Robust Spectrum Decision Protocol against 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*— We propose a spectrum decision protocol resilient to primary user emulation attacks (PUEA) in dynamic spectrum access networks. PUEA is a type of denial-of-service attack that can severely interfere with the spectrum sensing process and unfairly deprive legitimate secondary users of spectrum access. In this paper, we present a robust spectrum decision protocol that can mitigate PUEA using individual spectrum decisions made by secondary nodes in the network. In order to enable each secondary node to make an individual spectrum decision to detect PUEA, we first characterize the received power at good secondary user. This is done by using a flexible log-normal sum approximation. The received power thus characterized is used to determine the probability of successful PUEA on each secondary user, which is used to develop the proposed protocol. Simulation results demonstrate that the proposed protocol can significantly reduce the probability of successful PUEA under Byzantine attacks (i.e., when the malicious users intentionally provide false spectrum decisions), while still following the spectrum evacuation etiquette.**

Keywords – Dynamic spectrum access (DSA), primary user emulation attack (PUEA), spectrum decision protocol

I. Introduction

Dynamic spectrum access (DSA) networks have received extensive attention recently because of their ability to better serve the growing bandwidth demands of the users. This is achieved by allowing unlicensed "secondary users" to access spectrum bands when the licensed "primary users" do not use these bands. Secondary users continuously sense the spectrum and follow a spectrum evacuation etiquette to evacuate the band, upon the return of the primary user. This spectrum evacuation protocol, however, can be manipulated by malicious users, by tricking the system into believing that there is a primary user, when none is present. This can be done in various ways, one of which is to emulate the signal characteristics of the primary. Thus, the good secondary users following the normal spectrum evacuation process evacuate the spectrum unnecessarily, leading to what is known as primary user emulation attack (PUEA) [1].

Several methods exist to thwart PUEA and can be classified into location aware [2] and location unaware techniques [3],[4]. Typically, location aware techniques involve significant infrastructure overhead like a dedicated sensor network to determine the locations of transmitters [2]. We recently proposed a Wald's sequential probability ratio test for individual secondary users to detect PUEA in [3] and extended the analysis in [4] to include a Neyman-Pearson composite hypothesis test as an alternative. The network may also use a centralized decision rule (where individual secondaries transmit data concerning primary activity to a centralized controller[1] which then makes the final decision on PUEA's presence) or operate in a non-centralized manner (where each secondary user makes its own decision about the presence of PUEA) to detect PUEA. If designed well, the probability of successful PUEA can be significantly reduced in the centralized model.

In this paper, we propose a robust spectrum decision protocol for DSA networks with centralized controller which uses the individual sensing results of secondary users to make the final spectrum decision for the entire network. We first use a flexible log-normal sum approximation to characterize the received power at good secondary user. We then propose an individual detection mechanism for secondary users to achieve individual sensing results. The probability of successful PUEA at each good user is then derived to analyze the effect of PUEA on the whole network, in terms of the number of good users successfully attacked by the malicious users. A robust spectrum decision protocol, in which a centralized controller collects individual sensing results from secondary users and makes the final spectrum decision for the entire network, is then developed to defend the network against PUEA. We also take into account that in addition to launching PUEA, malicious users could also launch Byzantine attacks [5] by sending false sensing results to the centralized controller. We show by simulations that the proposed protocol can effectively mitigate PUEA under Byzantine attacks while still following the spectrum evacuation etiquette.

The rest of the paper is organized as follows. In Section II, we present the system model. In Section III, we propose the robust spectrum decision protocol that is resilient to PUEA. Numerical results are presented in Section IV. Section V provides the conclusion.

[1]The centralized controller can be, e.g., a base station in IEEE 802.22 WRANs, or a trustworthy secondary user in ad-hoc DSA networks.

II. System Model

We consider a scenario where all secondary users, i.e., all the good users and the malicious users, are distributed in a square grid as shown in Fig. 1. A primary user is located at a distance d_p from the center of the square grid. Spectrum sensing of secondary user is based on energy detection, i.e., a secondary user compares its received power to some pre-defined thresholds. If the received power is below the detection sensitivity, then the spectrum band is considered to be vacant. Otherwise, the spectrum band could contain the signal transmitted by the primary transmitter, or the signal transmitted by the set of malicious users with the intent to launch PUEA. The good users, then have to determine whether the current transmission is from the primary user or from the malicious users.

