NEAT: A NEighbor AssisTed Spectrum Decision Protocol for Resilience against Primary User Emulation Attacks

Z. Jin, S. Anand and K. P. Subbalakshmi
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, New Jersey 07030, USA
{zjin, asanthan, ksubbala}@stevens.edu

***Abstract*—We propose a distributed spectrum decision protocol resilient to primary user emulation attacks (PUEA) in dynamic spectrum access (DSA) networks. PUEA is a type of denial-of-service attack that can result in unreliable and/or disconnected DSA networks by depriving legitimate secondary users of spectrum access. We first propose an individual detection mechanism for secondary users to achieve preliminary sensing results. For this, we characterize the received power at a good secondary user, using a flexible log-normal sum approximation. We then develop a distributed spectrum decision protocol in which secondary users exchange individual sensing results with their one-hop neighbors to increase resilience to PUEA. We call this protocol NEAT: NEighbor AssisTed spectrum decision protocol. We provide mathematical analysis of this protocol in terms of both the probability of successful PUEA as well as the probability of missing the primary, under Byzantine attacks – when the malicious users also lie about PUEA with some probability. We then compare the performance of the proposed protocol to the majority logic rule. We show that with negligible communication overhead, the proposed protocol reduces the probability of successful PUEA by 52%-100% in the presence of Byzantine attacks, while still following the spectrum evacuation etiquette.**

***Index Terms*—Dynamic spectrum access, primary user emulation, Byzantine attack, spectrum decision protocol.**

I. Introduction

Enhancing efficient usage of the limited spectrum resources has received extensive attention in the recent decades. Traditionally, spectral bands were assigned to licensed users. Users other than licensed holders were not allowed to access these bands. However, spectrum occupancy measurements show that this fixed spectrum assignment leads to an under-utilization of the spectrum resources [1],[2]. A new communication paradigm called cognitive radio (CR) enabled dynamic spectrum access (DSA) [3], provides a mechanism to address the under-utilization of licensed spectrum bands. DSA networks consist of two types of users: (i) the primary users who hold licenses to the spectrum bands and can access these bands at any time, and (ii) the secondary users who do not have licenses, but can use the spectrum bands *when they are not used* by the primary users, thus improving the spectrum utilization. In order to ensure that the primary communication is not disrupted in anyway, the secondary nodes must periodically sense the bandwidth for the return of primary user and promptly leave the band when the primary user is detected. This is called spectrum etiquette. One example of DSA networks is the utilization of unused spectrum (or white spaces) in the TV bands. The TV transmitter and receivers are the primary users. Other users who are not TV subscribers but wish to use the white spaces in the TV bands for their own communications are the secondary users. The IEEE 802.22 working group on wireless regional area networks (WRAN) provides the physical (PHY) layer and medium access control (MAC) layer specifications for the usage of the TV white spaces [4].

Spectrum sensing by the secondary users is one of the most important functionalities in the implementation of DSA networks since it is essential both for identification of white spaces as well as for prompt evacuation upon the return of the primary users. The well known detection techniques are: (i) energy detection, (ii) matched filter detection and (iii) cyclostationary feature detection [5]. In this paper, we use energy detection technique since it is the most widely used sensing mechanism due to its low implementation complexity. Protocols for spectrum sensing and spectrum evacuation can be found in [6] and [7].

In this paper we study a DoS attack that is unique to DSA networks, called the primary user emulation attack (PUEA) [8],[9]. In this type of attack, a set of malicious secondary users mimic the primary transmission, leading other secondary users to believe that the primary user is present when it is not. The good (non-malicious) secondary users following normal spectrum evacuation process will vacate the spectrum unnecessarily. This could result in the network being unreliable or become disconnected because the users that vacate the spectrum band could form the cut-vertices of the underlying DSA network. PUEA could also lead to loss of data that was incident on the users that leave the network. It therefore becomes important to devise efficient defence mechanisms against PUEA in DSA networks.

PUEA was first discussed by Chen *et al* in [8] and [9]. In [8], they propose two mechanisms to detect PUEA, i.e., the distance ratio test and the distance difference test based on the correlation between the length of wireless link and the received signal strength. However, their discussion was based on two strong assumptions that there exists only one malicious user in the network and that secondary users can locate themselves via global positioning system (GPS). In [9], Chen *et al* propose a defense mechanism against PUEA by locating the spurious transmission via an underlying sensor network and comparing it with the known location of the primary transmitter. The mechanisms described thus far do not consider the fading characteristics of the wireless channel. Moreover, they either require a dedicated sensor network or require significant enhancement of the secondary users themselves.

We presented the first analytical model to characterize the probability of PUEA based on energy detection [10]. We then proposed a Wald's sequential probability ratio test [11],[12] and a Neyman-Pearson composite hypothesis test [12] to detect PUEA using hypothesis testing. The mechanisms proposed in [11] and [12] were non-cooperative, i.e., secondary users detected PUEA only based on their individual sensing observations and without cooperation or sharing information with other secondary users. Sharing the individual decisions with other secondary users could help users mitigate PUEA better because, the users who are successfully attacked by the malicious users could potentially correct their sensing decision based on the information obtained from neighboring users.

In this paper, we propose a distributed spectrum decision protocol in which secondary users exchange their individual sensing results with their one-hop neighbors, in order to mitigate PUEA. We first propose an individual detection mechanism for secondary users. We model the received power at each good secondary user using a flexible log-normal sum approximation. We present a mechanism where each individual user senses to see if a primary is present or if a PUEA is being launched. Users then exchange this information with their one-hop neighbors. We propose a distributed spectrum decision protocol where the individual spectrum sensing decision exchanged between the users and their one-hop neighbors is used to mitigate PUEA, with minimum communication overheads. We analyze the effectiveness of the protocol in the presence of Byzantine attacks from the malicious users. Numerical results indicate that the proposed protocol can reduce the probability of successful PUEA by $52\% - 100\%$ in the presence of Byzantine attacks, while still following the spectrum evacuation etiquette.

The rest of the paper is organized as follows. Section II presents the system model. The analysis for the proposed distributed spectrum decision protocol is presented in Section III. In Section IV, we provide the security analysis of the protocol. Numerical results are presented in Section V. In Section VI, we discuss some practical considerations when implementing the proposed protocol. Section VII provides the conclusion.

