Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing *

Z. Jin *zjin@stevens.edu*
S. Anand *asanthan@stevens.edu*
K. P. Subbalakshmi *ksubbala@stevens.edu*
Department of Electrical and Computer Engineering
Stevens Institute of Technology, Hoboken, New Jersey, USA

We present a Neyman-Pearson composite hypothesis test (NPCHT) and a Wald's sequential probability ratio test (WSPRT) to detect primary user emulation attacks (PUEA) in cognitive radio networks. Most approaches in the literature on PUEA assume the presence of underlying sensor networks for localization of the malicious nodes. There are no analytical studies available in the literature to study PUEA in the presence of multiple malicious users in fading wireless environments. We present an NPCHT and WSPRT based analysis to detect PUEA in fading wireless channels in the presence of multiple randomly located malicious users. We show that there is a range of network radii in which PUEA are most successful. Results also show that for the same desired threshold on the probability of missing the primary, WSPRT can achieve a probability of successful PUEA 50% less than that obtained by NPCHT.

I. Introduction

Traditionally, radio spectrum bands have been assigned to license holders or services on a long term basis for large geographical regions. This fixed spectrum assignment policy has led to under-utilization of the available spectrum. The inefficiency in spectrum usage and the limited availability of spectrum have given rise to cognitive radio enabled dynamic spectrum access (DSA) as a new communication paradigm [1], [2], [3]. "Secondary" nodes in a DSA networks can use the licensed spectrum bands when it is idle, under the condition that they vacate it upon the return of the "primary" licensed users (incumbent, primary users). In the rest of the paper, we use the term primary or incumbent to refer to the licensed, high priority user and the term secondary to denote the unlicensed users. One example of cognitive radio networks (CRN) is the usage of unused spectrum in the TV band. The TV transmitter and receivers are primary users who are licensed to use these bands. Other users who access the white spaces in the TV band on an ad-hoc basis are termed secondary users. The IEEE 802.22 working group on wireless regional area networks [4] provides the physical layer and medium access control specifications for usage of the TV white spaces.

The FCC's mandated spectrum policy reform [5] has resulted in a great deal of research activities on various aspects of CRN including spectrum sensing and management, network architectures, capacity, codes, transmission techniques, spectrum etiquette and evacuation protocols as well as test-bed development. Standardization efforts for DSA networks include the IEEE Standards Coordinating Committee 41 (IEEE SCC41)'s sponsored projects as well as IEEE 802.22 [6].

Spectrum sensing in DSA is essential both for identification of empty spectral bands (white spaces) as well as for prompt evacuation upon the return of incumbent. Protocols for sensing primary transmission and spectrum evacuation can be found in [7], [8]. Primary transmitter detection techniques include energy detection, cyclostationary feature detection and matched filter detection [3]. Among these, energy based detection is generally more popular due to ease of implementation.

Despite the body of work on other aspects of CRN, research on security issues is still in its nascence [9]-[17]. In the particular case of DSA networks, it can be argued that in order to stage a denial-of-service (DoS) attack at the sensing level, it is necessary to affect the decision on primary activity during the sensing phase. This can be done in one of the following ways: (a) some malicious nodes can transmit spurious signals that emulate the primary user – primary user emulation attacks (PUEA) [11], [12], [16], [17]; (b) the spectrum sensing nodes can lie about the spectrum data (Byzantine attack) [13]; (c) by making use of the weaknesses of existing protocols for evacuation [9] or (d) by modifying messages passed between the sens-

*This work was supported in part by NSF Cyber Trust Grant No. 0627688.

ing nodes and the centralized decision maker [10].

In this paper we study DoS attacks via primary user emulation. In this type of attacks, a set of "malicious" secondary users could forge the essential characteristics of the primary signal transmission to make other "good" secondary users believe that the primary user is present when it is not. The secondary users following normal spectrum evacuation process (the good users) will vacate the spectrum unnecessarily, resulting in what are known as the primary user emulation attacks (PUEA). PUEA become easier when energy detection based mechanisms are used for identification of primary activity, since the detector only checks received energy against a threshold rather than look for particular signal characteristics.

Chen *et al* [11] propose two mechanisms to detect PUEA: distance ratio test and distance difference test based on the correlation between the length of wireless link and the received signal strength. They consider a *single* malicious user in a *non-fading* wireless environment and detect PUEA using the ratio and the difference, respectively, of the distances from primary transmitter and the malicious user, to the secondary users equipped with global positioning system (GPS). In [12], Chen *et al* discuss defense against PUEA by localization of the suspect transmission via an underlying sensor network and comparing it with the known location of the primary transmitter. A mitigation technique for DoS attacks arising from fraudulent reporting of sensing results by malicious nodes is studied in [13]. *The PUEA methods described thus far do not take into account, the fading characteristics of the wireless environment and require estimation of the location of the malicious users via either a dedicated sensor network or via significant enhancement of the secondary nodes themselves.*

The first analytical expression for the probability of successful PUEA based on energy detection was derived in [16], where we modeled the received power at a secondary user as a log-normally distributed random variable and used Fenton's approximation to determine the mean and the variance of this distribution. This was then used to determine, a lower bound on the probability of successful PUEA using Markov inequality. In this paper, we propose a Neyman-Pearson composite hypothesis test (NPCHT) and a Wald's sequential probability ratio test (WSPRT) to detect PUEA in fading wireless environments, *without assuming additional features to the secondary nodes or the presence of dedicated sensor nodes to assist in gathering information about the direction of received signal*. Fenton's approximation is used to model the received power at the secondary user from the transmission of the malicious users. Simulations confirm the theoretical result that NPCHT allows the secondary user to keep the probability of missing the primary around a desired threshold while trying to minimize the probability of successful PUEA. Since the NPCHT cannot *simultaneously* provide a cap on the probability of missing the primary as well as the probability of a successful PUEA, we develop the WSPRT, which will allow us this flexibility in return for some added time complexity, in terms of number of observations needed to arrive at a decision. We show that with modest increase in computation, it is possible to mitigate PUEA significantly even when using only the energy based detection.