Our objective in this paper is two fold.

1) Develop a detection mechanism to enable each individual node to make a spectrum decision (i.e., determine whether the received signal is from the primary transmitter or PUEA).
2) Develop a centralized spectrum decision protocol, in which a centralized controller gathers the spectrum decisions made by each secondary node, to perform a common spectrum decision for all the nodes, to detect PUEA.

In order to achieve objective 1) mentioned above, it is desired to analyze the received power at each secondary node, due to transmission by the primary transmitter, as well as due to transmission by the malicious users. The following assumptions are made to carry out our analysis.

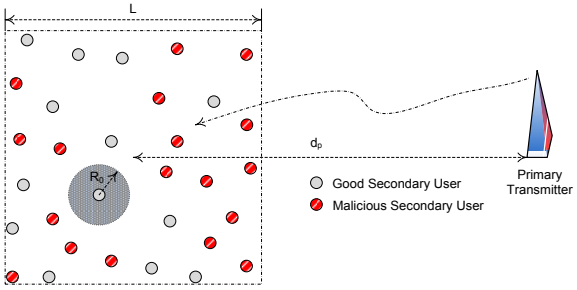


Fig. 1. A dynamic spectrum access network with length L, consisting of good secondary users and malicious secondary users. No malicious users are present within a radius R_0 about each good user. A primary transmitter is located at a distance d_p from the center of the grid.

1) There are N_g good users and N_m malicious users, spatially Poisson distributed with parameters λ_g and λ_m, respectively, in a square grid of length L.
2) The positions of the good users and the malicious users are statistically independent of each other.
3) For the i^{th} good user located at (x_i, y_i), no malicious users are present within a circle of radius R_0 centered at (x_i, y_i). R_0 is the "exclusive distance from the secondary user" [4].
4) The primary user transmits at a power of P_t and the malicious users transmit at a power of P_m.
5) The path loss exponent for the propagation from the primary user to any good user is 2 while that from any malicious user to any good user is 4 [4].
6) The RF signals also undergo log-normal shadowing. The shadowing at any good user both from the primary user and from any malicious user, denoted by G_p^2 and G_m^2, are log-normally distributed respectively, i.e., $10\log_{10}\left(G_p^2\right) \sim \mathcal{N}\left(0, \sigma_p^2\right)$ and $10\log_{10}\left(G_m^2\right) \sim \mathcal{N}\left(0, \sigma_m^2\right)$, where $\mathcal{N}(\mu, \sigma^2)$ denotes a normal distribution with mean μ and variance σ^2.
7) The Rayleigh fading is assumed to be averaged out and can hence be ignored [4].

III. Protocol to Mitigate Primary User Emulation Attacks

Before developing the protocol resilient to PUEA, we present the analysis to obtain the various parameters required to develop the protocol. We first characterize the received power at each good secondary user in Section III-A. We then use this to obtain the probability density function (pdf) of the received power in Section III-B. In Section III-C, an individual detection mechanism for secondary users is proposed and its effect on the entire network is studied. The parameters thus determined are finally used to develop the protocol in Section III-D.

A. Received Power at Good User

Since the primary user is usually far away from the secondary network, its distance to any good user can be approximated by d_p. Thus the received power at any good user from the primary, $P_r^{(p)}$, can be written as

$$P_r^{(p)} = P_t (d_p)^{-2} G_p^2. \tag{1}$$

For any good user, its received power from j^{th} malicious neighbor, $P_r^{(m_j)}$, can be written as

$$P_r^{(m_j)} = P_m (d_j^m)^{-4} G_m^2, \tag{2}$$

where d_j^m is the distance from the good user to its j^{th} malicious neighbor (therefore, $d_1^m \leq d_2^m \leq \cdots \leq d_{N_m}^m$). The total received power from all N_m malicious users, $P_r^{(m)}$, can be obtained as

$$P_r^{(m)} = \sum_{j=1}^{N_m} P_r^{(m_j)}. \tag{3}$$

Typically, the power received at a secondary user from its first two malicious neighbors is much larger than the sum of the power received from all the other malicious neighbors. This is because, $d_j^m >> d_i^m$, for $j > 2$ and $i = 1, 2$, and hence, $(d_j^m)^{-4}$, for $j > 2$, is negligible. Therefore, we only consider the power received from the first two malicious neighbors. Thus, $P_r^{(m)}$ can be approximated by[2]

$$P_r^{(m)} \approx P_r^{(m_1)} + P_r^{(m_2)}, \tag{4}$$

where $P_r^{(m_1)}$ and $P_r^{(m_2)}$ can be obtained from Eqn. (2).