II. System Model

We consider a scenario where all secondary users: both the good and the malicious are randomly placed in a square grid as shown in Fig. 1. A primary transmitter is located at a distance, d_p, from the center of the grid. Spectrum sensing is based on energy detection, i.e., a good user compares its received power to some pre-defined thresholds. If the received power is below detection sensitivity, the spectrum band is considered to be vacant, otherwise, the good user has to determine whether the received signal is from the primary user or from the malicious users. After each individual secondary user makes the decision, it is desired to design a distributed protocol resilient to PUEA, wherein individual users exchange their decisions with their one-hop neighbors. The following assumptions about the network are made to perform the analysis.

1) The good secondary users and malicious secondary users are spatially Poisson distributed in a square grid of dimension $L \times L$.
2) There are N_g good users and N_m malicious users, both spatially poisson distributed in the network with intensities λ_g and λ_m, respectively, i.e., $E\left[N_g\right] = \lambda_g L^2$ and $E\left[N_m\right] = \lambda_m L^2$. The positions of good users and malicious users are statistically independent of each other.
3) The primary transmitter is at a distance d_p from the center of the grid and d_p is known to all secondary users.

III. Distributed Spectrum Decision Protocol Resilient to Primary User Emulation Attacks

In order to devise the distributed protocol, it is essential to characterize the probability of successful PUEA at each individual good user. This is done by determining the received signal at each good user due to transmission from the primary and that from the malicious users. We present the analysis for modeling the received power in Section III-A. In Section III-B, the probability density function of the received power from malicious users is presented. Section III-C provides the analysis for detection mechanism at each individual user and the proposed distributed protocol is described in Section III-D.

A. Received Power at Good Secondary User

In order to model the received power due to transmission from the primary transmitter and that from the malicious users, we make the following assumptions in addition to assumptions 1)-3) mentioned in Section II.

1) The primary transmitter transmits with power, P_t, and each malicious user transmits with power P_m.
2) The RF signal from the primary transmitter and the malicious users undergoes log-normal shadowing and path loss[1].
3) The path loss exponent is taken to be 2 (as in free space propagation) for primary transmission and 4 for transmission from the malicious users (as in two-ray ground propagation).
4) The loss due to shadowing from the primary transmitter, G_p^2, is a log-normal random variable, i.e., $10\log_{10} G_p^2 \sim \mathcal{N}(0, \sigma_p^2)$.
5) The loss due to shadowing from the malicious users, G_m^2, is a log-normal random variable, i.e., $10\log_{10} G_m^2 \sim \mathcal{N}(0, \sigma_m^2)$.

[1] If Rayleigh fading is included, it scales all the expressions by a factor, Δ, which is the mean of Rayleigh fading [10]. Since typically, $\Delta = 1$ [13], we ignore Rayleigh fading.

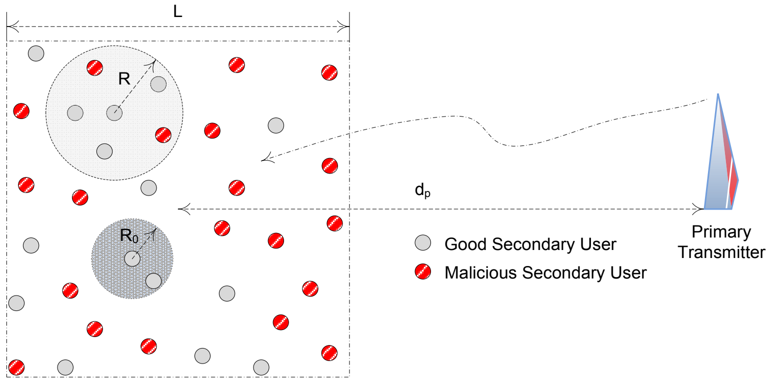


Fig. 1. A DSA consisting of good secondary users and malicious secondary users. No malicious users are present within a radius R_0 about each good user.

The received power at any good user due to primary transmission, $P_r^{(p)}$, can therefore be written as

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

Note that the distance from the primary transmitter is different for each secondary user. However, since typically $d_p >> L$, we approximate the distance between any secondary user and the primary transmitter by d_p in Eqn. (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 to its j^{th} malicious neighbor and P_m is the transmit power of the malicious user. The total received power from all N_m malicious users, $P_r^{(m)}$, is then given by

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

Typically, the power received at a secondary user from its two nearest malicious neighbors is much larger than that from all 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 compared to $(d_i^m)^{-4}$, $i = 1, 2$. Therefore, we only consider the received power at a good user from the first two malicious neighbors. Thus, $P_r^{(m)}$ can be simply approximated as

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

where $P_r^{(m_1)}$ is the received power from the nearest malicious neighbor and $P_r^{(m_2)}$ is that from the second nearest malicious neighbor, and both can be obtained from Eqn. (2).

Fig. 2 shows the comparison of received power at a good user from its two nearest malicious neighbors, and that from all other malicious neighbors, for a DSA network with an average of 500 secondary users (including good and malicious users) spatially Poisson distributed in a grid of dimensions $2000m \times 2000m$. The legend "Theoretical, 1^{st} two" represents the power received at a good user from its first two malicious neighbors, evaluated from the analysis which will be explained in Section III-B. The legend "Theoretical, all others" represents the received power at a good user from all other malicious neighbors (except the first two), obtained using the analysis that will be presented in Section III-B. The legends "Experimental, 1^{st} two" and "Experimental, all others" represent the received powers at a good user from its first two malicious neighbors and all other malicious neighbors except the first two, respectively, obtained by simulation experiments. It can be seen from Fig. 2, that the received power from the first two malicious neighbors is about two to four orders of magnitude larger than that from all other malicious neighbors, thus justifying the approximation in Eqn. (4).

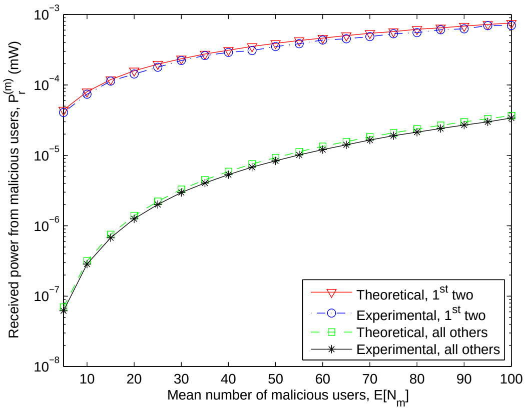


Fig. 2. Comparison of received power at good user from its two nearest malicious neighbors, and that from all other malicious neighbors. The mean number of all secondary users $E[N] = 500$.

