1}{a}\ln n. \quad (9)$$

In (8) and (9), $a = \frac{\ln 10}{10}$. In obtaining the expressions in (8) and (9), we assumed as in [3] that each term in the right hand side of the summation in (5) are independent and identically distributed (i. i. d). $E[I_c]$ can then be obtained by evaluating the mean of the log-normally distributed random variable, I_c, as

$$E[I_c] = n\exp\{-a\mu_n + \frac{1}{2}a^2\sigma_n^2\}, \quad (10)$$

which, from (8) and (9) can be written as

$$E[I_c] = n\Delta e^{\frac{1}{2}a^2\sigma^2} E\left[\left(d_c^{(ji)}\right)^{-\alpha}\right]. \quad (11)$$

The term $E\left[\left(d_c^{(ji)}\right)^{-\alpha}\right]$ in (11) was evaluated in [3]. Hence, using the results in [3], the mean interference from all cognitive users to a primary user, $E[I_c]$, can be obtained as

$$E[I_c] = \lambda_c \Delta e^{\frac{1}{2}a^2\sigma^2} \int_{R_0+\epsilon_p}^{R} \frac{rdrd\theta}{\left(r^2 + R_0^2 - 2rR_0 cos\theta\right)^{\frac{\alpha}{2}}}, \quad (12)$$

where, (r, θ) denotes the location of the cognitive transmitter (which is uniformly distributed in the annular region $(R_0 + \epsilon_p, R)$) in polar co-ordinates. For $\alpha = 4$, the integral in (12) was obtained in closed form in [3]. Using the results in [3], $E[I_c]$ can be obtained as

$$E[I_c] = \lambda_c \pi \Delta e^{\frac{1}{2}a^2\sigma^2}\left[\frac{\left(R_0 + \epsilon_p\right)^2}{\epsilon_p^2\left(2R_0 + \epsilon_p\right)^2} - \frac{R^2}{\left(R^2 - R_0^2\right)^2}\right]. \quad (13)$$

Similarly, the mean interference to a primary receiver from all primary transmitters, $E[I_p]$, can be evaluated by replacing ϵ_p by R_0 and λ_c by λ_p in (12) and (13). From (1) and (2),

$$\Pr\{C_p < C_p^{th}\} \quad \leq \quad \Pr\{I_p + I_c > \nu\}, \quad (14)$$

where $\nu = P_0 R_0^{-\alpha}\left(2^{\frac{C_p^{th}}{W}} - 1\right)^{-1} - N_0 W$. As in [3], (14) can be written using Markoff's inequality [10] as

$$\Pr\{C_p < C_p^{th}\} \leq \frac{E[I_p] + E[I_c]}{\nu} \quad (15)$$

The R_0 that maximizes $E[I_p] + E[I_c]$ but keep the expression in (15) less than β is the PER.

It is observed from (11)-(15) that the mean interference $E[I_c]$ and $E[I_p]$ are similar to the expressions in [3] (in which a wireless channel without fading and shadowing was considered), except that they are scaled by a factor $\Delta e^{\frac{1}{2}a^2\sigma^2}$. Therefore, we observe that the Rayleigh fading term degrades the SIR by a linear factor while the log-normal shadowing degrades the SIR exponentially.

B. Evaluation of the Secrecy Capacity

In order to evaluate the secrecy capacity, we assume that the eavesdropper is passive and is one of the secondary receivers. The reason for this is that we assume that the network has some mechanism to integrity protect the primary users and hence, any passive eavesdropper can only be a secondary user. The other assumptions in Section II also hold in addition to the assumption made in this sub-section.