The rest of the paper is organized as follows. Section II presents the system model and the assumptions made to formulate the problem. The NPCHT as well as the WSPRT are formulated and solved in Section III. In Section IV, we provide the simulation results and discussion. Section V presents the conclusion.

II. System Model

In our model all secondary and malicious users are distributed in a circular grid of radius R as shown in Fig. 1. A primary user is located at a distance of at least d_p from all other users. We consider energy based mechanisms to detect the presence of the primary. Typical energy based detection methods assume that the primary is present if the received signal strength is -93dBm [4]. Such a sensing technique will cause serious security issues if malicious users exist in the network. As described earlier, this detection method is susceptible to PUEA. In order to mitigate this threat, we devise two hypothesis based testing mechanisms to decide if the primary is transmitting or if an attack is in progress. The assumptions and mathematical terminologies needed to derive the hypothesis tests are listed below.

1. There is no communication or co-operation between the secondary users. The PUEA on each secondary user can be analyzed independent of each other.

2. There are M malicious users in the system. M is a geometrically distributed random variable with the mean $E[M]$ known to the secondary users.

3. The primary transmitter is at a minimum distance of d_p from all the users.

4. The positions of the secondary and the malicious users are uniformly distributed in the circular

gird of radius R, and their positions are statistically independent of each other.

5. For the secondary user fixed at polar co-ordinates (r_0, θ_0), no malicious users are present within a circle of radius R_0 centered at (r_0, θ_0). We call R_0 the "exclusive distance from the secondary user". Without this restriction, 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 failed PUEA all the time [16]. We use the polar co-ordinate system for the rest of the paper.

6. The co-ordinates of the primary transmitter are known to all the users in the system.

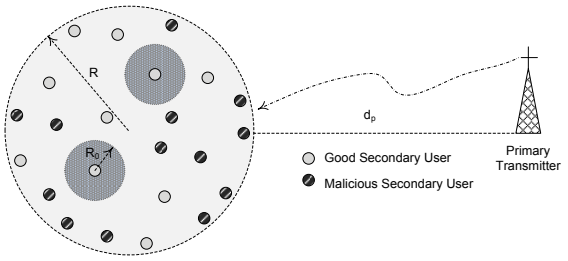


Figure 1: A typical cognitive radio network in a circular grid of radius R consisting of good secondary users and malicious secondary users. No malicious users are present within a radius R_0 about each good secondary user. A primary transmitter is located at a distance of at least d_p from all other users.

7. The primary transmits at a power P_t and the malicious at a power P_m. Malicious nodes do not use power control.

8. The RF signals from the primary transmitter and the malicious users undergo path loss and log-normal shadowing. The Rayleigh fading is assumed to be averaged out and can hence be ignored. This is because, the probabilities scale linearly with the mean of the Rayleigh fading, Δ, (as shown in [16]) and $\Delta = 1$ in most cases [18].

9. The shadowing loss (expressed in dB) at any secondary user both from the primary transmitter and from any malicious user is normally distributed with mean 0 and variance σ_p^2 and σ_m^2, respectively.

10. 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 [16].

III. Analytical Model

Since there is no co-operation between the secondary users, the probability of PUEA on any user is the same as that on any other user. Hence, without loss of generality, we analyze the probability density function (pdf) of the received signal at one secondary user. We transform the co-ordinates of all malicious users such that the secondary user of interest lies at the origin (i.e., at $(0, 0)$). The transformed co-ordinates of the primary will then be (d_p, θ_p). Note that the transformed co-ordinates of the primary will depend on the actual location of the secondary user of interest and will not be (d_p, θ_p) for all the secondary users. However, typically, $d_p >> R$ and hence it is justified to approximate the co-ordinates of the primary user to be (d_p, θ_p) irrespective of which secondary user we consider for the analysis. The scenario with the transformed co-ordinates is shown in Fig. 2. By assumptions 4. and 5. in Section II, all malicious nodes are uniformly distributed in the annular region with radii R_0 and R.

In order to obtain a hypothesis test using NPCHT and WSPRT, it is essential to obtain the pdf of the received signal at the secondary user due to transmission by the primary and the malicious users. We first describe the analysis to obtain the pdf in Section III.A.

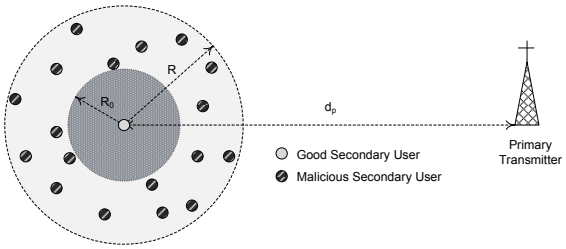


Figure 2: Scenario with transformed co-ordinates. The secondary user of interest is at (0,0). Malicious users are uniformly distributed in the annular region (R_0, R). The primary is at (d_p, θ_p).

III.A. Probability Density Function of the Received Signal

Consider M malicious users located at co-ordinates (r_j, θ_j) $1 \leq j \leq M$, where M is a geometrically distributed random variable. The probability mass function (pmf) of M, $Pr\{M = k\}$ is therefore given by

$$Pr\{M = k\} = (1-p)^{k-1}p \quad k = 1, 2, ..., \qquad (1)$$

where $p = \frac{1}{E[M]}$. From assumptions 4. and 5. in Section II, the position of the j^{th} malicious user is uniformly distributed in the annular region between R_0 and R. Also, r_j and θ_j are statistically independent $\forall\ j$. The pdf of r_j, $p(r_j)$ is therefore given by

$$p(r_j) = \begin{cases} \frac{2r_j}{R^2 - R_0^2} & r_j \in [R_0, R] \\ 0 & \text{otherwise,} \end{cases} \qquad (2)$$

while θ_j is uniformly distributed in $(-\pi, \pi)$ $\forall\ j$.