From Eqn. (4), the total received power from its first two malicious neighbors depends on $(d_1^m)^{-4}$ and $(d_2^m)^{-4}$, which, in turn, is determined by the location of the good user and its two nearest malicious neighbors. Since all locations are randomly distributed, analytical computation of $P_r^{(m)}$ is complex. Therefore, we use $E[(d_j^m)^{-4}]$ instead of $(d_j^m)^{-4}$, $j = 1, 2$, in Eqn. (2), to simplify analysis. Since the positions of 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

$$E[(d_j^m)^{-4}] = \sum_{n=j}^{N-1} E[(d_n)^{-4}] \binom{n-1}{j-1} \left(\frac{\lambda_m}{\lambda}\right)^j \left(\frac{\lambda_g}{\lambda}\right)^{n-j}, \tag{5}$$

which is further simplified by replacing N by $E[N]$.

In Eqn. (5), $E[(d_n)^{-4}]$ is obtained as follows. Let N denote the number of all secondary users including both good and malicious users, i.e., $N = N_g + N_m$. since good users and malicious users are both spatially Poisson distributed and independent of each other, N is also spatially Poisson distributed with intensity $\lambda = \lambda_g + \lambda_m$. The probability density function (pdf) of the distance between any good user and its n^{th} neighbor, d_n, is given by ([14], Theorem 1)

$$f_n(d_n) = e^{-\lambda \pi d_n^2} \frac{2(\lambda \pi d_n^2)^n}{d_n \Gamma(n)}, \tag{6}$$

where $\Gamma(\cdot)$ is the generalized Gamma function. $E\left[(d_n)^{-4}\right]$ can be obtained from Eqn. (6) as

$$E\left[(d_n)^{-4}\right] = \int_\beta \beta^{-4} f_n(\beta) d\beta. \tag{7}$$

$P_r^{(m_j)}$ is obtained by substituting Eqn. (5) in Eqn. (2), and then $P_r^{(m)}$ can be calculated from Eqn. (3).

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

$$\mu_p = 10\log_{10}(P_t) - 20\log_{10}(d_p). \tag{8}$$

Similarly, upon replacing $(d_j^m)^{-4}$ by $E[(d_j^m)^{-4}]$, both terms on the right hand side of Eqn. (4) are also log-normally distributed. Thus, $P_r^{(m)}$ can be approximated as another log-normal random variable (RV). Extensive studies have been done in the literature to characterize the sum of log-normal random variables [15]-[22]. In this paper, we adopt the flexible log-normal sum method proposed by Xu *et al* in [22], which is explained as follows.

$P_r^{(m_1)}$ is log-normally distributed, i.e., $10\log_{10}\left(P_r^{(m_1)}\right) \sim \mathcal{N}(\mu_{m_1}, \sigma_m^2)$, where

$$\mu_{m_1} = 10\log_{10}(P_m) + 10\log_{10}\left(E[(d_1^m)^{-4}]\right). \tag{9}$$

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

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

$P_r^{(m)}$ can then be modeled as a log-normal RV, i.e., $10\log_{10}\left(P_r^{(m)}\right) \sim \mathcal{N}(\mu_M, \sigma_M^2)$. μ_M and σ_M can be numerically solved from the system of two independent equations,

$$\sum_{n=1}^{N} \frac{w_n}{\sqrt{\pi}} \exp\left[-s_m \exp\left(\frac{\sqrt{2}\sigma_M a_n + \mu_M}{\xi}\right)\right] = \prod_{i=1}^{K} \hat{\Psi}_X(s_m; \mu_{m_i}, \sigma_{m_i}),\ m = 1, 2, \tag{11}$$

where $\hat{\Psi}_X(s; \mu, \sigma)$ is given by

$$\hat{\Psi}_X(s; \mu, \sigma) = \sum_{n=1}^{N} \frac{w_n}{\sqrt{\pi}} \exp\left[-s \exp\left(\frac{\sqrt{2}\sigma a_n + \mu}{\xi}\right)\right]. \tag{12}$$

Eqn. (12) is the Gauss-Hermite series expansion of the moment generating function (MGF) of a log-normal RV X, without the remainder term. The weights, w_n, and the abscissas, a_n, are tabulated in Tbl. 25.10 in [23] for $N \leq 20$. N is the Hermite integration order, $\xi = 10/\ln 10$ is a scaling constant, and K in Eqn. (11) is the number of log-normal components in the summation. We choose $K = 2$ as shown in Eqn. (4). $N = 12$ is sufficient to accurately determine μ_M and σ_M, and the head portion of pdf is well matched when $(s_1, s_2) = (0.2, 1.0)$[2].

C. Individual Detection Mechanism

Although no policy on spectrum sensing has incorporated any counter-measure to PUEA so far, it is not recommended for good users to sense the primary transmission based only on the detection sensitivity (usually -94dBm). This is because even a small number of malicious users can transmit enough power to exceed the detection sensitivity, thus resulting in successful PUEA all the time. We propose an individual detection mechanism for secondary users first. The primary goal of the proposed mechanism is to achieve superior PUEA detection while not sacrificing the sensitivity to the return of the primary user. The proposed detection mechanism is then incorporated into the distributed spectrum decision protocol that will be proposed in Section III-D, to better mitigate PUEA.