Consider a cognitive user who is also an eavesdropper. Without loss of generality, let the main channel be the channel between primary transmitter 1 and receiver 1. The eavesdropper receives the signal from the primary transmitter and interference from other primary transmitters and cognitive transmitters. Let γ_c be the SIR experienced by the eavesdropper. The capacity of the channel between the primary transmitter 1 and the eavesdropper be C_s. Similar to (1), C_s can be written as

$$C_s = W\log_2\left(1 + \gamma_c\right), \quad (16)$$

where, similar to (2), γ_c can be written as

$$\gamma_c = \frac{S_c}{N_0 W + \hat{I}_p + \hat{I}_c}, \quad (17)$$

where S_c is the received signal at the eavesdropper from the primary transmitter 1, $\hat{I}_p$ is the interference experienced at the eavesdropper due to other primary transmitters and $\hat{I}_c$ is the interference experienced by the eavesdropper due to the cognitive transmitters. The expressions for S_c, $\hat{I}_p$ and $\hat{I}_c$ are similar to the ones in (3), (4) and (5), respectively.

The secrecy capacity of the primary receiver, $S_e^{(p)}$, is then given by

$$S_e^{(p)} = C_p - C_s. \quad (18)$$

The position of the primary receiver and the eavesdropper are statistically independent of each other. Also, the Rayleigh fading and the log-normal shadowing experienced by the primary receiver and the eavesdropper from all transmitters are statistically independent of each other as mentioned in Section II. Hence, the minimum secrecy capacity, S_e^{min} can be written as

$$S_e^{min} = \min C_p - \max C_s, \quad (19)$$

where the minimum and maximum are with respect to the interference experienced and the distances from the primary transmitter. In order to compute the minimum and the maximum mean interference, the bounds provided in [4] for the system with no fading and log-normal shadowing has to be

extended for the system with shadowing and fading. Using the arguments in Section III-A, we see that these bounds can be obtained by scaling the bounds in [4] by a factor of $\Delta e^{\frac{1}{2}a^2\sigma^2}$.

It is observed that the minimum secrecy capacity will be experienced by the primary receiver when it is located farthest from the transmitter and the eavesdropper is located as near to the transmitter as possible. This scenario occurs when the primary receiver is at a distance R_0 and the eavesdropper is at a distance $R_0+\epsilon_p$. Following the argument in [4], C_p^{min} is given by

$$C_p^{min} = W\log_2\left(1+\frac{P_0 R_0^{-\alpha}}{N_0 W + E[I_p] + E[I_c]}\right), \quad (20)$$

where $E[I_p]$ and $E[I_c]$ are obtained as in Section III-A. For $\alpha = 4$, the expression in (13) is used. For $\alpha \neq 4$, $E[I_p]$ and $E[I_c]$ are replaced by their upper bounds, $E[I_c]^{\mathrm{UB}}$ and $E[I_p]^{\mathrm{UB}}$, respectively. $E[I_c]^{\mathrm{UB}}$ for the fading cognitive network is obtained by scaling the expression in [4] by a factor $\Delta e^{\frac{1}{2}a^2\sigma^2}$ as

$$E[I_c]^{\mathrm{UB}} = \frac{\Delta e^{\frac{1}{2}a^2\sigma^2} 2\pi\lambda_c P}{\alpha-2}\left(\frac{1}{\epsilon_p^{\alpha-2}} - \frac{1}{(R+R_0)^{\alpha-2}}\right). \quad (21)$$

$E[I_p]^{\mathrm{UB}}$ is obtained by replacing λ_c by λ_p, P by P_0 and ϵ_p by R_0 in (21). C_s^{max} can be obtained as

$$C_s^{max} = W\log_2\left(1+\frac{P_0\left(R_0+\epsilon_p\right)^{-\alpha}}{N_0 W + E[I_c]^{\mathrm{LB}} + E[I_p]^{\mathrm{LB}}}\right). \quad (22)$$

