An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks

S. Anand, Z. Jin and K. P. Subbalakshmi
Department of Electrical and Computer Engineering
Stevens Institute of Technology, New Jersey, USA

***Abstract*— In this paper, we study the denial-of-service (DoS) attack on secondary users in a cognitive radio network by primary user emulation (PUE). Most approaches in the literature on primary user emulation attacks (PUEA) discuss mechanisms to deal with the attacks but not analytical models. Simulation studies and results from test beds have been presented but no analytical model relating the various parameters that could cause a PUE attack has been proposed and studied. We propose an analytical approach based on Fenton's approximation and Markov inequality and obtain a lower bound on the probability of a successful PUEA on a secondary user by a set of co-operating malicious users. We consider a fading wireless environment and discuss the various parameters that can affect the feasibility of a PUEA. We show that the probability of a successful PUEA increases with the distance between the primary transmitter and secondary users. This is the first analytical treatment to study the feasibility of a PUEA.**

Keywords – Cognitive radio networks malicious user, primary user emulation attack

I. Introduction

Spectrum sharing has always been an important aspect of system design in wireless communication systems due to the scarcity of the available resources/spectrum. Cognitive radio networks [1] enable usage of unused spectrum in a network, **A**, by users belonging to another network, **B**. These users thereby become "secondary users" to the network **A**. The users that originally subscribed to the network **A** are called "primary users" of network **A**. One example of cognitive radio network is the usage of white spaces (or unused spectrum) in the television (TV) band. The TV transmitter then becomes a primary transmitter and TV receivers are primary receivers. Other users who are not TV subscribers but wish to use the white spaces in the TV band for their own communication become secondary transmitters/receivers. The IEEE 802.22 working group on wireless regional area networks (WRAN) [2] provide the physical layer (PHY) and medium access control (MAC) specifications for usage of the TV white spaces. More details on the IEEE 802.22 can be found in [3], [4]. The developments in software defined radio (SDR) [5] enables implementation of re-configurable MAC for dynamic spectrum access (DSA). Akyildiz *et al* [6] provide a detailed survey of the developments in SDR, DSA and cognitive radio. The etiquette followed in cognitive radios is that the secondary users evacuate the used spectrum once they detect a primary transmission. In [6], the authors also provide a detailed description of the different sensing mechanisms that enable secondary users to detect the presence of a primary user namely: (a) Transmitter detection, (b)co-operative detection and (c) interference-based detection. Transmitter detection, in turn, can be performed using one of three mechanisms namely: (i) matched filter detection, (ii) energy detection and (iii) cyclostationary feature detection. A detailed description and comparative study of the above methods are also provided in [6]. Protocols for sensing primary transmission and evacuating the spectrum were discussed by Visotsky *et al* [4] and by Liu and Ding [7].

The etiquette of spectrum evacuation could however result in denial-of-service attacks on secondary users if the system is not carefully designed. This is explained as follows. Consider a set of secondary users in the system. A subset of users could forge the essential signal characteristics of the primary and generate enough power at the good secondary user locations to confuse the secondaries into thinking that a primary transmission is under way. The secondaries obeying the normal etiquette will vacate the spectrum unnecessarily. The subset of users would then use the evacuated white space for themselves. The secondary users who transmit to emulate the primary transmitter are referred to as "malicious users" while the other secondary users who evacuate the spectrum upon sensing the transmission from the primary transmitter or the malicious users are termed as "good" secondary users[1]. Such an attack by malicious users on secondary users is called a primary user emulation attack (PUEA). It is noted that such attacks could lead to big disadvantages because several good users could lose access to the network due to the presence of a few malicious users. This, in turn, leads to poor usage of spectrum for authorized users and an unfair advantage for the malicious users.

PUEA in cognitive radio networks was studied in [8],[9],[10]. In [8], Chen and Park propose two mechanisms to detect a PUEA namely the distance ratio test (DRT) and the distance difference test (DDT), which use the ratio and the difference, respectively, of the distances of the primary and malicious transmitters from the secondary user to detect a PUEA. In [9], Chen *et al* discuss defense against PUEA by localization of primary transmitters. Directional antennas were proposed to determine the angle of arrival of the primary

This work was funded by a research grant from NSF Cyber Trust Grant No. 0627688

[1]Henceforth, throughout the paper, whenever we mention "secondary users", we refer to "good secondary users" unless explicitly mentioned otherwise.

signal, and using this, the time of arrival and the received signal strength, the secondary users determine the location of the primary transmitter. A different kind of threat albeit not directly a PUEA, was discussed by Chen *et al* in [10]. The authors consider a system where spectrum sensing is done and a hypothesis testing method is used to detect a transmission, which in the case of cognitive radio networks could be a primary transmission. A Byzantine failure model due to fraudulent reporting of spectrum sensing was discussed and a weighted sequential ratio test was proposed to overcome this attack.