The proposed detection mechanism is based on the assumption 3) in Section II. Since all users know d_p, they can estimate the received power from the primary transmitter, $P_r^{(p)}$, from Eqn. (1). Since $10\log_{10} P_r^{(p)} \sim \mathcal{N}(\mu_p, \sigma_p^2)$ with μ_p given by Eqn. (8), we propose to use the empirical rule of normal distribution to detect the primary user, i.e., the received power from the primary represented in decibels (dB), $P_r^{(p)}(dB)$, is most likely to satisfy $\mu_p - 3\sigma_p \leq P_r^{(p)}(dB) \leq \mu_p + 3\sigma_p$. Therefore, the probability of missing primary user (i.e., the probability that a secondary user fails to detect primary user when it is present), p_{miss}, is given by

$$\begin{aligned} p_{\text{miss}} &= 1 - \Pr\left\{\mu_p - 3\sigma_p \leq P_r^{(p)}(dB) \leq \mu_p + 3\sigma_p\right\} \\ &= 1 - Q(-3) + Q(3) \\ &= 0.002701, \end{aligned} \tag{13}$$

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

$$\begin{aligned} p_{\text{PUEA}} &= \Pr\left\{\mu_p - 3\sigma_p \leq P_r^{(m)}(dB) \leq \mu_p + 3\sigma_p\right\} \\ &= Q\left(\frac{\mu_p - 3\sigma_p - \mu_M}{\sigma_M}\right) \\ &\quad - Q\left(\frac{\mu_p + 3\sigma_p - \mu_M}{\sigma_M}\right). \end{aligned} \tag{14}$$

[2] Interested readers are referred to [22] for more details.

By employing the proposed detection mechanism based on the empirical rule, the probability of missing the primary user can be fixed to a negligibly low number while the probability of successful PUEA, $p_{\text{PUEA}} < 1$. Thus, it is more secure against PUEA, compared to the sensitivity based detection mechanism.

D. Distributed Spectrum Decision Protocol

After each individual good user makes a decision as mentioned in Section III-C, they can exchange the information with their neighbors to further mitigate PUEA. In order to develop the protocol, we assume that each user has a transmission range, R. All users that are located within a distance R from each other can exchange spectrum sensing information with each other. The flowchart for the protocol is shown in Fig. 3. The sequence of operations for the proposed protocol are as described in Algorithm 1.

Algorithm 1 The proposed distributed spectrum decision protocol (NEAT: NEighbor AssisTed spectrum decision protocol).

```
1) A good secondary user detects a signal in a licensed
   band during spectrum sensing.
2)  a) Good user uses the individual detection mechanism
       described in Section III-C, to check if the received
       signal is due to a PUEA or not. This preliminary
       result is broadcasted to all one-hop neighbors.
    b) If Step 2) a) above concludes that the received
       signal is due to an attack, STOP. Else go to Step 3).
3) The good user uses the information on individual sensing
   results from its one-hop neighbors.
    a) If ALL neighbors also claim primary transmission
       based on the proposed individual detection mech-
       anism, the good user concludes that the current
       transmission is from primary user, else
    b) The good user concludes that the current trans-
       mission is from malicious users, indicating that an
       attack is being launched.
```

IV. Security Analysis

We now present the analysis for the probability of successful PUEA and the probability of missing the primary user when deploying the protocol proposed in Algorithm 1. It is also of interest to analyze the performance of the protocol in the presence of Byzantine attacks from the malicious users. In other words, it is essential to take into account, the fact that the malicious users may not provide correct sensing results to the good secondary user of interest. This Byzantine attack could threaten the data fusion process if not dealt with carefully [24]-[26]. Hence, in addition to the assumptions listed in Section II and Section III-A, we also make the following assumptions to analyze the security performance of the protocol.

1) Malicious users coordinate between themselves and know the instances when PUEA is launched[3].

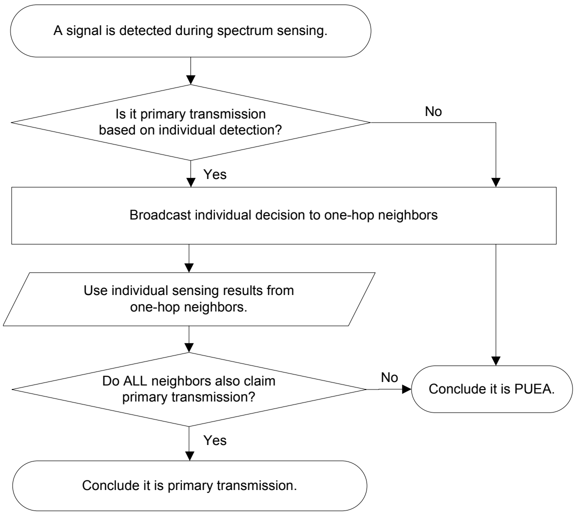

A signal is detected during spectrum sensing.
Is it primary transmission based on individual detection?
No
Yes
Broadcast individual decision to one-hop neighbors
Use individual sensing results from one-hop neighbors.
Do ALL neighbors also claim primary transmission?
No
Conclude it is PUEA.
Yes
Conclude it is primary transmission.

Fig. 3. A flowchart of the proposed distributed spectrum decision protocol.

2) When launching PUEA, malicious uses also launch a Byzantine attack with a probability, p_{lying}. That is, the attacking nodes transmit “Primary Transmission” with probability p_{lying} and “PUEA in progress” with probability $1 - p_{\text{lying}}$.
3) When primary transmitter transmits, the malicious users broadcast“Primary Transmission”, i.e., when primary transmitter transmits, $p_{\text{lying}} = 0$[4].

Let $\tilde{N}_g$ be the number of good neighbors and let $\tilde{N}_m$ be the number of malicious neighbors for a good user. It is noted that in order for a good user to become a victim of PUEA when deploying the proposed protocol, the good user must first individually conclude “Primary Transmission” when a PUEA is launched AND *all* its good neighbors must come to the same individual conclusion AND *all* its malicious neighbors must lie. Hence, if we denote by $\tilde{p}_{\text{PUEA}}^{(\text{protocol})}(\tilde{N}_g, \tilde{N}_m)$, the probability that a good user is a victim of the PUEA after implementing the protocol, conditioned on $\tilde{N}_g$ and $\tilde{N}_m$, then

$$\begin{aligned}\tilde{p}_{\text{PUEA}}^{(\text{protocol})}(\tilde{N}_g, \tilde{N}_m) \; = & \\ & \Pr\{\textit{all} \text{ good neighbors suffer PUEA without protocol}, \\ & \textit{all} \text{ malicious neighbors lie}|\text{this user becomes a victim of PUEA}\}. \quad (15)\end{aligned}$$

Applying Bayes’ rule to obtain the conditional probability, we have

$$\tilde{p}_{\text{PUEA}}^{(\text{protocol})}(\tilde{N}_g, \tilde{N}_m) = (p_{\text{PUEA}})^{\tilde{N}_g} \, (p_{\text{lying}})^{\tilde{N}_m} \, . \tag{16}$$

