# Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks

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

***Abstract*— In this paper, we present an analytical model as well as a practical mechanism to detect denial of service (DoS) attacks on secondary users in dynamic spectrum access (DSA) networks. In particular, we analyze primary user emulation attacks (PUEA) in cognitive radio networks without using any location information and therefore can do away with any dedicated sensor network. To the best of our knowledge, there are no studies available that detect PUEA using analytical models. We present an analysis using Fenton's approximation and Wald's sequential probability ratio test (WSPRT) to detect PUEA. Simulation results demonstrate that it is possible to keep the probability of missing the primary below a desired threshold while at the same time keeping the probability of successful PUEA low.**

*Keywords* – Dynamic spectrum access networks, primary user emulation, hypothesis test

## I. Introduction

Dynamic spectrum access (DSA) networks [1] have received a lot of attention in the recent decade since they provide more efficient utilization of limited radio resources. Cognitive radio networks [2] enable usage of licensed spectrum by unlicensed "secondary users" when the licensed "primary users" are not using it. Secondary users in a DSA network sense the spectrum to detect unused spectrum bands ("white spaces") which are then used for secondary network communication. A detailed description of the different sensing mechanisms to detect white spaces is provided in [3], and protocols for sensing primary transmission can be found in [4]. The Federal Communications Commission (FCC) [5] mandates that the secondary users must evacuate the spectral bands as soon as a primary transmission is detected. However, since there is no policing in place to ensure this, several denial-of service (DoS) attacks are possible on either the primary users [6] or the secondary users [7], [8], [9]. For example, a set of secondary users (called "malicious users") could transmit signals with characteristics identical to that of a primary transmitter, leading other "good" secondary users (that follow the normal spectrum evacuation etiquette) to vacate the spectrum unnecessarily. The malicious users then use the entire white space for themselves thus causing a DoS attack to the good secondary users. Such attacks are called primary user emulation attacks (PUEA), which were first discussed by Chen and Park in [7].

Chen and Park propose detection of PUEA using the distance ratio test and the distance difference test in [7]. In [8], Chen *et al* proposed a defense mechanism using localization. Localization based methods often assume the presence of a dedicated sensor network to help with the localization of transmitters which is then used to compare against known location of TV transmitters to detect PUEA. Other studies on detection of primary user using spectrum sensing and false spectrum reporting (e.g., [10]) were made, but they do not discuss PUEA. To the best of our knowledge, there are no studies available that use analytical models for received power to detect and evaluate the probability of successful PUEA.

We presented the first analytical model to obtain a lower bound on the probability of successful PUEA in [9]. We considered a fading wireless environment and derived expressions for the probability of successful PUEA using Fenton's approximation. We then used Markov inequality to provide a lower bound on the probability of successful PUEA. In this paper, we present a Wald's sequential probability ratio test (WSPRT) to detect PUEA. We extend our analysis by Fenton's approximation in [9] to obtain the probability density function (pdf) of the received signal from the malicious users, which we use in the derived pdf in the WSPRT. We also show by simulations that our proposed detection mechanism rarely results in a violation of the spectrum evacuation etiquette by setting lower tolerance limits.

The rest of the paper is organized as follows. In Section II, we present the formulation of the problem, the system model and the assumptions made in our analysis. We present our analysis in Section III. Numerical results are presented in Section IV. Section V provides the conclusion.

## II. System Model

We consider a scenario where all secondary and malicious users are distributed in a circular grid. A primary user (e.g., a TV tower), is located at some distance from all the users. Secondary users sense the spectrum (using energy detection [3]) to detect white spaces or presence of the primary transmission. The secondary users[1] measure the received power on a spectrum band. If the received power is below a specified threshold then the spectrum band is considered to be vacant (white space). If the received power is above the specified threshold, then based on the measured power, they make a decision whether the received signal was transmitted by

This work was partially supported by NSF Cyber Trust Grant No. 0627688.

[1]By "secondary users", we mean the "good secondary users" through out this paper unless stated otherwise.

a primary transmitter or by a set of malicious users. We design a WSPRT to obtain a criterion for making the decision mentioned above. We make the following assumptions (most of them are same as in [9]) to perform the analysis.