In most approaches, the detection of PUEA depends on the determination of the location of the primary transmitter, which, in turn, depends on the direction of signal arrival. The dependence on the directionality of the antennas at the receiver makes the detection process complex because most of the incumbent receivers in wireless and cellular networks use omni directional antennas.

We present the first ever analytical treatment of the feasibility of a PUEA. We derive mathematical expressions for the probability of a successful PUEA and provide lower bounds on the probability of a successful attack using Fenton's approximation and Markov inequality. We consider a wireless environment with losses due to attenuation, fading and shadowing. We consider a variation of the energy detection mechanism mentioned in [6]. We model the received power at a secondary user as a log-normally distributed random variable and use Fenton's approximation to determine the mean and the variance of the received power. We then use the value of the derived mean and variance to determine a lower bound on the probability of a successful PUEA using Markov inequality. We discuss the various parameters that can affect the feasibility of a PUEA. We show that the probability of a successful PUEA increases with the distance between the primary transmitter and secondary users. The rest of the paper is organized as follows. In Section II, we present the system model. Section III presents the analytical model for the probability of a successful PUEA. In Section IV, we present the numerical results and discussion. Section V presents the conclusion.

II. System Model

Consider a system as shown in Fig. 1. All secondary and malicious users are distributed in a circular grid of radius R. A primary transmitter is present at a distance of at least D_p from all the users. The energy detection method for spectrum sensing by secondary users in as follows [6]. Each secondary user measures the energy of the received signal and compares the measured energy with a pre-set threshold, Λ. If the measured energy is greater than Λ, then the secondary user concludes that a primary transmission is present. Else, the secondary user concludes that the spectrum is free for usage. We consider a variation of this method for spectrum sensing, where each secondary user measures the received power and compares them with two thresholds, ϵ_l and ϵ_h. If the measured signal power lies between ϵ_l and ϵ_h, then the secondary user concludes that a primary transmission is present and refrains from using the spectrum. Otherwise, the secondary users concludes that there exists a white space. The reason for such a mechanism is that the measurement threshold for typical cognitive radio system is -93 dBm [2]. If the measurement is based on a single energy threshold, then even a single malicious user transmitting at sufficiently large power can cause a successful PUEA. In this case also, a set of malicious users can transmit in such a way that the total received power at a good secondary user due to the transmission by all the malicious users is very close to that due to the transmission from the primary transmitter, thus resulting in a primary user emulation attack (PUEA). A successful PUEA is defined as the event that the absolute difference between the received powers from the primary and that from all the malicious users is below a specified threshold, ϵ. It is of interest to determine the probability of a successful PUEA at any secondary user. We make the following assumptions for our analysis.

- There are M malicious users and N good secondary users in the system.
- The primary transmitter is at a minimum distance of D_p from all the users.
- The primary transmitter transmits at a power P_t.
- The malicious users transmit at a power P_m. (Typically, $P_m << P_t$).
- The positions of the good and malicious users are uniformly distributed in the circular grid of radius R.
- The co-ordinates[2] of the primary transmitter are fixed at a point (r_p, θ_p) and this position is known to all the users in the grid.
- The positions of the good users and the malicious users are statistically independent of each other.
- The RF signals from the primary transmitter and the malicious users undergo path loss, log-normal shadowing and Rayleigh fading.
- The shadowing random variable from the primary transmitter to the i^{th} secondary user is $\left(G_p^{(i)}\right)^2 = 10^{\frac{\xi_p^{(i)}}{10}}$, where $\xi_p^{(i)} \sim \mathcal{N}\left(0, \sigma_p^2\right)$.
- The shadowing random variable from the j^{th} malicious user to the i^{th} secondary user is $(G_{ij})^2 = 10^{\frac{\xi_{ij}}{10}}$, where $\xi_{ij} \sim \mathcal{N}\left(0, \sigma_m^2\right)$.
- The Rayleigh fading random variables from the primary transmitter and all malicious users to all secondary users are identically distributed with mean Δ.
- We consider a free space propagation model for the signal from the primary transmitter and a two-ray ground model for the signal from the malicious users thus resulting in a path loss exponent of 2 for the propagation from the primary transmitter and a path loss exponent of 4 for the propagation from the malicious users. This is because, the primary transmitter is so far away from the secondary and malicious users that the signal due to multi-path can be neglected. However, the distances from malicious users are not large enough to ignore the effects of multi-path.
- For any secondary user fixed at co-ordinates (r, θ), no