Averaging over $\tilde{N}_g$ and $\tilde{N}_m$, the probability of successful PUEA on a good user located at (x, y), $\hat{p}_{\text{PUEA}}^{(\text{protocol})}(x, y)$, can be obtained as

$$\begin{aligned}\hat{p}_{\text{PUEA}}^{(\text{protocol})}(x, y) \; = & \\ \sum_{m=0}^{N_m} \sum_{g=0}^{N_g - 1} \tilde{p}_{\text{PUEA}}^{(\text{protocol})}(\tilde{N}_g, \tilde{N}_m) & \Pr\{\tilde{N}_g = g\} \Pr\{\tilde{N}_m = m\}, \quad (17)\end{aligned}$$

which, from Eqn. (16) can be written as

$$\hat{p}_{\text{PUEA}}^{(\text{protocol})}(x, y) = \phi_g(p_{\text{PUEA}}) \phi_m(p_{\text{lying}}), \tag{18}$$

[3] The mechanisms by which they coordinate is beyond the scope of this paper.

[4] This is because, malicious users do not gain anything by launching Byzantine attacks when primary transmission takes place.

where $\phi_g(\cdot)$ and $\phi_m(\cdot)$ represent the moment generating functions (MGF's) of $\tilde{N}_g$ and $\tilde{N}_m$, respectively. In order to compute ϕ_g and ϕ_m, we proceed as follows. For a good user located at (x, y), let $p_n(x, y)$ denote the probability that it has a neighbor. Also let $\tilde{\lambda}_g$ and $\tilde{\lambda}_m$ be the intensities of $\tilde{N}_g$ and $\tilde{N}_m$, respectively. $\tilde{\lambda}_g$, $\tilde{\lambda}_m$ and $p_n(x, y)$ are then given by $\tilde{\lambda}_g = \lambda_g p_n(x, y)$, $\tilde{\lambda}_m = \lambda_m p_n(x, y)$ and

$$p_n(x,y) \;=\; \frac{1}{L^2}\int_{x_0=\max(0,x-R)}^{\min(L,x+R)}\int_{y_0=\max(0,y-\sqrt{R^2-(x_0-x)^2})}^{\min(L,y+\sqrt{R^2-(x_0-x)^2})} dy_0 dx_0. \quad (19)$$

The MGF, $\phi_g(z)$, can then be written as

$$\begin{aligned}\phi_g(z) &= \sum_{\tilde{N}_g=0}^{\infty} e^{-\tilde{\lambda}_g L^2 p_n(x,y)} \frac{\left(\tilde{\lambda}_g L^2 p_n(x,y)\right)^{\tilde{N}_g}}{\tilde{N}_g!} z^n \\ &= e^{\tilde{\lambda}_g L^2 p_n(x,y)(z-1)}. \end{aligned} \quad (20)$$

Similarly, $\phi_m(z)$ can be written as

$$\phi_m(z) = e^{\tilde{\lambda}_m L^2 p_n(x,y)(z-1)}. \quad (21)$$

The expressions in Eqns. (20) and (21) are used in Eqn. (18) to obtain $\hat{p}_{\text{PUEA}}^{(\text{protocol})}(x, y)$. Finally, the probability of successful PUEA after implementing the protocol, $p_{\text{PUEA}}^{(\text{protocol})}$, is obtained by averaging $\hat{p}_{\text{PUEA}}^{(\text{protocol})}(x, y)$ over x and y, i.e.,

$$p_{\text{PUEA}}^{(\text{protocol})} = \frac{1}{L^2}\int_{x=0}^{L}\int_{y=0}^{L} \hat{p}_{\text{PUEA}}^{(\text{protocol})}(x,y)dydx. \quad (22)$$

The probability of missing the primary user after implementing the protocol, $p_{\text{miss}}^{(\text{protocol})}$, is obtained as follows. Good secondary users miss detecting primary transmitter under two circumstances:

1) when the secondary user wrongly concludes the received signal to be a PUEA, OR
2) when the secondary user concludes that the received signal is a primary transmission but at least one of its neighbors wrongly concludes that the received signal is due to PUEA.

Case 1 mentioned above occurs with probability p_{miss}. For a good user located at (x, y), the probability of case 2 mentioned above conditioned on $\tilde{N}_g$ is

$$\tilde{p}_{\text{miss}}^{(\text{protocol})}(x, y, \tilde{N}_g) = 1 - (1 - p_{\text{miss}})^{\tilde{N}_g}. \quad (23)$$

Averaging $\tilde{p}_{\text{miss}}^{(\text{protocol})}(x, y, \tilde{N}_g)$ in Eqn. (23) over $\tilde{N}_g$, the probability of a good user located at (x, y) missing primary user, $\hat{p}_{\text{miss}}^{(\text{protocol})}(x, y)$ can be written as

$$\hat{p}_{\text{miss}}^{(\text{protocol})}(x, y) = 1 - \phi_g(p_{\text{miss}}), \quad (24)$$

where $\phi_g(z)$ is given by Eqn. (20). Finally, averaging over x and y, the probability of missing primary user after implementing the protocol, $p_{\text{miss}}^{(\text{protocol})}$, is obtained as

$$\begin{aligned} p_{\text{miss}}^{(\text{protocol})} &= \frac{(1-p_{\text{miss}})}{L^2}\int_{x=0}^{L}\int_{y=0}^{L} \hat{p}_{\text{miss}}^{(\text{protocol})}(x,y)dydx \\ &\quad + p_{\text{miss}}. \end{aligned} \quad (25)$$