- There are $M$ malicious users in the system.
- The primary transmitter is at a minimum distance of $d_p$ from all the users.
- The primary transmits at a power $P_t$ and the malicious users transmit at a power $P_m$.
- The positions of the secondary and malicious users are uniformly distributed in the circular grid of radius $R$. The positions of the good users and the malicious users are statistically independent of each other.
- The co-ordinates[2] of the primary transmitter are fixed at a point $(r_p, \theta_p)$ and this position is known to all the users in the grid.
- 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, we showed in [9] that the probabilities scale linearly with the mean of the Rayleigh fading, $\Delta$, and $\Delta = 1$ in most cases [11].
- When represented in decibels (dB), the loss due to shadowing at any secondary user both from the primary transmitter and from any malicious user is normally distributed with mean 0 and variance $\sigma_p^2$ and $\sigma_m^2$, respectively.
- As explained in [9], the path loss exponent for the propagation from the primary transmitter to any secondary users is 2 and that between any malicious user and any secondary user is 4.
- For any secondary user fixed at co-ordinates $(r, \theta)$, no malicious users are present within a circle of radius $R_0$ (called the "exclusive distance from the secondary user") centered at $(r, \theta)$[3].
- There is no communication or co-operation between the secondary users. The PUEA on each secondary user can be analyzed independent of each other.

## III. Analytical Model

Since there is no co-operation between the secondary users. The probability of successful PUEA on any user is same as that on any other user. Hence, without loss of generality, we analyze the pdf of the received signal at any 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 primary transmitter is then at a co-ordinate $(d_p, \theta_p)$[4]. By assumption 4 in Section II, all malicious nodes are uniformly distributed in the annular region with radii $R_0$ and $R$. This scenario is shown in Fig. 1. In order to obtain a hypothesis test using 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 and then describe how we use the obtained pdf to perform the WSPRT and detect PUEA in Section III-B.

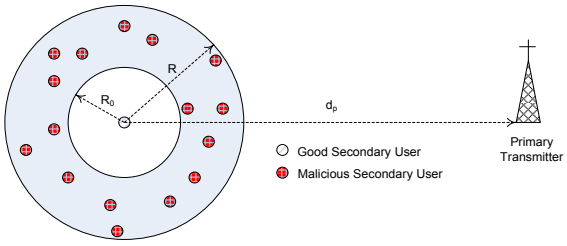



Fig. 1. A typical cognitive radio network in a circular grid with secondary and malicious users. No malicious users can be closer than $R_0$ to the secondary user because if this restriction is not posted, then the power received due to transmission from any subset of malicious users present within this grid will be much larger than that due to a transmission from a primary transmitter thus resulting in failed PUEA all the time [9].

### A. Received Signal pdf

Consider $M$ malicious users located at co-ordinates $(r_j, \theta_j)$ $1 \leq j \leq M$. Since the position of the $j^{th}$ malicious user is uniformly distributed in the annular regions between $R_0$ and $R$, $r_j$ and $\theta_j$ are statistically independent $\forall\ j$. The pdf of $r_j$, $p(r_j)\ \forall\ j$ is given by

$$p(r_j) = \begin{cases} \frac{2r_j}{R^2 - R_0^2} & r_j \in [R_0, R] \\ 0 & \text{otherwise,} \end{cases} \tag{1}$$

while $\theta_j$ is uniformly distributed in $(-\pi, \pi)\ \forall\ j$. The received power at a secondary user from the primary transmitter, $P_r^{(p)}$, is given by

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

where $G_p^2 = 10^{\frac{\xi_p}{10}}$, where $\xi_p \sim \mathcal{N}(0, \sigma_p^2)$ 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

$$p^{(Pr)}(\gamma) = \frac{1}{A\sigma_p\sqrt{2\pi}\gamma} \exp\left\{ -\frac{(10\log_{10}\gamma - \mu_p)^2}{2\sigma_p^2} \right\}, \tag{3}$$

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

$$\mu_p = 10\log_{10} P_t - 20\log_{10} d_p. \tag{4}$$

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

$$P_r^{(m)} = \sum_{j=1}^{M} P_m d_j^{-4} G_j^2, \tag{5}$$

where $d_m$ is the distance between the $j^{th}$ malicious user and the secondary user and $G_m^2$ 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

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

[3]The reason for this is explained in [9].

[4]Note that the actual co-ordinates of the primary transmitter depends on the actual location of the secondary user and will not be exactly $d_p$ for all the users. However, typically, $d_p >> R$ and hence it is justified to approximate the co-ordinates of the primary user to be $(d_p, \theta_p)$ irrespective of which secondary user we consider for the analysis.

the summation in the right hand side of Eqn. (5) 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

$$\mu_j = 10\log_{10} P_m - 40\log_{10} r_j. \tag{6}$$

As we had explained in [9], 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 [12].