In the above, $E[I_c]^{\mathrm{LB}}$ can be obtained by scaling the expression in [4] by a factor $\Delta e^{\frac{1}{2}a^2\sigma^2}$ as

$$E[I_c]^{\mathrm{LB}} = \frac{\Delta e^{\frac{1}{2}a^2\sigma^2} P\lambda_c}{\alpha-2}\left(\frac{A(\alpha)}{\epsilon_p^{\alpha-2}} - \frac{A(\alpha)}{(2R_0+\epsilon_p)^{\alpha-2}} - \frac{\pi}{R^{\alpha-2}}\right), \quad (23)$$

where $A(\alpha)$ is given by

$$A(\alpha) = \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \cos^{\alpha-2}(\phi)d\phi. \quad (24)$$

$E[I_p]^{\mathrm{LB}}$ can be obtained by replacing P by P_0, λ_c by λ_p and ϵ_p by R_0 in (23).

IV. Results and Discussion

For numerical computations we consider a system with an infinite area, i. e., $R \to \infty$. We first present the results for the maximum value of the outage probability with respect to R_0 and then present the results for the secrecy capacity. We consider the following values as in [3] for the various parameters: $\alpha = 4$, $\lambda_c = 1$, $\lambda_p = 2$, $\epsilon_p = 2$, $\epsilon_c = 3$, $P_0 = 2$, $P = 1$, $W = 5$ MHz, $C_p^{th} = 2$ Mbps, $\Delta = 1$ and $\sigma = 8$ dB [8].

Fig. 2 presents the bound specified in (15) for the outage probability for various values of R_0. It is observed that the shadowing and the Rayleigh fading play a significant role in degrading the outage probability, and hence, the PER. For example, for an outage probability of 0.2, the PER without shadowing is 10 units whereas, with shadowing and fading, the PER is 6 units, thus resulting in a degradation of about 40% in the PER.

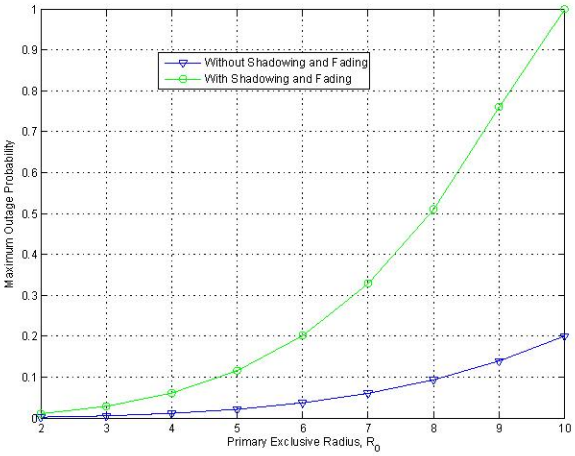

Fig. 2. Maximum outage probability (specified in (15)) with respect to the PER, R_0, for $\Delta = 1$ and $\sigma = 8$ dB.

Fig. 3 shows the variation of the minimum secrecy capacity, S_e^{min} in (19) for various values of R_0. It is observed again that shadowing and fading play significant roles in degrading the secrecy capacity. For $R_0 = 4$, the secrecy capacity for a primary user without shadowing and fading is about 75 Kbps, whereas, with shadowing and fading, the secrecy capacity is about 20 Kbps, resulting in a degradation of about 73%. It is also observed that for an outage threshold of 0.2, $R_0 = 10$ without shadowing and fading and $R_0 = 6$ with shadowing and fading. However, if an additional constraint of $S_e^{min} = 50$ Kbps is imposed, then, $R_0 = 4$ without shadowing and fading, and $R_0 = 2$ with shadowing and fading. Thus the additional constraint on secrecy further impacts the PER.