V. Results and Discussion

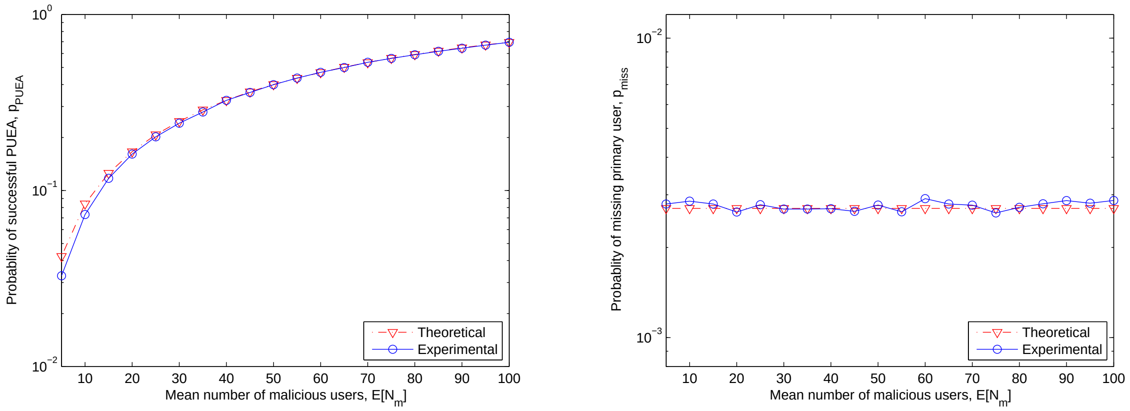
We consider the following values of the system parameters for our numerical simulations. All secondary users including both good and malicious users are spatially Poisson distributed in a $2000m \times 2000m$ square network. Each user has a transmission range, $R = 250m$ [27]. A primary transmitter (e.g., a TV tower) is located at a distance of $d_p = 100km$ from the center of the square grid, and it has a transmitting power of $P_t = 100kW$. Malicious users have transmitting power of $P_m = 4W$ [4]. The variances of shadowing loss for primary and malicious transmissions are taken as $\sigma_p = 8$ and $\sigma_m = 5.5$, since we can model primary transmission and malicious transmissions as those occurring in urban and suburban environments, respectively [13]. The exclusive distance from secondary user, R_0, is chosen as $30m$ [12]. We evaluate the performance of proposed protocol by comparing it with two other detection mechanisms, i) majority logic as data fusion technique, i.e., good users first make their own decisions based on the individual detection mechanism proposed in Section III-C and then upon receiving their neighbors' individual sensing results, take the same decision as the majority of its neighbors, and ii) individual decision based on the proposed individual detection mechanism in Section III-C only, without cooperation with neighbors.

A. Impact of Varying Attack Strength

Here, we fix the expected number of all secondary users $E[N] = 500$, while varying the expected number of malicious users $E[N_m]$ from 5 to 100 in increments of 5.

Fig. 4 presents the probability of successful PUEA (Fig. 4(a)) and the probability of missing the primary user (Fig. 4(b)) when good users make their decision based on the proposed individual detection mechanism in Section III-C. It is observed from Fig. 4(a) that the theoretical results closely follow the experimental results, thus validating the analysis presented in Sections III-B and III-C. It is noted that malicious users can successfully launch PUEA on individual good users, and the probability of successful PUEA increases with the number of malicious users. This is because the total transmitting power from a larger number of malicious users can make the received power at good users large enough and close to the expected received power from primary transmitter, thus making good users unable to distinguish the source of the received signal. Fig. 4(a) also indicates that without any further actions, DSA networks are vulnerable to PUEA, which justifies the need for additional mechanisms to mitigate PUEA.

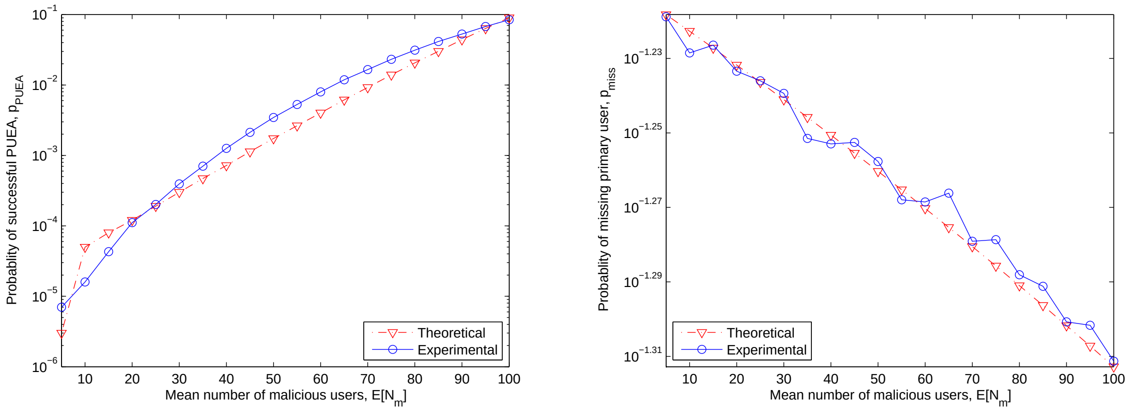
Fig. 5(a) shows the probability of successful PUEA while deploying the proposed distributed spectrum decision protocol, when in addition to launching PUEA, the malicious users also launch a Byzantine attack with probability $p_{\text{lying}} = 1$. An average of 500 secondary users are considered in the network, with the percentage of malicious users varying from $1 - 20\%$ (i.e., the average number of malicious users varies from 5 to 100 and hence, the average number of good secondary users varies from 495 to 400). It is again observed that the theoretical results closely follow the experimental results. From Fig. 5(a), it is also observed that *the probability of successful PUEA is*



(a) Probability of successful PUEA

(b) Probability of missing primary user

Fig. 4. Performance of the proposed individual detection mechanism. $p_{\text{lying}} = 1$ when malicious users launch PUEA and $p_{\text{lying}} = 0$ during primary transmission.