[2]This approximation will be justified in Fig. 2 in Section IV.

Since the good users and the malicious users are both spatially Poisson distributed, and their locations are independent of each other, all $N = N_g + N_m$ secondaries including both good and malicious users are also spatially Poisson distributed with parameter $\lambda = \lambda_g + \lambda_m$. The pdf of the distance between any good user and its n^{th} neighbor, d_n, is given by ([6], Theorem 1)

$$f_n(d_n) = e^{-\lambda\pi d_n^2} \frac{2(\lambda\pi d_n^2)^n}{d_n \Gamma(n)}, \quad (5)$$

where $\Gamma(\cdot)$ is the generalized Gamma function. From Eqn. (3), the total received power from all N_m malicious users depends on $(d_j^m)^{-4}$, $\forall\ j$, which, in turn, is determined by the location of the good user and the location of the malicious user. Since all locations are random, computation of $P_r^{(m)}$ is complex. Therefore, we use $E[(d_j^m)^{-4}]$ to simplify analysis. Since the positions of the secondary users (good and malicious) are independent, the j^{th} malicious neighbor of a good user is the n^{th} neighbor $(j \leq n \leq N-1)$ with probability $\binom{n-1}{j-1} \left(\frac{\lambda_m}{\lambda}\right)^j \left(\frac{\lambda_g}{\lambda}\right)^{n-j}$. Therefore, $E[(d_j^m)^{-4}]$ is given by

$$E[(d_j^m)^{-4}] = \sum_{n=j}^{N-1} E[(d_n)^{-4}] \binom{n-1}{j-1} \left(\frac{\lambda_m}{\lambda}\right)^j \left(\frac{\lambda_g}{\lambda}\right)^{n-j}, \quad (6)$$

which can be further simplified by approximating N by $E[N]$. In Eqn. (6), $E[(d_n)^{-4}]$ can be obtained by using Eqn. (5). $P_r^{(m_j)}$ is thus obtained by substituting Eqn. (6) in Eqn. (2), and then $P_r^{(m)}$ can be calculated from Eqn. (4).

B. Probability Density Function of Received Power

Since d_p and P_t are fixed, $P_r^{(p)}$ is log-normally distributed, i.e., $10\log_{10}\left(P_r^{(p)}\right) \sim \mathcal{N}(\mu_p, \sigma_p^2)$, where μ_p is given by

$$\mu_p = 10\log_{10}(P_t) - 20\log_{10}(d_p). \quad (7)$$

Similarly, conditioned on $E[(d_j^m)^{-4}]$ and P_m, every term of the right hand side of Eqn. (3) is also log-normally distributed, thus, $P_r^{(m)}$ can be approximated as a log-normal random variable (RV). To compute the statistical parameters of $P_r^{(m)}$, we adopt the flexible log-normal sum approximation method proposed by Wu *et al* in [7]. Thus, conditioned on the distance to the 1^{st} malicious neighbor and P_m, $P_r^{(m_1)}$ is log-normally distributed, i.e., $10\log_{10}\left(P_r^{(m_1)}\right) \sim \mathcal{N}(\mu_{m_1}, \sigma_m^2)$. Since the distance to the 1^{st} malicious neighbor is approximated by $E[(d_1^m)^{-4}]$, μ_{m_1} is given by

$$\mu_{m_1} = 10\log_{10}(P_m) + 10\log_{10}\left(E[(d_1^m)^{-4}]\right). \quad (8)$$

Similarly, $10\log_{10}\left(P_r^{(m_2)}\right) \sim \mathcal{N}(\mu_{m_2}, \sigma_m^2)$, where μ_{m_2} is given by

$$\mu_{m_2} = 10\log_{10}(P_m) + 10\log_{10}\left(E[(d_2^m)^{-4}]\right). \quad (9)$$

$P_r^{(m)}$ is then modeled as a log-normal RV, i.e., $10\log_{10}\left(P_r^{(m)}\right) \sim \mathcal{N}(\mu_M, \sigma_M^2)$. The expressions for μ_{m_1} and μ_{m_2} in Eqns. (8) and (9) are used to compute μ_M and σ_M by using the technique described in [7].