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

$$P_r^{(p)} = P_t d_p^{-2} G_p^2, \qquad (3)$$

where $G_p^2 = 10^{\frac{\xi_p}{10}}$ and $\xi_p \sim \mathcal{N}(0, \sigma_p^2)$ as mentioned in Section II. Since P_t and d_p are fixed, the pdf of $P_r^{(p)}$, $p^{(Pr)}(\gamma)$, follows a log-normal distribution and can be written as

$$p^{(Pr)}(\gamma) = \frac{1}{A\sigma_p\sqrt{2\pi}\gamma} \exp\left\{-\frac{(10\log_{10}\gamma - \mu_p)^2}{2\sigma_p^2}\right\}, \qquad (4)$$

where $A = \frac{\ln 10}{10}$ and

$$\mu_p = 10\log_{10} P_t - 20\log_{10} d_p. \qquad (5)$$

The total received power at the secondary node from all M malicious users is given by

$$P_r^{(m)} = \sum_{j=1}^{M} P_m d_j^{-4} G_j^2, \qquad (6)$$

where d_j is the distance between the j^{th} malicious user and the secondary user and G_j^2 is the shadowing between the j^{th} malicious user and the secondary user. As mentioned in Section II, $G_j^2 = 10^{\frac{\xi_j}{10}}$, where $\xi_j \sim \mathcal{N}(0, \sigma_m^2)$. Conditioned on the positions of all the malicious users, each term in the summation in the right hand side of Eqn. (6) is a log-normally distributed random variable of the form $10^{\frac{\omega_j}{10}}$, where $\omega_j \sim \mathcal{N}(\mu_j, \sigma_m^2)$, where

$$\mu_j = 10\log_{10} P_m - 40\log_{10} d_j. \qquad (7)$$

As we had explained in [16], conditioned on the positions of all the malicious users, $P_r^{(m)}$ can be approximated as a log-normally distributed random variable whose mean and variance can be obtained by using Fenton's method [19].

The pdf of $P_r^{(m)}$ conditioned on the positions of all M malicious users, $p^{(m)}_{\chi|\mathbf{r}}(\chi|\mathbf{r})$, can be written as

$$p^{(m)}_{\chi|\mathbf{r}}(\chi|\mathbf{r}) = \frac{1}{A\hat{\sigma}_M\sqrt{2\pi}\chi} \exp\left\{-\frac{(10\log_{10}\chi - \hat{\mu}_M)^2}{2\hat{\sigma}_M^2}\right\}, \qquad (8)$$

where $\mathbf{r}$ is the vector with elements $r_1 \cdots r_M$ and $\hat{\sigma}_M^2$ and $\hat{\mu}_M$ are given by[1]

$$\hat{\sigma}_M^2 = \frac{1}{A^2}\ln\left[1 + \frac{(e^{A^2\sigma_m^2} - 1)\sum_{j=1}^{M} e^{2A\mu_j}}{\left(\sum_{j=1}^{M} e^{A\mu_j}\right)^2}\right] \qquad (9)$$

and

$$\hat{\mu}_M = \frac{1}{A}\ln\left(\sum_{j=1}^{M} e^{A\mu_j}\right) - \frac{A}{2}(\hat{\sigma}_M^2 - \sigma_m^2), \qquad (10)$$

respectively. The pdf of the received power from all M malicious users, $p^{(m)}(\chi)$, can then be obtained by averaging Eqn. (8) over r_1, r_2, $\cdots$ r_M and can be written as[2]

$$p^{(m)}(\chi) = \sum_{k=1}^{\infty}\left[\int_{[R_0,R]^M} p^{(m)}_{\chi|\mathbf{r}}(\chi|\mathbf{r})p(\mathbf{r}|M)d\mathbf{r}\right] P\{M = k\}, \qquad (11)$$

where $p(\mathbf{r}|M) = \prod_{j=1}^{M} p(r_j)$, and $p(r_j)$ can be obtained from Eqn. (2).

Evaluating Eqn. (11) is very complex. However, Eqn. (11) is an integral which can be looked upon as a weighted sum of conditional pdf's, each of which is log-normal. Therefore, applying Fenton's approximation for the weighted sum, the expression for the pdf $p^{(m)}(\chi)$ in Eqn. (11) can be approximated as a log-normal distribution with parameters μ_χ and σ_χ^2 of the form

$$p^{(m)}(\chi) = \frac{1}{A\sigma_\chi\sqrt{2\pi}\chi} \exp\left\{-\frac{(10\log_{10}\chi - \mu_\chi)^2}{2\sigma_\chi^2}\right\}. \qquad (12)$$

If $P_r^{(m)}$ is a log-normally distributed random variable with pdf given in Eqn. (12), σ_χ^2 and μ_χ can be

[1]The expressions in Eqns. (9) and (10) can be obtained by following the steps specified in the Appendix in [16].

[2]The expressions in Eqns. (8) and (11) should also be conditioned and averaged over the co-ordinates (and hence have integrations over) θ_1, θ_2, $\cdots$, θ_M. However, from Eqns. (7), (9) and (10), it is observed that the expressions are independent of θ_1, θ_2, $\cdots$, θ_M. Therefore, it is sufficient if the averaging (and integrations) are performed over r_1, r_2, $\cdots$, r_M.

obtained as in [20]

$$\sigma_\chi^2 = \frac{1}{A^2} \ln \left[\frac{Var\left(P_r^{(m)}\right) + E^2\left[P_r^{(m)}\right]}{E^2\left[P_r^{(m)}\right]} \right] \quad (13)$$

and

$$\mu_\chi = \frac{1}{A} \ln \left[\frac{E^2\left[P_r^{(m)}\right]}{\left(Var\left(P_r^{(m)}\right) + E^2\left[P_r^{(m)}\right]\right)^{\frac{1}{2}}} \right]. \quad (14)$$

From Eqn. (8), the expectation of $P_r^{(m)}$ conditioned on M, $E\left[P_r^{(m)}|M\right]$, and the variance of $P_r^{(m)}$, $Var\left(P_r^{(m)}|M\right)$, can be obtained by averaging $E\left[P_r^{(m)}|\mathbf{r}\right]$ and $Var\left(P_r^{(m)}|\mathbf{r}\right)$ over r_1, r_2, $\cdots$, r_M and can be obtained in closed-form as

$$E\left[P_r^{(m)}|M\right] = \frac{MP_m}{R_0^2 R^2} e^{\frac{1}{2}A^2\sigma_m^2}, \quad (15)$$

and

$$Var\left(P_r^{(m)}|M\right) = \frac{MP_m^2 e^{A^2\sigma_m^2}}{3R_0^6 R^6}\left[\left(\frac{R^6 - R_0^6}{R^2 - R_0^2}\right) e^{A^2\sigma_m^2} - 3R_0^2 R^2\right]. \quad (16)$$