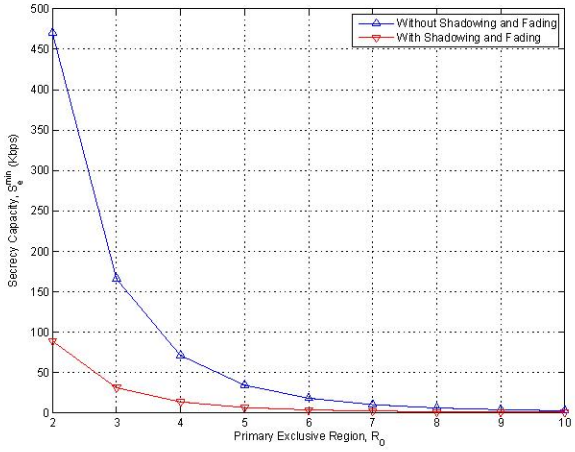

Fig. 3. Secrecy Capacity, S_e^{min} (specified in (19)) with respect to the PER, R_0, for $\Delta = 1$ and $\sigma = 8$ dB.

Figs. 4 and 5 depict the behaviors of the bound in (15) with respect to the standard deviation of the shadowing σ, and the mean Rayleigh fading Δ, respectively, for $R_0 = 4$. It is observed that while the degradation in the outage probability with respect to the mean Rayleigh fading is close to a linear

behavior, the degradation with respect to the shadowing is non-linear. This is because, as mentioned in Section III-A, (11)-(15) scale linearly with respect to Δ and exponentially with respect to σ^2. Figs. 6 and 7 show the behavior of the minimum secrecy capacity, S_e^{min}, with respect to the standard deviation of the shadowing σ and the mean Rayleigh fading Δ, respectively for $R_0 = 4$.

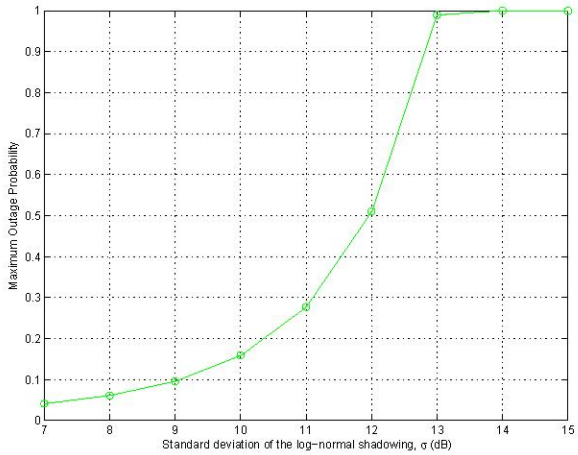

Fig. 4. Maximum outage probability (in (15)) with respect to the standard deviation of the log-normal shadowing, σ, for $\Delta = 1$ and $R_0 = 4$.

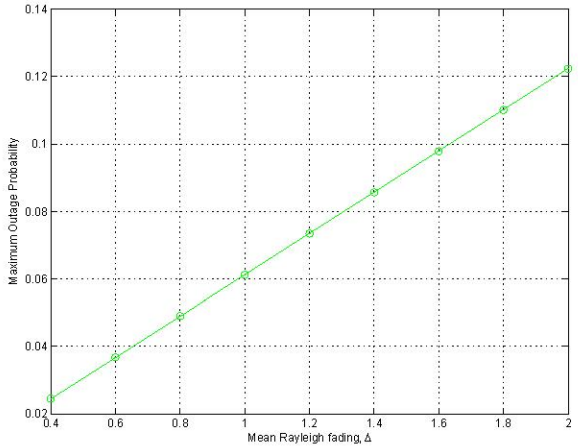

Fig. 5. Maximum outage probability (in (15)) with respect to the mean Rayleigh fading Δ, for $\sigma = 8$ dB and $R_0 = 4$.

V. Conclusion

We computed the primary exclusive region (PER) and the secrecy capacity at a primary receiver in a cognitive radio network. We also studied the effect of secrecy capacity on the PER. We showed that shadowing and fading can degrade the PER by about 40% and the secrecy capacity by about 70%. Our approach can also be extended to study cognitive networks with power control and to systems with Ricean fading.

ACKNOWLEDGMENT

This work was partially supported by grants from the U.S. Armament Research Development and Engineering Command, Picatinny, NJ and a National Science Foundation (NSF) CA-REER Award.