[2]Throughout this paper, whenever we mention "co-ordinates" we mean "polar co-ordinates" unless explicitly mentioned otherwise.

malicious users are present within a circle of radius R_0 centered ar $(r\theta)$. If this restriction is not posted, then the power received due to transmission from any subset of malicious users present within this grid will be much larger than that due to a transmission from a primary transmitter thus resulting in a failed PUEA all the time. On the other hand, if the malicious users deploy power control, then the malicious user present in this grid can modify its transmit power in such a way so that the PUEA is successful all the time. The distance R_0 is called the "exclusive distance from the secondary user".

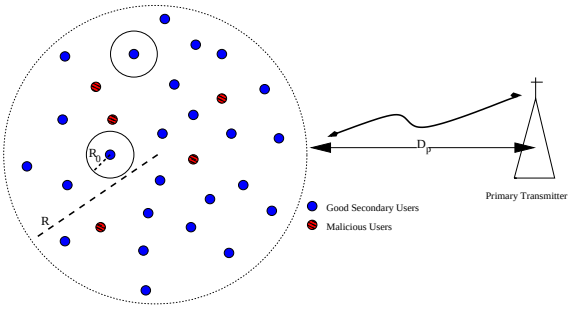

Fig. 1. A typical cognitive radio network in a circular grid with secondary and malicious users.

III. Analytical Model

The received power at the i^{th} secondary user from the primary transmitter, $P_r^{(p)}(i)$, is given by

$$P_r^{(p)}(i) = P_t \left(d_p^{(i)}\right)^{-2} \left(G_p^{(i)}\right)^2 \left(R_p^{(i)}\right)^2, \quad (1)$$

where $d_p^{(i)}$ is the distance from the primary transmitter to the i^{th} secondary user, $\left(G_p^{(i)}\right)^2$ is the log-normal shadowing from the primary transmitter to the i^{th} secondary user and $R_p^{(i)}$ is the Rayleigh fading from the primary transmitter to the i^{th} secondary user. The received power at the i^{th} secondary user due to the transmission from all the malicious users, $P_r^{(m)}(i)$, is given by

$$P_r^{(m)}(i) = \sum_{j=1}^{M} P_m d_{ij}^{-4} \left(G_{ij}\right)^2 \left(R_{ij}\right)^2, \quad (2)$$

where d_{ij} is the distance from the j^{th} malicious user to the i^{th} secondary user, $(G_{ij})^2$ is the log-normal shadowing from the j^{th} malicious user to the i^{th} secondary user and R_{ij} is the Rayleigh fading from the j^{th} malicious user to the i^{th} secondary user. A PUEA on the i^{th} secondary user is deemed successful if for a specified threshold, ϵ,

$$\left|P_r^{(p)}(i) - P_r^{(m)}(i)\right| < \epsilon. \quad (3)$$

The probability of a successful PUEA on the i^{th} secondary user is given by

$$p_{PUEA} = \Pr\left\{\left|P_r^{(p)}(i) - P_r^{(m)}(i)\right| < \epsilon\right\}. \quad (4)$$

Conditioned on the positions of the secondary and malicious users and the Rayleigh fading terms from the primary and all the malicious users, $P_r^{(p)}(i)$ and each term in the summation of the right hand side in Eqn. (2) are log-normally distributed random variables. $P_r^{(m)}(i)$ can be approximated as a log-normally distributed random variable whose mean and variance can be obtained by using Fenton's method [11]. A detailed description of Fenton's method is provided in Appendix I.