Therefore, $E\left[P_r^{(m)}\right]$ and $Var\left(P_r^{(m)}\right)$ can be calculated as

$$E\left[P_r^{(m)}\right] = E\left[E\left[P_r^{(m)}|M\right]\right], \quad (17)$$

and

$$Var\left(P_r^{(m)}\right) = E\left[Var\left(P_r^{(m)}|M\right)\right] + Var\left(E\left[P_r^{(m)}|M\right]\right). \quad (18)$$

Substituting the above expressions in Eqns. (13) and (14), we evaluate σ_χ^2 and μ_χ, which, in turn, can be substituted in Eqn. (12) to evaluate the pdf $p^{(m)}(\chi)$.

III.B. Neyman-Pearson Composite Hypothesis Test to detect PUEA

The Neyman-Pearson composite hypothesis test can be used to distinguish between two hypotheses, given some constraints on the miss probability. In our case, the two hypotheses are:

$$\begin{array}{ll} H_1: & \text{Primary transmission in progress} \\ H_2: & \text{Emulation attack in progress.} \end{array} \quad (19)$$

The observation space is the sample space of received power measured at the secondary user. It is observed that there are two kinds of risks incurred by a secondary user in this hypothesis test.

- *False Alarm:* When the actual transmission is made by malicious users but the secondary decides that the transmission is due to the primary. In our case, this is also the probability of a successful PUEA.
- *Miss:* When the actual transmission is made by the primary transmitter but the secondary decides that the transmission is due to the malicious users. This is a serious concern if the good secondary does not wish to violate the spectrum etiquette.

The Neyman-Pearson criterion allows the secondary to minimize the probability of successful PUEA while fixing the probability of missing the primary user at a desired threshold, α. The decision variable, Λ, is given by

$$\Lambda = \frac{p^{(m)}(x)}{p^{(Pr)}(x)}, \quad (20)$$

where x is the measured power of the received signal. In the above, $p^{(Pr)}(x)$ and $p^{(m)}(x)$ are given by Eqns. (4) and (12), respectively. The decision is then made based on the following criterion:

$$\begin{array}{ll} \Lambda \leq \lambda & D_1\text{: Primary transmission} \\ \Lambda \geq \lambda & D_2\text{: PUEA in progress,} \end{array} \quad (21)$$

where λ satisfies the constraint that miss probability, $Pr\{D_2|H_1\}$, is fixed at α, i.e.,

$$Pr\{D_2|H_1\} = \int_{\Lambda \geq \lambda} p^{(Pr)}(x)dx = \alpha. \quad (22)$$

The probability of successful PUEA can be written as

$$Pr\{D_1|H_2\} = \int_{\Lambda \leq \lambda} p^{(m)}(x)dx. \quad (23)$$

We can also represent the above detection statistic in shorthand notation as

$$\Lambda \underset{D_1}{\overset{D_2}{\gtrless}} \lambda. \quad (24)$$

Let the received power in dB be denoted by y and let

$$\begin{aligned} a &= \frac{1}{2\sigma_p^2} - \frac{1}{2\sigma_\chi^2} \\ b &= \frac{\mu_\chi}{\sigma_\chi^2} - \frac{\mu_p}{\sigma_p^2} \\ c &= \frac{\mu_p^2}{2\sigma_p^2} - \frac{\mu_\chi^2}{2\sigma_\chi^2} + \ln\sigma_p - \ln\sigma_\chi - \ln\lambda, \end{aligned} \quad (25)$$

by substituting $p^{(Pr)}(x)$ and $p^{(m)}(x)$, we obtain the decision statistic as:

$$ay^2 + by + c \underset{D_1}{\overset{D_2}{\gtrless}} 0. \tag{26}$$

Without loss of generality, we assume $a \neq 0$. Let $\Delta = b^2 - 4ac$, two conditions are of interest:

- Case 1: $a > 0$, $\Delta > 0$
  The constraint of $Pr\{D_2|H_1\} = \alpha$ can be written as

$$\Phi\left(\frac{-b-\sqrt{\Delta}-2a\mu_p}{2a\sigma_p}\right) + \Phi\left(\frac{b-\sqrt{\Delta}+2a\mu_p}{2a\sigma_p}\right) = \alpha, \tag{27}$$

  where $\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{t^2}{2}}\,dt$, and $Pr\{D_1|H_2\}$ can be derived as

$$Pr\{D_1|H_2\} = \Phi\left(\frac{-b+\sqrt{\Delta}-2a\mu_\chi}{2a\sigma_\chi}\right) - \Phi\left(\frac{-b-\sqrt{\Delta}-2a\mu_\chi}{2a\sigma_\chi}\right). \tag{28}$$

- Case 2: $a < 0$, $\Delta > 0$
  The constraint of $Pr\{D_2|H_1\} = \alpha$ can be written as

$$\Phi\left(\frac{-b-\sqrt{\Delta}-2a\mu_p}{2a\sigma_p}\right) - \Phi\left(\frac{-b+\sqrt{\Delta}-2a\mu_p}{2a\sigma_p}\right) = \alpha, \tag{29}$$

  and $Pr\{D_1|H_2\}$ can be derived as

$$Pr\{D_1|H_2\} = \Phi\left(\frac{-b+\sqrt{\Delta}-2a\mu_\chi}{2a\sigma_\chi}\right) + \Phi\left(\frac{b+\sqrt{\Delta}+2a\mu_\chi}{2a\sigma_\chi}\right). \tag{30}$$

As is expected, the Neyman-Pearson test only allows us to place a cap on one of the quantities: the miss probability or the false alarm probability. In our experimental results we found that under certain circumstances, the probability of false alarm (successful PUEA) is very high for the desired probability of miss. So, we now develop a Wald's sequential probability ratio test which allows the user to set thresholds for both false alarm and miss probabilities. This is possible, since Wald's test is set up to take *more than one sample observation* if necessary to arrive at a decision.