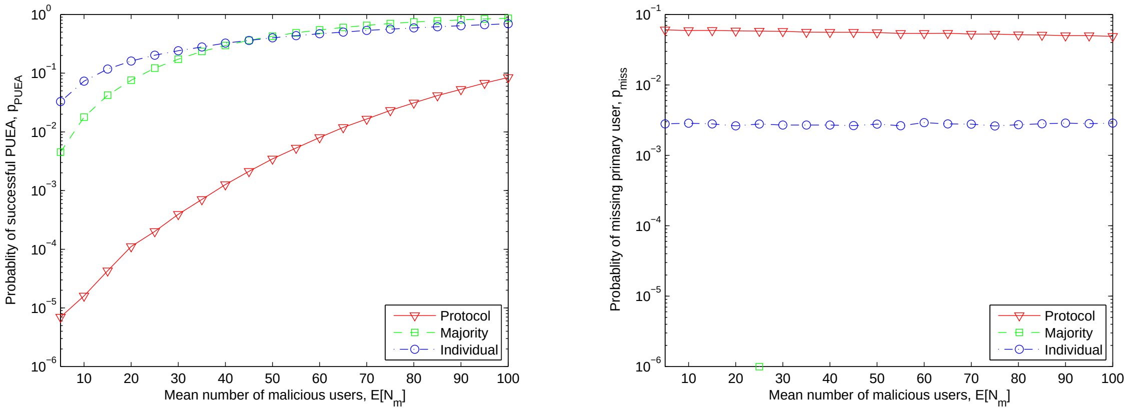
(a) Probability of successful PUEA

(b) Probability of missing primary user

Fig. 5. Performance of the proposed distributed spectrum decision protocol. $p_{\text{lying}} = 1$ when malicious users launch PUEA and $p_{\text{lying}} = 0$ during primary transmission.

reduced by one to five orders of magnitude. As an example, for $E[N_g] = 400$ and $E[N_m] = 100$, the probability of successful PUEA reduces from 0.694780 when good users make individual decision to 0.084342 when deploying the proposed protocol. Similarly, for $E[N_g] = 495$ and $E[N_m] = 5$, the probability of successful PUEA decreases from 0.032795 without the protocol to 7×10^{-6} with the protocol, which is a reduction of about five orders of magnitude. This is because, in order to launch a successful PUEA with the proposed protocol, the malicious users should launch successful PUEA, not only on a given good user but also on *all* its neighbors. This significantly reduces the probability of successful PUEA. The trade off for the protocol is that, the probability of missing primary user, p_{miss}, increases due to the protocol, as depicted in Fig. 5(b). However, it is noted that the magnitudes of the probabilities of missing primary user are still quite small (around 5%). Hence, the proposed protocol is resilient to PUEA while yet following the spectrum evacuation etiquette. Fig. 5(b) also shows that the probability of missing primary user decreases as $E[N_m]$ increases. This is because, as the average number of malicious users increases, the average number of good users decreases (since the average number of total secondary users is fixed). From Eqn. (25), it is observed that the probability $p_{\text{miss}}^{(\text{protocol})}$ is a decreasing function of $E[N_g]$. Intuitively, this is explained as follows. As the average number of good users decreases, fewer users wrongly conclude PUEA when primary transmission takes place, thus reducing the probability of the missing primary user.

We also compare the performance of the proposed protocol with another possible protocol to mitigate PUEA, namely majority logic protocol. Here, good users obtain the sensing results from all their neighbors and go with a majority vote



(a) Probability of successful PUEA

(b) Probability of missing primary user

Fig. 6. Performance of different spectrum decision mechanisms. $p_{\text{lying}} = 1$ when malicious users launch PUEA and $p_{\text{lying}} = 0$ during primary transmission.

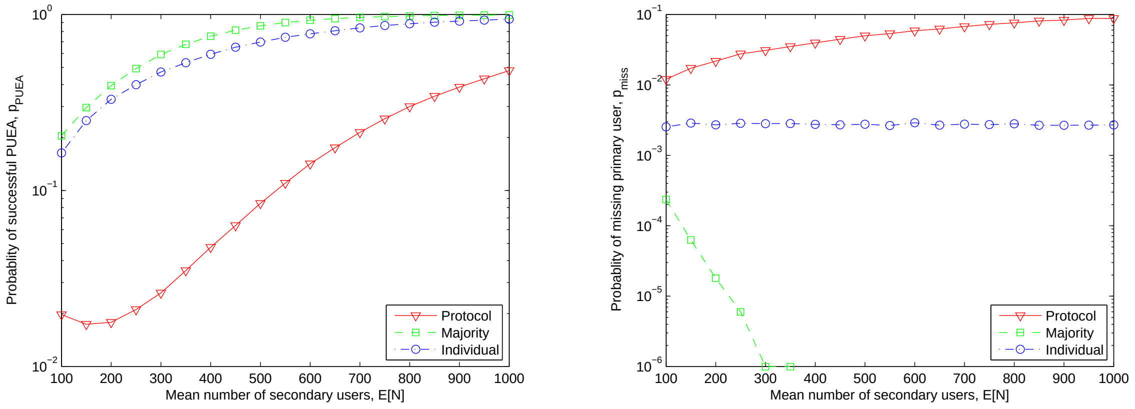
(including their own vote). Hence, for a good user with n neighbors, if more than $\frac{n+1}{2}$ neighbors conclude that the detected signal is due to primary transmission, then the good user concludes primary transmission, else it concludes PUEA. The comparison of the performance of the proposed protocol with that of the majority logic protocol is shown in Fig. 6. The case when no additional protocol is used, i.e., good users rely only on their individual decisions based on the proposed individual detection mechanism in Section III-C, is also shown. From Fig. 6(a), it is observed that the proposed protocol performs the best in terms of mitigating PUEA. The majority logic protocol performs almost the same as when no protocol is deployed. This is because, the number of neighbors that suffer PUEA is binomially distributed and the probability mass function maximizes at $\frac{n}{2}$ for a good user with n neighbors. When the probability of successful PUEA for individual good user is large (of the order of 0.4 and above), it would result in more than half of the number of neighbors easily being attacked. However, the probability that *all* neighbors are attacked is small thus resulting in an improved performance for the proposed protocol. It is observed that the proposed protocol outperforms the other two mechanisms by reducing the probability of successful PUEA by at least 90% compared to majority logic, and at least 88% compared to individual decision, even in the presence of Byzantine attacks. The majority logic performs the best in terms of missing the primary transmission though (the probability is almost zero), as observed from Fig. 6(b). However, as mentioned earlier, even with the proposed protocol the probability of missing primary user is too small to violate the spectrum evacuation etiquette.