Let $P_r^{diff}(i) \triangleq P_r^{(p)}(i) - P_r^{(m)}(i)$. The random variable $P_r^{diff}(i)$ is modeled as a log-normally distributed random variable of the form $P_r^{diff}(i) = 10^{\frac{\omega^d(i)}{10}}$, where $\omega^d(i) \sim \mathcal{N}\left(\mu_d(i), \sigma_d^2(i)\right)$. Fenton's method needs to be applied again to obtain the values of $\mu_d(i)$ and $\sigma_d^2(i)$. Conditioned on the Rayleigh fading random variables from the primary and all the malicious users to the secondary user i and the positions of the secondary user and all the malicious users, the probability of a successful PUEA, $\hat{p}_{PUEA}$, can be obtained as

$$\hat{p}_{PUEA} = 1 - Q\left(\frac{\epsilon_{dB} + \mu_d(i)}{\sigma_d(i)}\right) - Q\left(\frac{\epsilon_{dB} - \mu_d(i)}{\sigma_d(i)}\right), \quad (5)$$

where ϵ_{dB} is the threshold ϵ expressed in decibels (i. e., $\epsilon_{dB} = 10\log_{10}\epsilon$) and $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{y^2}{2}}dy$. The probability of a successful PUEA, p_{PUEA} defined in Eqn. (4) can be obtained by averaging $\hat{p}_{PUEA}$ in Eqn. (5) over the positions of the secondary and malicious users and the Rayleigh fading from the primary and all the malicious users to the secondary user. For M malicious users, this results in $2M$ integrations corresponding to the positions of the malicious users (since each position has two co-ordinates), two integrations corresponding to the position of the secondary user, M integrations corresponding to the Rayleigh fading from all the malicious users to the secondary user and one integration corresponding to the Rayleigh fading from the primary transmitter to the secondary user. Thus, a total of $3(M+1)$ integrations needs to be performed for M malicious users. Therefore, exact evaluation of the probability in Eqn. (4) is very complex. Hence, we use the Markov inequality [12] to bound the probability.

Consider a random variable X such that $\Pr\{X < 0\} = 0$. For any $\alpha > 0$, the Markov inequality is [12]

$$\Pr\{X > \alpha\} \leq \frac{E[X]}{\alpha}. \quad (6)$$

Using this, the probability p_{PUEA} in Eqn. (4) can be bounded as

$$p_{PUEA} \geq 1 - \frac{\left|E\left[P_r^{(p)}(i)\right] - E\left[P_r^{(m)}(i)\right]\right|}{\epsilon}. \quad (7)$$

To evaluate the expectations in the above, we adopt an approach based on Fenton's approximation. This is described in detail as follows. As mentioned earlier, conditioned on the position of the secondary user, the received power at a secondary user due to the primary transmission is a log-normally distributed random variable. The mean $E\left[P_r^{(p)}(i)\right]$ is then given by

$$E\left[P_r^{(p)}(i)\right] = P_t \Delta e^{\frac{1}{2}a^2\sigma_p^2} E\left[\left(d_p^{(i)}\right)^{-2}\right], \quad (8)$$

where $a = \frac{\ln 10}{10}$. The distance $d_p^{(i)}$ is given by

$$d_p^{(i)} = \sqrt{r_i^2 + r_p^2 - 2r_i r_p \cos(\theta_i - \theta_p)}, \tag{9}$$

where (r_i, θ_i) are the co-ordinates of the i^{th} secondary user and (r_p, θ_p) are the co-ordinates of the primary transmitter. The expectation, $E\left[\left(d_p^{(i)}\right)^{-2}\right]$, in Eqn. (8) can be evaluated as

$$E\left[\left(d_p^{(i)}\right)^{-2}\right] = \frac{1}{\pi R^2} \int_{r_i=0}^{R}\int_{\theta_i=0}^{2\pi} \frac{r_i dr_i d\theta_i}{\left[r_i^2 + r_p^2 - 2r_i r_p \cos(\theta_i - \theta_p)\right]}. \tag{10}$$

The expression in Eqn. (10) is substituted in Eqn. (8) to obtain the value of $E\left[P_r^{(p)}(i)\right]$.