III.C. Wald's Sequential Probability Ratio Test to detect PUEA

The WSPRT allows us to specify desired thresholds (α_1 and α_2 respectively) for both the false alarm and miss probabilities. The decision variable after n sequential tests, Λ_n, is given by

$$\Lambda_n = \prod_{i=1}^{n} \frac{p^{(m)}(x_i)}{p^{(Pr)}(x_i)}, \tag{31}$$

where x_i is the measured power at the i^{th} stage. In the above equation, $p^{(Pr)}(x_i)$ and $p^{(m)}(x_i)$ are given by Eqns. (4) and (12), respectively. The decision is then made based on the following criterion:

$$\begin{array}{ll} \Lambda_n \leq T_1 = \frac{\alpha_1}{1-\alpha_2} & D_1\text{: Primary transmission} \\ \Lambda_n \geq T_2 = \frac{1-\alpha_1}{\alpha_2} & D_2\text{: PUEA in progress} \\ \text{Otherwise} & D_3\text{: Take another observation .} \end{array} \tag{32}$$

The average number of observations required to arrive at a decision is given by [21]

$$E[n|H_k] = \begin{cases} \frac{(1-\alpha_2)\ln T_1 + \alpha_2 \ln T_2}{E[f(x_1)|H_1]} & k = 1 \\ \frac{\alpha_1 \ln T_1 + (1-\alpha_1)\ln T_2}{E[f(x_1)|H_2]} & k = 2, \end{cases} \tag{33}$$

where the function $f(x_1) = \ln \Lambda_1$. From Eqns. (4), (12) and (31), we can derive the expression for $E[f(x_1)|H_1]$ and $E[f(x_1)|H_2]$ as follows:

$$E[f(x_1)|H_1] = \ln\left(\frac{\sigma_p}{\sigma_\chi}\right) + \frac{\sigma_\chi^2\mu_p^2 - \sigma_p^2\mu_\chi^2}{2\sigma_p^2\sigma_\chi^2} + \frac{2\mu_p(\sigma_p^2\mu_\chi - \sigma_\chi^2\mu_p)}{2\sigma_p^2\sigma_\chi^2} + \frac{(\sigma_\chi^2 - \sigma_p^2)(\sigma_p^2 + \mu_p^2)}{2\sigma_p^2\sigma_\chi^2}, \tag{34}$$

and

$$E[f(x_1)|H_2] = \ln\left(\frac{\sigma_p}{\sigma_\chi}\right) + \frac{\sigma_\chi^2\mu_p^2 - \sigma_p^2\mu_\chi^2}{2\sigma_p^2\sigma_\chi^2} + \frac{2\mu_\chi(\sigma_p^2\mu_\chi - \sigma_\chi^2\mu_p)}{2\sigma_p^2\sigma_\chi^2} + \frac{\sigma_\chi^2 - \sigma_p^2}{2\sigma_p^2\sigma_\chi^2}(\sigma_\chi^2 + \mu_\chi^2). \tag{35}$$

Substituting $E[f(x_1)|H_1]$ and $E[f(x_1)|H_2]$ in Eqn. (33), we evaluate $E[n|H_1]$ and $E[n|H_2]$.

Based on Section IV.B, we can see that though experimental results of WSPRT do not perfectly match their theoretically designed criterion, they can significantly lower the probability of successful PUEA than NPCHT do. The price WSPRT pays to achieve a finer decision is to take more observations.

IV. Simulations

We consider the following values of the system parameters for our numerical simulations. The variances for the primary and malicious transmissions are assumed to be $\sigma_p = 8$ and $\sigma_m = 5.5$, since we can model the primary and malicious transmissions as those occurring in urban and suburban environments [18]. A primary transmitter (a TV tower), located at a distance of $d_p = 100km$ to the secondary user, has a transmit power of $P_t = 100kW$. The transmit power of the malicious users, P_m, is taken to be 4 Watts as in [12]. The exclusive distance from the secondary user, R_0, is fixed at $30m$, the same as in [16]. The network radius, R, is increased from $30m$ to $270m$, thus changing the average distance from the malicious

user to the secondary user accordingly. The number of malicious users is assumed to be a geometrically distributed random variable with $E[M]$ equal to 25. As the calculation shows, the above numerical parameters always guarantee the case where $a < 0$ and $\delta > 0$ in the NPCHT.

In our simulations, we assume that the primary user is modeled as a Bernoulli ($\frac{1}{2}$), which means that there is equal probability of the primary to be ON or OFF. The primary user transmissions are simulated as per the distribution discussed earlier which includes path loss and shadowing. To simulate the PUEA, we first generate a geometrically distributed random number, M, representing the number of malicious users. We then generate M independent and identically distributed (i.i.d.) sets of co-ordinates for M malicious users, such that the malicious users are uniformly distributed in the annulus with radii R_0 and R. The received power from the transmission of all M malicious users is calculated based on Eqn. (6), including path loss and i.i.d. shadowing.

For each value of R, we run 100,000 simulations. We calculate false alarm probabilities and miss probabilities by counting the number of times that the decision statistic meets the corresponding decision criterion. For WSPRT, we also record average number of observations required to make a decision in each simulation.

IV.A. Neyman-Pearson Composite Hypothesis Test Results

The results of NPCHT with theoretical probability of missing the primary user set to α=0.2 are shown in Fig. 4. It is observed from Fig. 3(a) that the probability of false alarm rises and then falls down with increasing value of R. This is because, for a given R_0, if R is small, i.e., malicious users are closer to the secondary user, the total received power from all malicious users is likely to be larger than that received from the primary transmitter, thus decreasing the probability of successful PUEA. Similarly, for large R, the total received power from the malicious users may not be enough to successfully launch a PUEA. Fig. 3(b) shows that the experimental probability of missing the primary user is always close to the required value (within ± 0.04 of the desired value).

As we lower α from 0.2 to 0.1, the maximum error between the experimental curve and the theoretical one falls from 0.133, shown in Fig. 3(a), to 0.083, shown in Fig. 4(a). These discrepancies exist, because we needed to make approximations while deriving the expressions for the received power. However, since the experimental and theoretical values are not far apart, our approximations are fairly good. From Fig. 3(a) and Fig. 4(a) we note that as α is decreased, the probability of successful PUEA increases. This is expected, since NPCHT only allows a threshold to be set on one of these parameters.