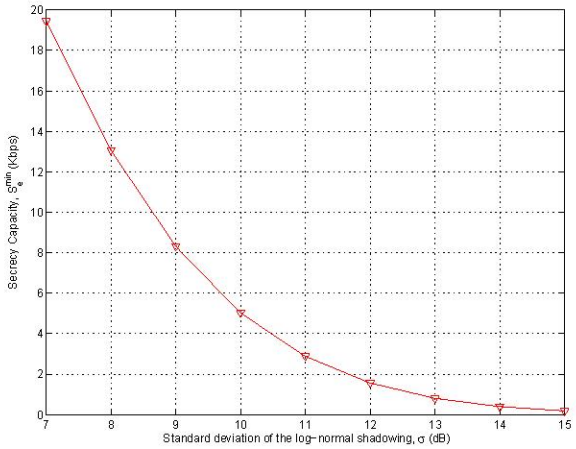

Fig. 6. Secrecy Capacity, S_e^{min} (in (19)) with respect to the standard deviation of the log-normal shadowing, σ, for $\Delta = 1$ and $R_0 = 4$.

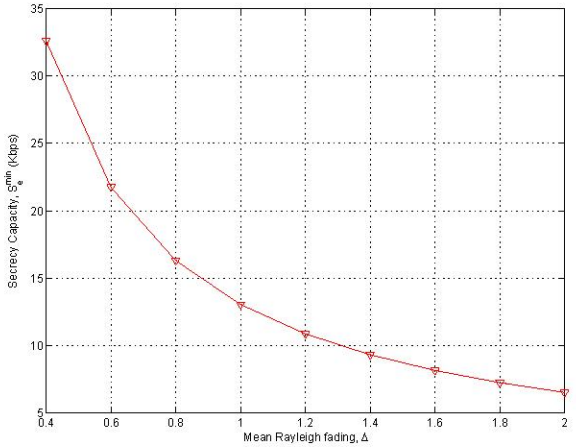

Fig. 7. Secrecy Capacity, S_e^{min} (in (19)) with respect to the mean Rayleigh fading, Δ, for $\sigma = 8$ dB and $R_0 = 4$.

References

[1] A. Harrington, C. Hong, and T. Piazza "Software defined radio: The revolution of wireless communication," *White paper, Ball State University,* http://www.bsu.edu/cics/alumni/whitepapers/

[2] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio: A survey *Elsevier Jl. on Computer Networks,* vol. 50, pp. 2127-2158, May 2006.

[3] M. Vu, N. Devroye and V. Tarokh, "Primary exclusive region in cognitive networks," *Proc., IEEE Consumer Commun. and Networking Conf (CCNC'2008),* January 2008.

[4] M. Vu, N. Devroye, M. Sharif and V. Tarokh, "Scaling laws of cognitive networks," *Submitted to IEEE Jl. on Sel. Topics in Signal Proc.*

[5] A. D. Wyner, "The wire-tap channel," *Bell Systems Tech, Jl.,* vol. 54, no. 8, pp. 1355-1387, 1995.

[6] P. K. Gopala, L. Lai, H. Elgamal, "On the secrecy capacity of fading channels," *Accepted in IEEE Trans. on Info. Theory.*

[7] E. Tekin and A. Yener, "The general Gaussian multiple access and two way wiretap channels: Achievable capacity and co-operative jamming," *IEEE Trans, on Info. Theory, Spl. Issue on Info. Theoretic Security.*

[8] T. S. Rappaport, *Wireless Communications: Principles and Practice,* Prentice Hall, New Jersey, 1996.

[9] L. F. Fenton, "The sum of log-normal probability distributions in scatter transmission systems," *IRE Trans. on Commun. Systems,* CS-8, pp. 57-67, March 1960.

[10] S. Ross, *Probability Models,* Academic Press, 2003.