To evaluate $E\left[P_r^{(m)}(i)\right]$ we first note that conditioned on the locations of the malicious and secondary users and the Rayleigh fading term, each term in the summation of Eqn. (2) is a log-normally distributed random variable of the form $10^{\frac{\xi_{ij}}{10}} = e^{a\xi_{ij}}$, where $\xi_{ij} \sim \mathcal{N}(\mu_{ij}, \sigma_m^2)$, where μ_{ij} is given by

$$\mu_{ij} = P_m^{dB} + 10\log_{10}\Delta - 20\log_{10} d_{ij}^2, \tag{11}$$

where P_m^{dB} is the transmit power from the malicious users represented in decibels (i. e., $10\log_{10} P_m$) and d_{ij} is given by Eqn. (9) by replacing r_p and θ_p by r_j and θ_j, repespectively. We then approximate the sum of the log-normally distributed random variables (in the right hand side of Eqn. (2)) to be a log-normally distributed random variable of the form $10^{\frac{\omega_M}{10}} = e^{a\omega_M}$, where $\omega_i^M \sim \mathcal{N}(\hat{\mu}, \hat{\sigma}^2)$, by using Fenton's approximation. Conditioned on the locations of the malicious and the secondary users, $\hat{\sigma}^2$ and $\hat{\mu}$ can be obtained as[3]

$$\hat{\sigma}^2 = \frac{1}{a^2}\ln\left[1 + \frac{\left(e^{a^2\sigma_m^2} - 1\right)\sum_{j=1}^{M} e^{2a\mu_{ij}}}{\left(\sum_{j=1}^{M} e^{a\mu_{ij}}\right)^2}\right], \tag{12}$$

and

$$\hat{\mu} = \frac{1}{a}\ln\sum_{j=1}^{M} e^{a\mu_{ij}} - \frac{a}{2}\left(\hat{\sigma}^2 - \sigma_m^2\right). \tag{13}$$

It is essential to average over the positions of the malicious and secondary users to obtain the mean and variance of ω_M. This would involve integrating the expressions in Eqn. (12) and Eqn. (13) over r_j, θ_j for $j = 1, 2, 3, \ldots, M$ and r_i and θ_i, thus resulting in $2(M+1)$ integrations. Although this is smaller than the number of integrations required to obtain the exact value or p_{PUEA}, it still remains too complex to evaluate. In order to reduce the complexity of the computations, we make two modifications to the analysis:

1) Without loss of generality, we fix the position of the secondary user at $(0, 0)$[4].
2) We approximate the received power at a secondary user from each of the malicious users to be independent and identically distributed. This is valid due to the symmetry of the system and the fact that the malicious users can be present uniformly in an annular region between the circles centered at $(0, 0)$ and radii R_0 and R. Such approximations for analysis of other parameters in cognitive radio networks were made in [13],[14],[15].

Using the above modifications, $\hat{\sigma}^2$ and $\hat{\mu}$ can be obtained as

$$\hat{\sigma}^2 = \frac{1}{a^2}\ln\left[1 + \frac{\left(e^{a^2\sigma_m^2} - 1\right)}{M}\right], \tag{14}$$

and

$$\hat{\mu} = \mu_{ij} + \frac{1}{a}\ln M - \frac{a}{2}\left(\hat{\sigma}^2 - \sigma_m^2\right). \tag{15}$$

The expectation $E\left[P_r^{(m)}(i)\right]$ can then be obtained as

$$E\left[P_r^{(m)}(i)\right] = \frac{1}{\pi(R^2 - R_0^2)} e^{\frac{1}{2}a^2\hat{\sigma}^2} \int_{\theta_j=0}^{2\pi}\int_{r_j=R_0}^{R} e^{a\hat{\mu}} r_j dr_j d\theta_j. \tag{16}$$

Using the expression for distance between two points in polar co-ordinates given by Eqn. (9), the above can be simplified and obtained as

$$E\left[P_r^{(m)}(i)\right] = M\frac{1}{2R_0^2(R^2 - R_0^2)} e^{\frac{1}{2}a^2\hat{\sigma}^2}\Delta. \tag{17}$$

By fixing the co-ordinates of a secondary user at $(0, 0)$, $E\left[P_r^{(p)}(i)\right]$ is obtained by removing the integration in Eqn. (8) as

$$E\left[P_r^{(p)}(i)\right] = \frac{P_t e^{\frac{1}{2}a^2\sigma_p^2}\Delta}{r_p^2}. \tag{18}$$

The expression for $E\left[P_r^{(m)}(i)\right]$ from Eqn. (17) and $E\left[P_r^{(p)}(i)\right]$ from Eqn. (18) are substituted in Eqn. (7) to obtain the lower bound on a succesful PUEA on a secondary user.