C. Individual Detection Mechanism for Good User

Currently, no policy on spectrum sensing has incorporated any counter-measure to PUEA. This however, is not recommended for good users to sense the primary transmission (i.e., based only on the detection sensitivity), because even a small number of malicious users can transmit enough power to make the received power at good user exceed the detection sensitivity (usually -94dBm), thus resulting in successful PUEA all the time. In this subsection, we propose an individual detection mechanism for good user, with the goal of achieving moderate PUEA resilience while not compromising the sensitivity required to detect the return of the primary user. The proposed detection mechanism is then incorporated into the spectrum decision protocol that will be proposed in Section III-D, to further mitigate PUEA.

Since $10\log_{10} P_r^{(p)} \sim \mathcal{N}(\mu_p, \sigma_p^2)$ with μ_p given by Eqn. (7), we propose to use the empirical rule of normal distribution to detect the primary user, which is as follows. The received power from the primary user represented in decibels (dB), $P_r^{(p)}$(dB), is most likely to satisfy $\mu_p - 3\sigma_p \leq P_r^{(p)}\,(\text{dB}) \leq \mu_p + 3\sigma_p$. Therefore, by setting the detection thresholds as $\mu_p - 3\sigma_p$ and $\mu_p + 3\sigma_p$, the probability of missing the primary (i.e., failing to detect the presence of primary user), p_{miss}, is given by

$$\begin{aligned} p_{\text{miss}} &= 1 - \Pr\left\{\mu_p - 3\sigma_p \leq P_r^{(p)}\,(\text{dB}) \leq \mu_p + 3\sigma_p\right\} \\ &= 1 - Q(-3) + Q(3) \\ &= 0.002701, \end{aligned} \quad (10)$$

where $Q(\cdot)$ is the Q-function defined by $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{t^2}{2}\right) dt$. Thus, the probability of successful PUEA, p_{PUEA}, is given by

$$\begin{aligned} p_{\text{PUEA}} &= \Pr\left\{\mu_p - 3\sigma_p \leq P_r^{(m)}\,(\text{dB}) \leq \mu_p + 3\sigma_p\right\} \\ &= Q\left(\frac{\mu_p - 3\sigma_p - \mu_M}{\sigma_M}\right) \\ &\quad - Q\left(\frac{\mu_p + 3\sigma_p - \mu_M}{\sigma_M}\right). \end{aligned} \quad (11)$$

Let K denote the number of good users attacked by the malicious users and K' denote the number of good users that miss the primary. Since the probability of successful PUEA on any good user is independent of that on any other good user and the number of good users is a Poisson RV, the set of attacked users can be obtained by splitting the number of good users, N_g, according to a Bernoulli process with probability of success, p_{PUEA}. Thus K is a Poisson RV with parameter $E[N_g]p_{\text{PUEA}}$. Similarly, K' is a Poisson RV with parameter $E[N_g]p_{\text{miss}}$. Hence, the expected number of attacked users, μ_K, and the variance of the number of attacked users, σ_K^2, are given by

$$\mu_K = \sigma_K^2 = E[N_g]\, p_{\text{PUEA}}. \quad (12)$$

Similarly, the expected number of good users missing the primary, $\mu_{K'}$, and the variance of the number of good users

missing the primary, $\sigma^2_{K'}$, are given by

$$\mu_{K'} = \sigma^2_{K'} = E[N_g]\, p_{\text{miss}}. \quad (13)$$

The values of μ_K, σ_K, $\mu_{K'}$ and $\sigma_{K'}$ can be used to obtain a spectrum decision protocol to mitigate PUEA, as will be explained in the following subsection.