IV.B. Wald's Sequential Probability Ratio Test Results

Fig. 5 shows the results of WSPRT with thresholds for the probability of successful PUEA, probability of missing primary user set to 0.2 each. Although the experimental curve in Fig. 5(a) goes above the theoretical one, we achieve much lower probabilities of successful PUEA compared to Fig. 3(a). In fact, the maximum probability of successful PUEA in the NP test can go as high as 0.778 whereas in the Wald's test we can limit this to 0.407. The lower probabilities of successful PUEA are achieved at the cost of more observations as shown in Fig. 5(c) and Fig. 5(d). It is observed that number of observation behaves similar to the probability curves. This is because, more observations are always taken if a decision can not be made easily, where decision error probabilities also tend to be relatively high. Note that the gap between the experimental and theoretical curves is typical of WSPRT because, the expression for the expected number of observations in Eqn. (33) is an approximation rather than an exact expression [21].

Fig. 6(a) shows the results obtained when the threshold for PUEA is set to 0.1. Comparing this with Fig. 5(a) we see that for any α_2, it is not possible to achieve arbitrary lower probabilities of successful PUEA. *Note, however, that it is always possible to make sure that the probability of missing primary user stays strictly below the required threshold, which can be seen from Fig. 5(b), Fig. 6(b) and Fig. 7(b).* This is particularly important in CRN to ensure that the secondaries still obey the spectrum sharing etiquette.

As both α_1 and α_2 are lowered to 0.1 (Fig. 7), only the experimental curve of miss probability in Fig. 7(b) decreases accordingly. This indicates that it is not possible to always keep both the false alarm probability as well as the miss probability below arbitrarily desired thresholds.

From the curves showing the number of observations required to make a decision (Fig. 5(c), Fig. 6(c) and Fig. 7(c)), it can be noticed that more observations are required as the α_1 and α_2 are decreased. This is because, from Eqn. (32), as α_1 and α_2 decreases, the threshold T_1 decreases and the threshold T_2 increases which effectively reduces the range of values of the

test statistic for which a decision is taken. Thus, it is more likely that the secondary user takes decision D_3 (i.e., observes more samples). Therefore, there is a tradeoff between reliable decision and time to detect.

V. Conclusion

We proposed a Neyman-Pearson composite hypothesis test (NPCHT) and a Wald's sequential probability ratio test (WSPRT) to detect primary user emulation attacks (PUEA) in cognitive radio networks. Both WSPRT and NPCHT resulted in a range of radii in which PUEA were most successful. For a desired threshold on the probability of missing the primary, WSPRT was found to achieve 50% reduction in the probability of successful PUEA compared to NPCHT. We are currently investigating the extension of our analysis for other distributions of the number of malicious users, M, and determination of the best fit for the distribution of M. The extension of our analysis to include power control at the malicious users is a topic for further investigation.

References

[1] J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

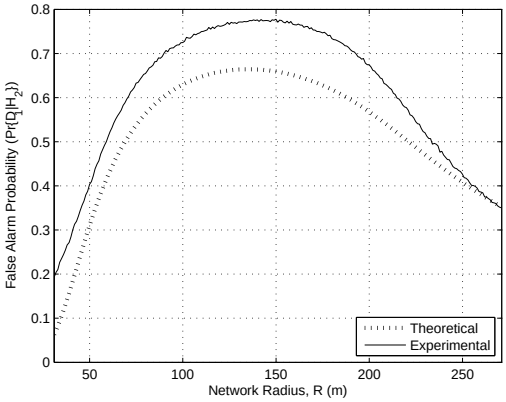
[2] S. Haykin, "Cognitive radio: Brain empowered wireless communications," *IEEE Jl. on Sel. Areas in Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[3] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Elsevier Jl. on Computer Networks*, vol. 50, no. 13, pp. 2127–2159, Sep. 2006.

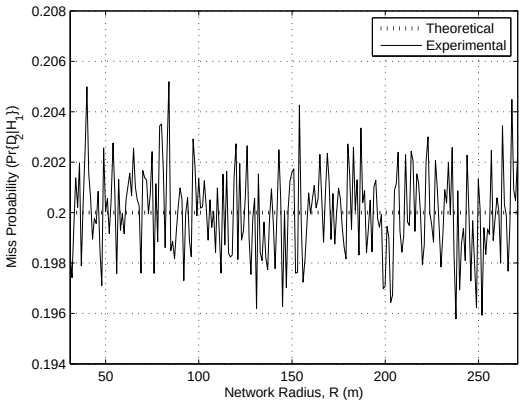
[4] "IEEE Standards for information technology-Telecommunications and information exchange between systems- Wireless Regional Area Networks-Specific Requirements- Part 22-Cognitive wireless RAN medium access control (MAC) and physical layer (PHY) specifications: Policies and procedures for operation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

[5] [Online]. Available: http://www.fcc.gov

[6] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar, "IEEE 802.22: The first world-

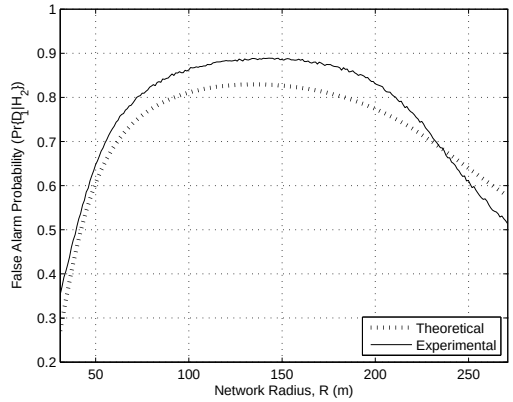


(a) Probability of successful PUEA using the NPCHT. The average number of malicious users is fixed at 25.