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

$$p^{(m)}_{\chi|\mathbf{r}}(\chi|\mathbf{r}) = \frac{1}{A\hat{\sigma}_M\sqrt{2\pi}\chi}\exp\left\{-\frac{(10\log_{10}\chi - \hat{\mu}_M)^2}{2\hat{\sigma}_M^2}\right\}, \tag{7}$$

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[5]

$$\hat{\sigma}_M^2 = \frac{1}{A^2}\ln\left[1 + \frac{(e^{A^2\sigma_m^2} - 1)\sum_{j=1}^{M} e^{2A\mu_j}}{\left(\sum_{j=1}^{M} e^{A\mu_j}\right)^2}\right] \tag{8}$$

and

$$\hat{\mu}_M = \frac{1}{A}\ln\left(\sum_{j=1}^{M} e^{A\mu_j}\right) - \frac{A}{2}(\hat{\sigma}_M^2 - \sigma_m^2), \tag{9}$$

respectively. The pdf of the received power from all the malicious users, $p^{(m)}(\chi)$, can then be obtained by averaging Eqn. (7) over $r_1$, $r_2$, $\cdots$ $r_M$ and can be written as[6]

$$p^{(m)}(\chi) = \int_{[R_0,R]^M}\prod_{j=1}^{M} p^{(m)}_{\chi|\mathbf{r}}(\chi|\mathbf{r})p(r_j)dr_j, \tag{10}$$

where $p(r_j)$ can be obtained from Eqn. (1).

Evaluating Eqn. (10) is very complex. Therefore, we approximate the pdf $p^{(m)}(\chi)$ to be a log-normally distributed random variable with parameters $\mu_\chi$ and $\sigma_\chi^2$ of the form

$$p^{(m)}(\chi) = \frac{1}{A\sigma_\chi\sqrt{2\pi}\chi}\exp\left\{-\frac{(10\log_{10}\chi - \mu_\chi)^2}{2\sigma_\chi^2}\right\}. \tag{11}$$

If $P_r^{(m)}$ is a log-normally distributed random variable with pdf given in Eqn. (11), $\sigma_\chi^2$ and $\mu_\chi$ can be obtained as [13]

$$\sigma_\chi^2 = \frac{1}{A^2}\left(\ln E\left[\left(P_r^{(m)}\right)^2\right] - 2\ln E\left[P_r^{(m)}\right]\right) \tag{12}$$

and

$$\mu_\chi = \frac{1}{A}\left(2\ln E\left[P_r^{(m)}\right] - \frac{1}{2}\ln E\left[\left(P_r^{(m)}\right)^2\right]\right). \tag{13}$$

From Eqn. (7), the conditional expectation of $P_r^{(m)}$, $E\left[P_r^{(m)}|\mathbf{r}\right]$, and that of $\left(P_r^{(m)}\right)^2$, $E\left[\left(P_r^{(m)}\right)^2|\mathbf{r}\right]$, can be evaluated using the analysis mentioned in the Appendix in [9]. $E\left[P_r^{(m)}\right]$ and $E\left[\left(P_r^{(m)}\right)^2\right]$ can then be obtained by averaging $E\left[P_r^{(m)}|\mathbf{r}\right]$ and $E\left[\left(P_r^{(m)}\right)^2|\mathbf{r}\right]$ over $r_1$, $r_2$, $\cdots$, $r_M$ and can be obtained in closed-form as[7]

$$E\left[P_r^{(m)}\right] = \frac{MP_m}{R_0^2R^2}e^{\frac{1}{2}A^2\sigma_m^2}, \tag{14}$$

and

$$E\left[\left(P_r^{(m)}\right)^2\right] = \frac{MP_m^2e^{2A^2\sigma_m^2}}{3R_0^6R^6}\left[\left(\frac{R^6 - R_0^6}{R^2 - R_0^2}\right) + \frac{3(M-1)R^2R_0^2}{e^{A^2\sigma_m^2}}\right]. \tag{15}$$

Substituting the above expressions in Eqns. (12) and (13), we evaluate $\sigma_\chi^2$ and $\mu_\chi$, which, in turn, can be substituted in Eqn. (11) to evaluate the pdf $p^{(m)}(\chi)$.