D. Spectrum Decision Protocol against Primary User Emulation Attacks

We now develop the spectrum decision protocol resilient to PUEA, in which a centralized controller obtains the individual spectrum decisions made according to the discussion in Section III-C, from all the secondary users. The basic idea behind the protocol is as follows. From the values of μ_K and σ_K given by Eqn. (12), it is possible to estimate the number of secondary users who sense primary transmission when PUEA is launched. This set of users also includes the malicious users who launch Byzantine attacks, i.e., spuriously claim primary transmission while launching PUEA. Similarly, from $\mu_{K'}$ and $\sigma_{K'}$ given by Eqn. (13), we can estimate the number of secondary users who would successfully detect primary transmission when the primary user transmits. It is noted that when primary transmission takes place, the malicious users do not gain anything by launching Byzantine attacks and hence, will provide correct information to the centralized controller. Since the individual detection mechanism detects PUEA to some extent and hardly misses the primary user, one can expect more users claiming primary transmission when the primary user transmits than when PUEA is launched. Therefore by setting appropriate thresholds on the number of users whose individual detection indicates primary transmission, the centralized controller can mitigate PUEA. The detailed description of the protocol is as follows.

1) Each individual secondary user senses the spectrum and sends its sensing result to the centralized controller based on the individual detection mechanism proposed in Section III-C, i.e.,
   a) if the received power in dB is in the range $[\mu_p - 3\sigma_p, \mu_p + 3\sigma_p]$, the secondary user claims that the primary transmission is detected,
   b) else, it claims that PUEA is detected.
2) The centralized controller determines whether the ongoing transmission is from the primary user or due to PUEA, based on the following criteria,
   a) if the number of sensing results claiming primary transmission, denoted by N_p, is greater than $N_u = E[N_g] - \lceil \mu_{K'} \rceil - \lceil A\sigma_{K'} \rceil + E[N_m]$, the centralized controller determines that the transmission is from the primary user,
   b) else if $N_p < N_l = \lceil \mu_K \rceil + \lceil B\sigma_K \rceil + E[N_m]$, the centralized controller decides that the malicious users are launching PUEA,
   c) else (i.e., when $N_l \leq N_p \leq N_u$), the centralized controller concludes primary transmission with probability $\frac{N_p - N_l}{N_u - N_l}$ or PUEA with probability $\frac{N_u - N_p}{N_u - N_l}$.
3) After the good users receive the spectrum decision sent by the centralized controller, they
   a) vacate the spectrum if the centralized controller decides that it is primary transmission,
   b) else, continue using the spectrum if the centralized controller decides that it is PUEA.

The values of A and B are chosen to reduce the gap between N_u and N_l, and to maintain $N_u > N_l$. The choice of the actual values is empirical.

IV. Numerical Results

The values of the system parameters used in simulations are listed in Table I.

Parameter	Value	Parameter	Value
d_p	100 Km	P_t	100 KW
L	2000 m	P_m	4 W
$E[N_g]$	200	σ_p	8 dB
R_0	30 m	σ_m	5.5 dB
A	3	B	1

TABLE I

VALUES OF PARAMETERS USED IN SIMULATIONS.

Fig. 2 shows the comparison of the received power at any good user from its first two malicious neighbors and that from all the other malicious neighbors. It can be seen that the received power from the first two malicious neighbors is about one to three orders of magnitude greater than that from all the other malicious neighbors, thus justifying the approximation in Eqn. (4).

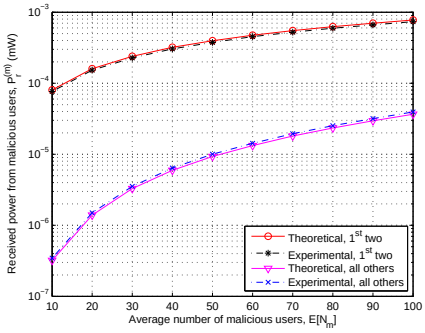
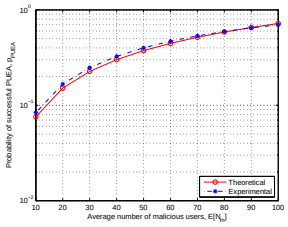


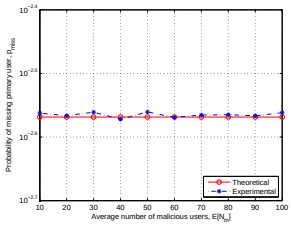
Fig. 2. Comparison of received power at good user from its first two malicious neighbors, and that from all the other malicious neighbors.