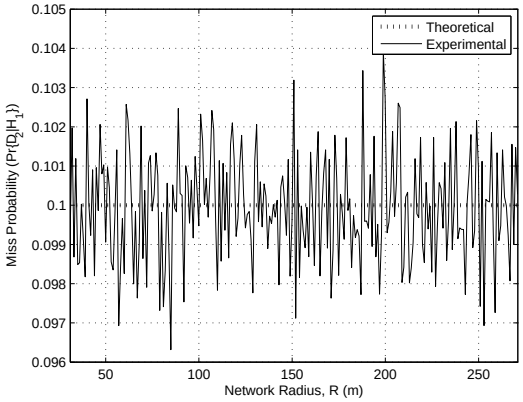


(b) Probability of missing primary user using the NPCHT. Note that the experimental values are not too far from the desired threshold.

Figure 3: NPCHT with theoretical probability of missing primary user α=0.2.

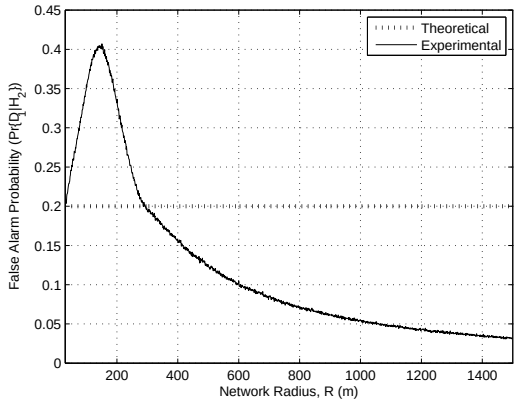


(a) Probability of successful PUEA using the NPCHT. The average number of malicious users is fixed at 25.

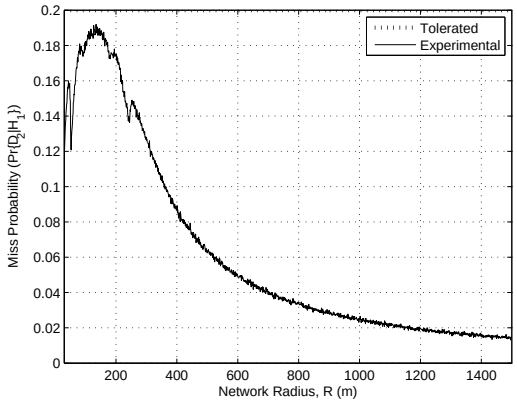


(b) Probability of missing primary user using the NPCHT. Note that the experimental values are not too far from the desired threshold.

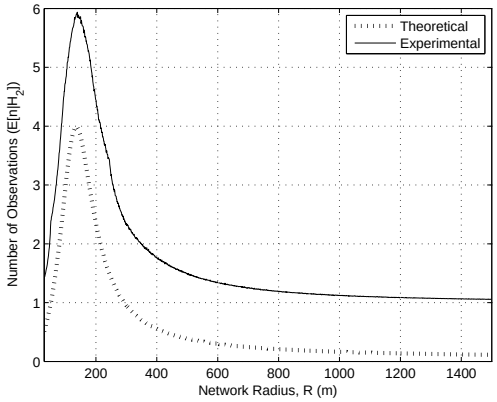
Figure 4: NPCHT with theoretical probability of missing primary user α=0.1.



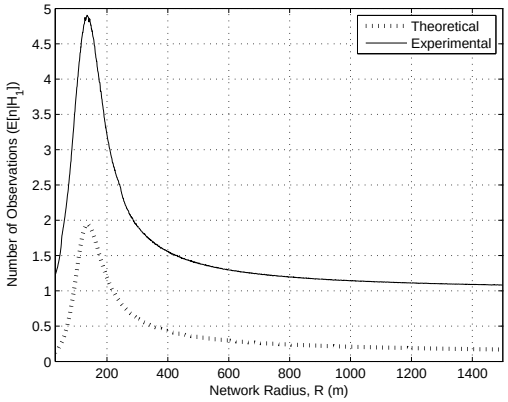
(a) Probability of successful PUEA



(b) Probability of missing primary user

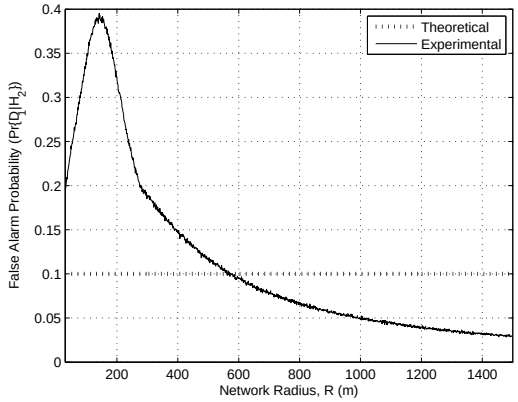


(c) Average number of observations when malicious users are transmitting

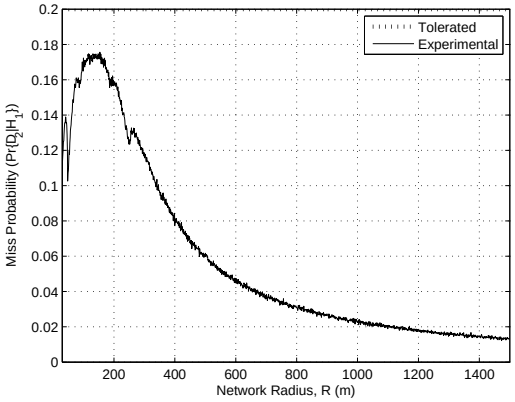


(d) Average number of observations when primary user is transmitting

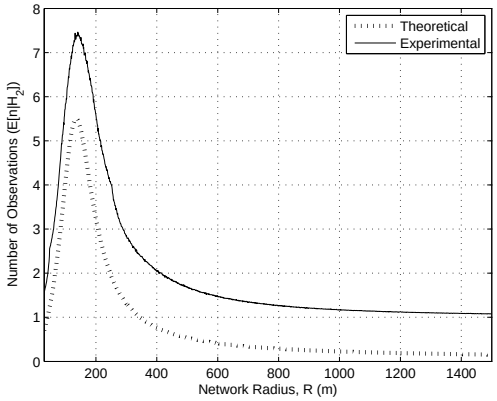
Figure 5: WSPRT with theoretical probability of successful PUEA $\alpha_1 = 0.2$ and theoretical probability of missing primary user $\alpha_2 = 0.2$.