### B. WSPRT

We consider two hypotheses, $H_1$ that the detected signal was transmitted by the primary, and $H_2$ that the detected signal was transmitted by malicious users. The space of all observations 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.

1) *False Alarm:* When the actual transmission is made by malicious users but the secondary decides that the transmission is due to the primary.
2) *Miss:* When the actual transmission is made by the primary transmitter but the secondary decides that the transmission is due to the malicious users.

It is noted that the probability of false alarm is also the probability of successful PUEA. The WSPRT allows us to specify desired thresholds $\alpha_1$ and $\alpha_2$ for the false alarm and miss probabilities respectively. The decision variable after $n$ sequential tests, $\Lambda_n$, is given by

$$\Lambda_n = \prod_{i=1}^{n}\frac{p^{(m)}(x_i)}{p^{(Pr)}(x_i)}, \tag{16}$$

where $x_i$ is the measured power at the $i^{th}$ stage. In the above, $p^{(Pr)}(x_i)$ and $p^{(m)}(x_i)$ are given by Eqns. (3) and (11), respectively. The decision is then made based on the following criterion:

$$\begin{cases} \Lambda_n \le T_1 = \frac{\alpha_1}{1-\alpha_2} & D_1\text{: Primary Transmitter} \\ \Lambda_n \ge T_2 = \frac{1-\alpha_1}{\alpha_2} & D_2\text{: Malicious Users} \\ \text{else} & D_3\text{: Take another observation .} \end{cases} \tag{17}$$

Eqn. (17) provides a practical mechanism to detect PUEA.

The average number of observations required to arrive at a decision is given by [14]

$$E[n|H_k] = \begin{cases} \frac{(1-\alpha_2)\ln T_1 + \alpha_2\ln T_2}{E[f(x_1)|H_1]} & k = 1 \\ \frac{\alpha_1\ln T_1 + (1-\alpha_1)\ln T_2}{E[f(x_1)|H_2]} & k = 2, \end{cases} \tag{18}$$

[5]The expressions in Eqns. (8) and (9) can be obtained by following the steps specified in the Appendix in [9].

[6]The expressions in Eqns. (7) and (10) should also be conditioned and averaged over the co-ordinates (and hence have integrations over) $\theta_1$, $\theta_2$, $\cdots$, $\theta_M$. However, from Eqns. (6), (8) and (9), it is observed that the expressions are independent of $\theta_1$, $\theta_2$, $\cdots$, $\theta_M$. Therefore, it is sufficient if the averaging (and integrations) are performed over $r_1$, $r_2$, $\cdots$, $r_M$.

[7]We omit the details of the derivation due to lack of space.

where the function $f(x_1) = \ln \Lambda_1$. From Eqns. (3), (11) and (16),

$$E[f(x_1)|H_1] = \ln\left(\frac{\sigma_p}{\sigma_\chi}\right) + \frac{\sigma_\chi^2\mu_p^2 - \sigma_p^2\mu_\chi^2}{2\sigma_p^2\sigma_\chi^2} + \frac{2\mu_p(\sigma_p^2\mu_\chi - \sigma_\chi^2\mu_p)}{2\sigma_p^2\sigma_\chi^2} + \frac{(\sigma_\chi^2 - \sigma_p^2)(\sigma_p^2 + \mu_p^2)}{2\sigma_p^2\sigma_\chi^2} \quad (19)$$

and

$$E[f(x_1)|H_2] = \ln\left(\frac{\sigma_p}{\sigma_\chi}\right) + \frac{\sigma_\chi^2\mu_p^2 - \sigma_p^2\mu_\chi^2}{2\sigma_p^2\sigma_\chi^2} + \frac{2\mu_\chi(\sigma_p^2\mu_\chi - \sigma_\chi^2\mu_p)}{2\sigma_p^2\sigma_\chi^2} + \frac{\sigma_\chi^2 - \sigma_p^2}{2\sigma_p^2\sigma_\chi^2}(\sigma_\chi^2 + \mu_\chi^2). \quad (20)$$

## IV. Results and Discussion

The values of the system parameters we consider for our numerical simulations are listed in Table I.

| Parameter | Value |
|---|---|
| $R_0$ | 30 m |
| $\sigma_p$ | 8 dB [9] |
| $\sigma_m$ | 5.5 dB[9] |
| $P_t$ | 100 KW |
| $P_m$ | 4 W |
| $d_p$ | 100 Km |
| $R$ | $30, \cdots, 1500$ m |
| $M$ | 5, 10, 30 |

TABLE I

VALUES OF PARAMETERS USED IN THE SIMULATIONS.