Fig. 3 presents the detection error in terms of the probability of successful PUEA and the probability of missing the primary user when good users make individual spectrum decisions, based on the detection mechanism proposed in Section III-C. It is observed that the theoretical results closely follow the experimental results, thus validating the analysis presented in Sections III-A, III-B and III-C. It can be seen from Fig. 3(a) that although sometimes PUEA may be detected easily by some individual nodes, by deploying the proposed individual

detection mechanism, the network as a whole, still suffers with the probability of successful PUEA as high as about 0.7. This brings forth, the need for additional security enhancements to further mitigate PUEA. It can also be seen that the probability of successful PUEA increases as the number of malicious users increases, indicating that more good users will be attacked if the malicious users accumulate more transmitting power. Note that in Fig. 3(b), the probability of missing the primary user is fixed, which follows from Eqn. (10).



(a) Probability of successful PUEA.



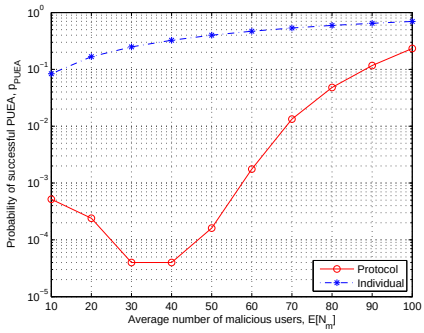
(b) Probability of missing the primary.

Fig. 3. Detection error when good users use the individual detection mechanism proposed in Section III-C.

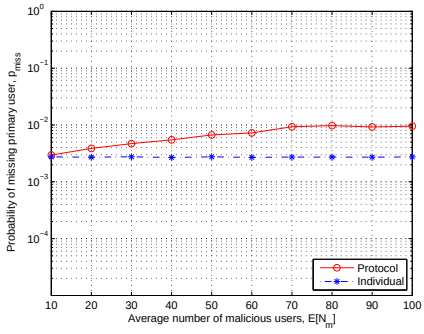
Fig. 4 presents the comparison on detection error between the protocol described in Section III-D and the individual detection mechanism proposed in Section III-C, under Byzantine attacks. From Fig. 4(a) we observe that the probability of successful PUEA can be significantly reduced after implementing the proposed protocol. For example, for $E[N_m] = 50$, the proposed protocol results in a probability of successful PUEA of 1.6×10^{-4}, as against the probability of 0.4 if nodes rely only on the individual detection mechanism. For $E[N_m] = 100$, a reduction of 66.5% on the probability of successful PUEA can be achieved when the proposed protocol is used. It is also shown in Fig. 4(b) that although the proposed protocol results in a higher probability of missing the primary user, the actual values of the probability never exceed 0.01. Therefore, the proposed protocol can successfully defend the network against PUEA in the presence of Byzantine attacks while still following the spectrum evacuation etiquette.

V. Conclusion

We presented a centralized spectrum decision protocol for mitigating PUEA in DSA networks. The proposed protocol made use of the individual spectrum decision made by each secondary user. The individual spectrum decision was obtained by characterizing the received power at good secondary user through a flexible log-normal sum approximation method. The proposed protocol was resilient to PUEA and resulted in a significantly reduced probability of successful PUEA in the presence of Byzantine attacks, while still following the spectrum evacuation etiquette. The extension of the proposed idea to obtain distributed spectrum decision protocols, is under investigation.



(a) Probability of successful PUEA.



(b) Probability of missing the primary.

Fig. 4. Comparison on detection error between the protocol described in Section III-D and the individual detection mechanism proposed in Section III-C, under Byzantine attacks.

Acknowledgment

This research was partially funded by NSF # 0917008 and NSF # 0916180 and partially funded by 2009-92667-NJ-IJ.

References

[1] 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*, pp. 110–119, Sep. 2006.

[2] 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.

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

[4] ——, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing," *ACM SIGMOBILE Mobile Computing and Commun. Review, Spl. Issue on Cognitive Radio Technol. and Sys.*, vol. 13, no. 2, pp. 74–85, April 2009.

[5] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. on Prog. Languages and Sys.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[6] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. on Info. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.

[7] J. Wu, N. B. Mehta, and J. Zhang, "A flexible lognormal sum approximation method," *Proc., IEEE Global Commun. Conf. (GLOBECOM'2005)*, vol. 6, pp. 3413–3417, Dec. 2005.