IV. Results and Discussion

We consider the following values of the system parameters for our numerical computations. We consider $\sigma_p = 8$ and $\sigma_m = 5.5$, by assuming urban and suburban environments for the propagations from the primary transmitter and malicious users, respectively [16]. We consider the mean Rayleigh fading, Δ, to be unity. The transmit power from the malicious users, P_m, is taken to be 4 Watts as in [9].

Fig. 2 presents the lower bound on the probability of a succesful PUEA obtained by the analysis in Section III, in a system with 100 malicious users when the primary transmitter is at a distance of 2000m from the secondary user. The threshold values of 0.1, 0.05 and 0.025 shown in Fig. 2 correspond to a difference of 100mW, 50mW and 25mW, respectively, between the received powers from the primary transmitter and that from the malicious users. The thresholds

[3]The detailed derivation for the expressions in Eqns. (12)- (15) can be obtained by following the description provided in Appendix I.

[4]For any other fixed position of the secondary user, the analysis would still be valid by making a suitable co-ordinate transformation.

are chosen based on the following argument. For a primary transmitter 2000m away from the secondary user, the received power at the receivers vary typically between 0.1mW to 7.5W with mean 150mW (this is from the fact that a Gaussian random variable $X \sim \mathcal{N}(\mu, \sigma^2)$ typically takes values between $\mu - 3\sigma$ and $\mu + 3\sigma$). Hence, a difference of 100mW or lesser can be considered a succesful PUEA.

It is noted that the plots only present a lower bound and the actual probability may be higher than that shown. It is noted that for small values of R_0, the lower bound is 0. This is because, for smaller values of R_0 the malicious users are too close to the secondary user and when transmitting at maximum power of 4 Watts each, they result in a very large received power at the secondary user, thereby making the secondary user able to differentiate between a primary transmission and a malicious transmission. As expected, when the threshold reduces, the lower bound becomes looser (i.e., the lower bound decreases).

Fig. 3 shows the lower bound when the primary transmitter is at a distance of 8000m from the secondary user. In this case, it is observed that for sufficiently large R_0 (i. e., $R_0 > 90$m), even a threshold of 0.01 (i.e., 10mW) of the differences between the received powers due to primary and malicious transmissions results in a significant probability of a succesful PUEA.

The following inferences can be made from Figs. 2 and 3.

1) Since small values of R_0 result in a large received power at the secondary user due to transmission from malicious users, very large values of R_0 may also result in low PUEA since the received powers at the secondary users due to transmission from malicious users may be too small. One can then find a range of R_0 in which an attack can be succesful.
2) The significantly high values of a succesful PUEA under the absence of any power control at the malicious users indicate that with suitable power control, the probability of a succesful PUEA can further be enhanced. In particular, it is possible to obtain a set of transmit powers for each of the malicious users such that the probability of a succesful PUEA at a secondary user is 1.

V. Conclusion

We proposed an analytical approach and obtained a lower bound on the probability of a successful PUEA on a secondary user in a cognitive radio network by a set of co-operating malicious users. We show that the probability of a succesful PUEA increases with the distance between the primary transmitter and secondary users. This is the first analytical treatment to study the feasibility of a PUEA. We showed that our bounds enable in obtaining insights on possible ranges of exclusive regions in which an attack is most likely. Our results motivate the study of energy efficient PUEA attacks. Extension of our approach to determine the lower bounds for the probability of successful PUEA in systems deploying other spectrum sensing mechanisms described in [6] is a topic for further investigation.

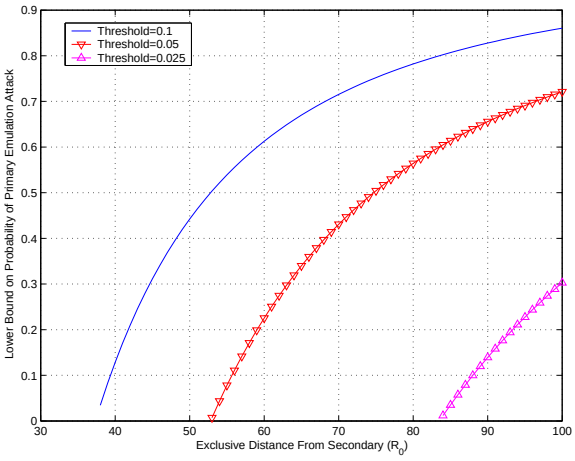

Fig. 2. Lower bound on the probability of a succesful PUEA when the primary transmitter is at a distance of 2 Km from the secondary user.