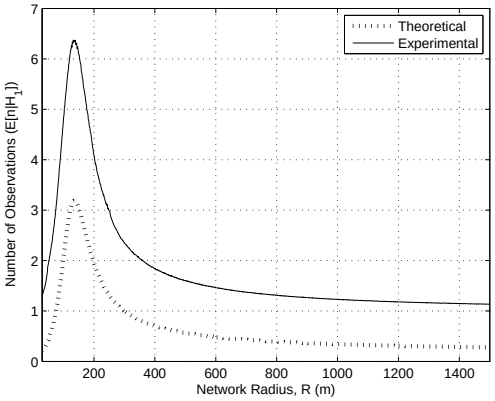
(a) Probability of successful PUEA



(b) Probability of missing primary user

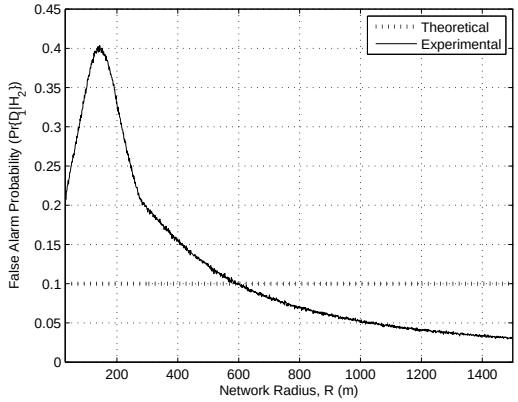


(c) Average number of observations when malicious users are transmitting

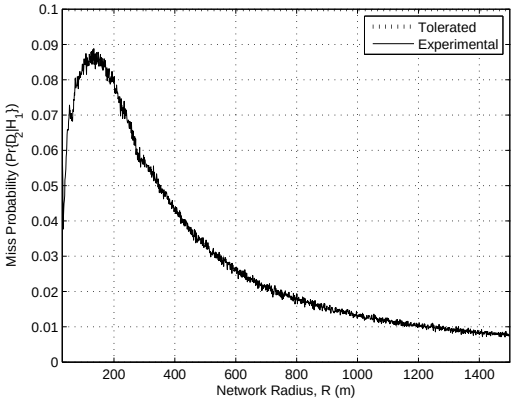


(d) Average number of observations when primary user is transmitting

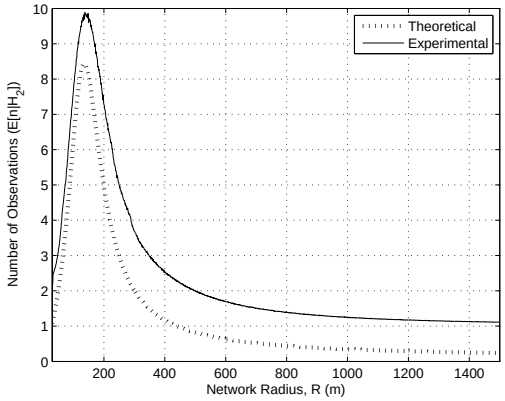
Figure 6: WSPRT with theoretical probability of successful PUEA $\alpha_1 = 0.1$ and theoretical probability of missing primary user $\alpha_2 = 0.2$.



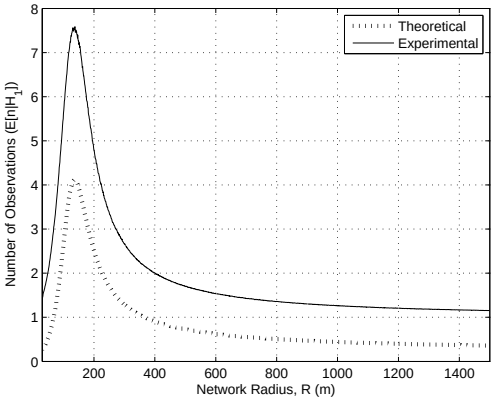
(a) Probability of successful PUEA



(b) Probability of missing primary user



(c) Average number of observations when malicious users are transmitting



(d) Average number of observations when primary user is transmitting

Figure 7: WSPRT with theoretical probability of successful PUEA $\alpha_1 = 0.1$ and theoretical probability of missing primary user $\alpha_2 = 0.1$.

wide wireless standard based on cognitive radios," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN'2005)*, pp. 328–337, Nov. 2005.

[7] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of TV transmission in support of dynamic spectrum sharing," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN'2005)*, pp. 338–345, Nov. 2005.

[8] 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.

[9] G. Jakimoski and K. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks," *IEEE CogNets Workshop, IEEE Intl. Conf. on Commun. (ICC'2008)*, pp. 524–528, May 2008.

[10] G. Jakimoski and K. P. Subbalakshmi, "Towards secure spectrum decision," *To appear, IEEE Intl. Conf. on Commun. (ICC'2009)*, Jun. 2009.

[11] 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.

[12] 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.

[13] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *Proc., IEEE Conf. on Comp. and Commun. (INFOCOM'2008)*, pp. 1876–1884, Apr. 2008.

[14] T. C. Clancy and N. Goergen, "Security in cognitive radio networks: Threats and mitigation," *Proc., Intl. Conf. on Cognitive Radio Oriented Wireless Networks and Commum. (CrownCom'2008)*, May 2008.

[15] A. Sethi and T. X. Brown, "Hammer model threat assessment of cognitive radio denial of service attacks," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN'2008)*, Oct. 2008.

[16] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An analytical model for primary user emulation attacks in cognitive radio networks," *Proc., IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN'2008)*, Oct. 2008.

[17] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," *To Appear, IEEE Intl. Conf. on Commun. (ICC'2009)*, Jun. 2009.

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

[19] L. F. Fenton, "The sum of log-normal probability distributions in scatter transmission systems," *IRE Trans. on Commun. Systems*, vol. 8, no. 1, pp. 57–67, Mar. 1960.

[20] S. Ross, *Probability Models*. Academic Pess, 2003.

[21] J. L. Melsa and D. L. Cohn, *Decision and Estimation Theory*. McGraw-Hill Inc., 1978.