Fig. 2 displays the false alarm probability (i.e., the probability of successful PUEA) for $(\alpha_1, \alpha_2)$=$(0.2, 0.1)$ and $(0.1, 0.1)$. It is observed that there is a value of $R$ for which the probability of false alarm is maximum. This is because, for a given $R_0$, if $R$ is small, the malicious users are closer to the secondary user and the total received power from all the malicious users is likely to be larger than that received from the primary transmitter. Therefore it is more probable that $\Lambda_n$ goes above $T_2$, thus decreasing the probability of successful PUEA. Similarly, for large $R$, malicious users may not accumulate enough power to reach the secondary user to successfully launch PUEA. It is observed from Fig. 2(b) that the experimental value of the false alarm probability exceeds the desired threshold when $\alpha_1 = \alpha_2 = 0.1$. This indicates that it is not possible to keep both the false alarm probability as well as the miss probability below arbitrarily desired thresholds. In other words, for each specified $\alpha_2$, there is minimum $\alpha_1$ below which thresholds on probability of successful PUEA may not be achieved.

Fig. 3 shows the probability of missing the primary transmitter for $(\alpha_1, \alpha_2)$=$(0.2, 0.1)$ and $(0.1, 0.1)$. It is observed that as in Fig. 2, there is some $R$ for which the miss probability is maximum. *Note, however, that it is always possible to make sure that the probability of missing the primary stays strictly below the required threshold*. This is particularly important in DSA networks to ensure that the secondaries still obey the spectrum sharing etiquette.

Another important parameter to consider when constructing sequential tests is the number of samples that are needed for convergence of the test. Fig. 4[8] shows the theoretical and experimental curves of average number of observations required by the secondary user to make a decision when there are 10 malicious users in the system[9]. The gap between the experimental and theoretical curves are typical of WSPRT [14]. Note that more observations are required as the threshold on false alarm probability reduces from $0.2$ to $0.1$. This is because, from Eqn. (17), as $\alpha_1$ decreases, the threshold $T_1$ decreases and the threshold $T_2$ increases. Thus, it is more likely that the secondary user takes decision $D_3$ (i.e., observes more samples).

## V. Conclusion

We proposed an analytical model and a practical mechanism using WSPRT to detect PUEA in cognitive radio networks. The detection mechanism allows the user to set thresholds on probability of missing the primary user and the probability of successful PUEA and hence can accommodate a range of sensitivities. It is possible to construct tests that always keep the probability of missing the primary user below a specified while still keeping the probability of successful PUEA low.

## References


[1] J. Mitola and G. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Personal Communications*, vol. 6, 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: A survey," *Elsevier Jl. on Computer Networks*, vol. 50, pp. 2127–2158, May 2006.

[4] 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.

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

[6] G. Jakimoski and K. P. Subbalakshmi, "Denial-of-service attacks on dynamic spectrum access networks," *IEEE CogNets Workshop, IEEE International Conference on Communications 2008*, May. 2008.

[7] 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.

[8] 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.

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

[10] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *Proc., IEEE Conf. on Comp. Commun. (INFOCOM) 2008 mini-conference*, Apr. 2008.

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

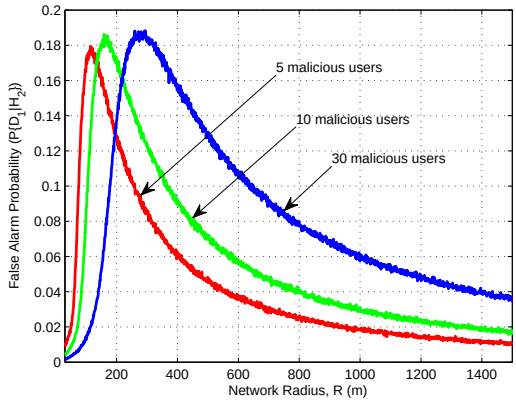
[12] L. F. Fenton, "The sum of log-normal probability distributions in scatter transmission systems," *IRE Trans. on Commun. Systems*, no. CS-8, pp. 57–67, Mar. 1960.