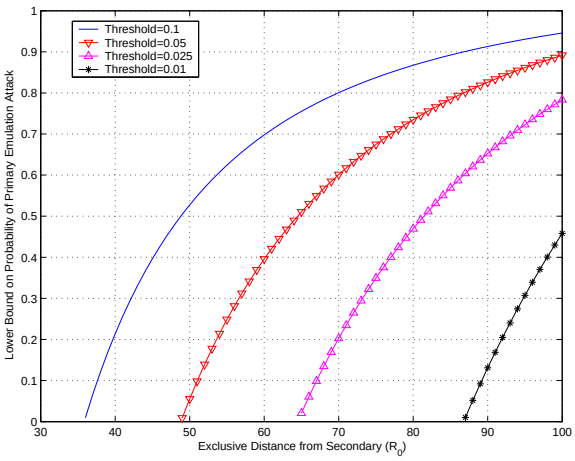

Fig. 3. Lower bound on the probability of a succesful PUEA when the primary transmitter is at a distance of 8 Km from the secondary user.

References

[1] S. Haykin, "Cognitive radio: Brain empowered wireless communications," *IEEE Jl. on Sel. Areas in Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[2] "IEEE Standards for information technology- Telecommunications and information exchange between systems- Wireless Regional Area Networks-Specific Requirements- Part 22-Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation in the TV bands," Jun. 2006.

[3] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "Ieee 802.22: The first worldwide wireless standard based on cognitive radios," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2005*, pp. 328–337, Nov. 2005.

[4] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmission in support of dynamic spectrum sharing," pp. 338–345, Nov. 2005.

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

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

[7] X. Liu and Z. Ding, "ESCAPE: a channel evacuation protocol for spectrum-agile networks," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN) 2007*, pp. 292–302, Apr. 2007.

[8] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing

in cognitive radio networks," *Proc., IEEE Workshop on Networking Technol. for Software Defined Radio Networks (SDR) 2006*, pp. 110–119, Sep. 2006.
[9] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Jl. on Sel. Areas in Commun.: Spl. Issue on Cognitive Radio Theory and Applications*, vol. 26, no. 1, pp. 25–37, Jan. 2008.
[10] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *Proc., IEEE Conference on Computer Communications (INFOCOM) 2008 mini-conference*, Apr. 2008.
[11] L. F. Fenton, "The sum of log-normal probability distributions in scatter transmission systems," *IRE Trans. on Commun. Systems*, no. CS-8, pp. 57–67, Mar. 1960.
[12] S. Ross, *Pobability Models*. Academic Pess, 2003.
[13] M. Vu, N. Devroye, and V. Tarokh, "Primary exclusive region in cognitive networks," *Proc., IEEE Consumer Communcations and Networking Conference (CCNC'2008)*, January 2008.
[14] M. Vu, N. Devroye, M. Sharif, and V. Tarokh, "Scaling laws of cognitive networks," *Submitted to IEEE Journal on Selected Topics in Signal Processing*.
[15] S. Anand and R. Chandramouli, "On the secrecy capacity of fading cognitive wireless networks," *Proc., IEEE Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM'2008)*, May 2008.
[16] T. S. Rappaport, *Wireless Communications: Principles and Practice*. Prentice Hall Inc., New Jersey, 1996.

APPENDIX I
FENTON'S APPROXIMATION TO MODEL THE SUM OF INDEPENDENT LOG-NORMAL RANDOM VARIABLES

Consider N independent log-normal random variables, Z_1, Z_2, $\cdots$, Z_N. Let $Z_i = 10^{\omega_i/10}$, where $\omega_i \sim \mathcal{N}(\mu_i, \sigma_i^2)$. Let

$$X_N = \sum_{i=1}^{N} Z_i. \tag{19}$$

Fenton's approximation [11] models X_N as a log-normally distributed random variable of the form $X_N = 10^{\Omega_N/10}$, where $\Omega_N \sim \mathcal{N}(\hat{\mu}_N, \hat{\sigma}_N^2)$. $\hat{\mu}_N$ and $\hat{\sigma}_N$ are determined as follows.

Equating the means on both the sides of Eqn. (19),

$$E\left[X_N\right] = \sum_{i=1}^{N} E\left[Z_i\right]. \tag{20}$$

Therefore,

$$E\left[10^{\frac{\Omega_N}{10}}\right] = \sum_{i=1}^{N} E\left[10^{\frac{\omega_i}{10}}\right], \tag{21}$$

i.e,

$$E\left[e^{a\Omega_N}\right] = \sum_{i=1}^{N} E\left[e^{a\omega_i}\right], \tag{22}$$

where $a = \ln 10/10$. Since ω_i and Ω_N are normal,

$$e^{a\hat{\mu}_N + \frac{1}{2}a^2\hat{\sigma}_N^2} = \sum_{i=1}^{N} e^{a\mu_i + \frac{1}{2}a^2\sigma_i^2}. \tag{23}$$

Equating the variances on both the sides of Eqn. (19), and using the fact that Z_i's are independent,

$$Var\left[X_N\right] = \sum_{i=1}^{N} Var\left[Z_i\right]. \tag{24}$$

Therefore,

$$E\left[X_N^2\right] - \left(E\left[X_N\right]\right)^2 = \sum_{i=1}^{N} E\left[Z_i^2\right] - \left(E\left[Z_i\right]\right)^2, \tag{25}$$

i.e.,

$$E\left[10^{\frac{2\Omega_N}{10}}\right] - \left(E\left[10^{\frac{\Omega_N}{10}}\right]\right)^2 = \sum_{i=1}^{N} E\left[10^{\frac{2\omega_i}{10}}\right] - \left(E\left[10^{\frac{\omega_i}{10}}\right]\right)^2, \tag{26}$$

i.e.,

$$E\left[e^{2a\Omega_N}\right] - \left(E\left[e^{a\Omega_N}\right]\right)^2 = \sum_{i=1}^{N} E\left[e^{2a\omega_i}\right] - \left(E\left[e^{a\omega_i}\right]\right)^2. \tag{27}$$

Since ω_i and Ω_N are normal,

$$e^{2a\hat{\mu}_N + a^2\hat{\sigma}_N^2}\left(e^{a^2\hat{\sigma}_N^2} - 1\right) = \sum_{i=1}^{N} e^{2a\mu_i + a^2\sigma^2}\left(e^{a^2\sigma_i^2} - 1\right). \tag{28}$$

From (23) and (28),

$$\hat{\sigma}_N^2 = \frac{1}{a^2}\ln\left[1 + \frac{\sum_{i=1}^{N} e^{2a\mu_i + a^2\sigma_i^2}\left(e^{a^2\sigma_i^2} - 1\right)}{\left(\sum_{i=1}^{N} e^{a\mu_i + \frac{1}{2}a^2\sigma_i^2}\right)^2}\right] \tag{29}$$

and

$$\hat{\mu}_N = \frac{1}{a}\ln\left[\sum_{i=1}^{N} e^{a\mu_i + \frac{1}{2}a^2\sigma_i^2}\right] - \frac{a}{2}\hat{\sigma}_N^2. \tag{30}$$

If $\sigma_i^2 = \sigma^2 \ \forall \ i$, then

$$\hat{\sigma}_N^2 = \frac{1}{a^2}\ln\left[1 + \left(e^{a^2\sigma^2} - 1\right)\frac{\sum_{i=1}^{N} e^{2a\mu_i}}{\left(\sum_{i=1}^{N} e^{a\mu_i}\right)^2}\right] \tag{31}$$

and

$$\hat{\mu}_N = \frac{1}{a}\ln\left[\sum_{i=1}^{N} e^{a\mu_i}\right] - \frac{a\left(\hat{\sigma}_N^2 - \sigma^2\right)}{2}. \tag{32}$$

If Z_is are independent and identically distributed (i.i.d), i.e., $\mu_i = \mu \ \forall \ i$ and $\sigma_i^2 = \sigma^2 \ \forall \ i$, then σ_N^2 and $\hat{\mu}_N$ are given by

$$\sigma_N^2 = \frac{1}{a^2}\ln\left[1 + \frac{e^{a^2\sigma^2} - 1}{N}\right] \tag{33}$$

and

$$\hat{\mu}_N = \mu - \frac{a}{2}\left(\sigma_N^2 - \sigma^2\right) + \frac{1}{a}\ln N. \tag{34}$$