[13] S. Ross, *Pobability Models*. Academic Pess, 2003.

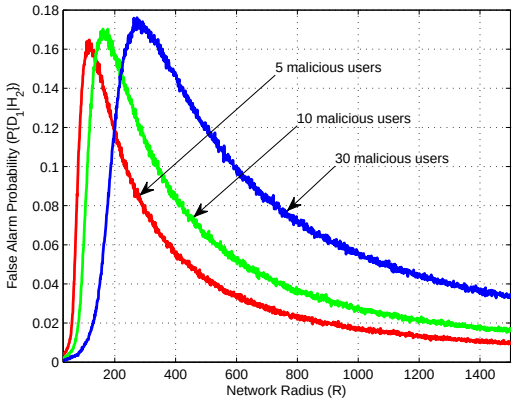
[14] J. L. Melsa and D. L. Cohn, *Decision and Estimation Theory*. McGraw-Hill Inc., 1978.


[8] The "Theoretical" curve in Fig. 4 depicts the $E[n/H_k]$ specified in Eqn. (18) and the experimental curve is the average number of observations obtained by simulations.

[9] Due to lack of space and similarity in results, we do not report the results for other values of $M$.

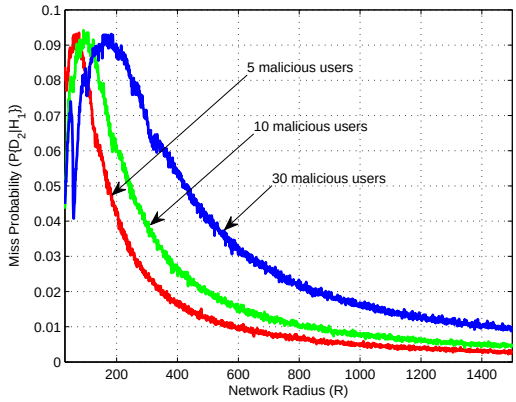



(a) $\alpha_1 = 0.2$, $\alpha_2 = 0.1$

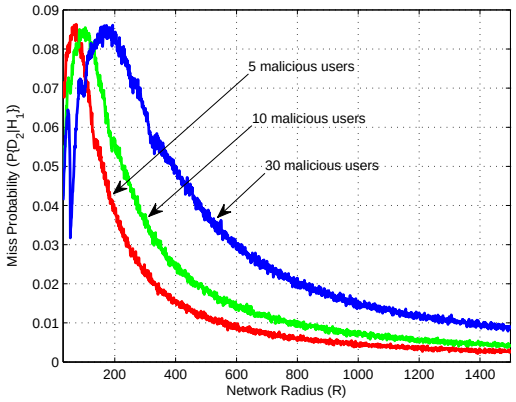



(b) $\alpha_1 = 0.1$, $\alpha_2 = 0.1$

Fig. 2. Probability of false alarm (successful PUEA).

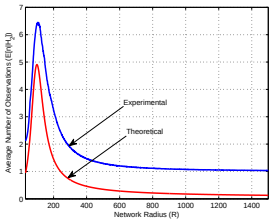



(a) $\alpha_1 = 0.2$, $\alpha_2 = 0.1$

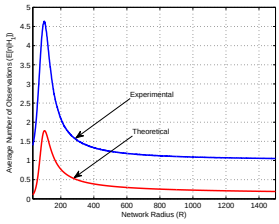



(b) $\alpha_1 = 0.1$, $\alpha_2 = 0.1$

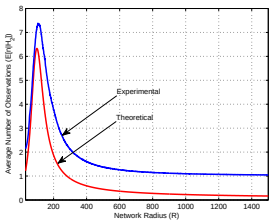
Fig. 3. Probability of missing the primary user.



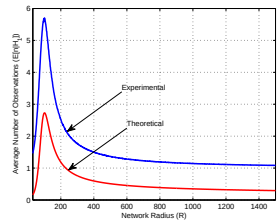

(a) $\alpha_1 = 0.2$, $\alpha_2 = 0.1$




(b) $\alpha_1 = 0.2$, $\alpha_2 = 0.1$




(c) $\alpha_1 = 0.1$,$\alpha_2 = 0.1$




(d) $\alpha_1 = 0.1$, $\alpha_2 = 0.1$

Fig. 4. Average number of observations when a) 10 malicious users are transmitting; b) primary user is transmitting; c) 10 malicious users are transmitting; d) primary user is transmitting.