B. Impact of Varying Secondary User Density

In this set of simulations, we fix the ratio of expected number of malicious users to that of all secondary users $E[N_m]/E[N] = 20\%$, while varying $E[N]$ from 100 to 1000. Malicious users lie with probability one when they are launching PUEA. Fig. 7 shows the performance of different mechanisms. From Fig. 7(a), it is observed that the proposed protocol lowers the probability of successful PUEA by $52\% - 96\%$, compared to the majority logic mechanism. Note that the probability of successful PUEA for the proposed protocol decreases first as $E[N]$ increases. This is because, when $E[N]$ is small, $E[N_m]$ is also small so that malicious users can not accumulate enough transmitting power to attack all good users, i.e., some good users can detect PUEA based on the proposed individual detection mechanism. Thus, it is very likely that good users have at least one disagreeing neighbor claiming PUEA even if they are not aware of ongoing attack themselves. Fig. 7(b) depicts the performance of the protocols in terms of missing the primary user. As is shown in Fig. 7(b), the majority logic protocol detects the primary transmitter best among the three. Although the proposed protocol results in higher probability of missing the primary user, all of its values are still within acceptable range, i.e., between 0.012032 and 0.087925. Thus, the values of p_{miss} are still small enough to follow the spectrum evacuation etiquette.

C. Impact of Varying Probability of Lying

In this set of simulations, we fix the expected number of all secondary users $E[N] = 500$ and also fix the expected number of malicious users $E[N_m] = 100$, while varying p_{lying} from 0.05 to 1.0. As is shown in Fig. 8, majority logic performs worst in terms of probability of successful PUEA even if malicious users lie with a small probability. Both majority logic and the proposed protocol become more vulnerable as malicious users lie with a higher probability. However, the proposed protocol can still effectively reduce the probability of successful PUEA by $90\% - 100\%$, compared to that of the majority logic protocol. The probability of missing primary user does not change because, when primary user transmits, malicious users do not lie.



(a) Probability of successful PUEA

(b) Probability of missing primary user

Fig. 7. Performance of different spectrum decision mechanisms for varying secondary user density. Malicious users form 20% of the total number of secondary users in the network.

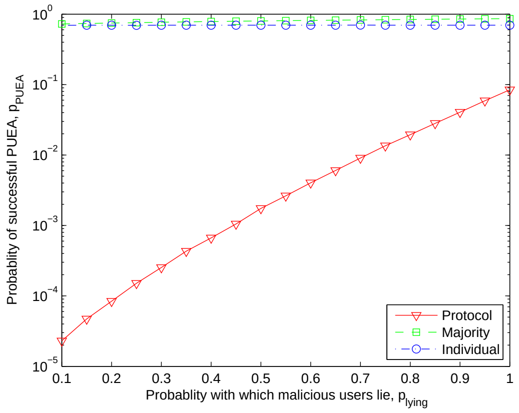


Fig. 8. Performance of different spectrum decision mechanisms for varying intensity of Byzantine attack. $E[N] = 500$ and $E\left[N_m\right] = 100$.

VI. Some Practical Considerations

We now present some practical considerations in implementing the proposed protocol. The IEEE 802.22 [4] consists of MAC protocol data units (MPDU) of two types- the generic MPDU and the bandwidth request MPDU. The bandwidth request MPDU is also used for initial network access (ranging) and to notify urgent co-existence situations (UCS). The proposed protocol requires only a single bit of information (i.e., whether a secondary user perceives PUEA or primary transmission). This bit can easily be included in the bandwidth request header. This is possible even if the DSA network deploys the IEEE 802.16 [28] mesh or the IEEE 802.11 [29] distributed co-ordination function (DCF) MAC protocols. When operating in the ad-hoc/mesh mode, users exchange beacons with each other to learn about their one-hop neighbors and to synchronize their timing information. The beacons are exchanged in every super-frame. Thus it only requires one super-frame for users to obtain the information about PUEA from their one-hop neighbors. Hence, the proposed protocol can also be implemented in real-time.

Fig. 8 indicates that the malicious users are likely to be most successful in launching PUEA when a Byzantine attack is also launched with probability of lying, $p_{\text{lying}} = 1$. Thus, the malicious users should always indicate primary transmission whenever there is PUEA. Note that malicious users do not lie when primary transmission takes place. Hence, they always indicate primary transmission irrespective of whether there is PUEA or not. The good users can then exploit this by isolating the malicious users as those device IDs which always indicate primary transmission. In order to avoid being isolated, malicious users should launch Byzantine attacks with probability $p_{\text{lying}} < 1$. However, values of $p_{\text{lying}} < 0.5$ result in low probability of successful PUEA. Values of p_{lying} close to one enable good users to isolate malicious users. Thus, malicious users should launch Byzantine attacks with p_{lying} close to 0.5. At this probability, the proposed protocol gives three orders of magnitude of improvement in reducing the probability of successful PUEA, compared to the majority logic protocol.

VII. Conclusion and Future Work

We presented a distributed spectrum decision protocol resilient to PUEA in DSA networks. We first characterized the received power at any good secondary user using a flexible log-normal sum approximation and used this to propose an individual detection mechanism. We then used the decisions made by individual secondary users to develop a distributed spectrum decision protocol that is resilient to PUEA combined with Byzantine attacks. We presented a security analysis of the proposed protocol. Compared to the majority logic protocol, the proposed protocol was found to reduce the probability of successful PUEA by $52\% - 100\%$ in the presence of Byzantine attacks while still following the spectrum evacuation etiquette. Some practical considerations were also presented for the implementation of the proposed protocol.

The impact of the proposed protocol on the network performance parameters is a topic for further study. The analysis of the protocol when malicious users are not aware of PUEA launched by others and also perform individual spectrum sensing, is also under investigation.

References

[1] P. Kolodzy, "Spectrum policy task force: findings and recommendations," *Proceedings, International Symposium on Advanced Radio Technologies (ISART'2003)*, Mar. 2003.

[2] M. McHenry, "Report on spectrum occupancy measurements," *Shared Spectrum Company,*. [Online]. Available: http://www.sharedspectrum.com/?section=nsf_summary.

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

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

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

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

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

[8] R. Chen and J. M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," *Proceedings, IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, pp. 110–119, Sep. 2006.

[9] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications: Special Issue on Cognitive Radio Theory and Applications*, vol. 26, no. 1, pp. 25–37, Jan. 2008.

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

[11] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," *Proceedings, IEEE International Conference on Communications (ICC'2009)*, Jun. 2009.

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

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

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

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

[16] J. I. Naus, "The distribution of the logarithm of the sum of two lognormal variates," *Journal of the American Statistical Association*, vol. 64, pp. 655–659, Jun. 1969.

[17] W. A. Janos, "Tail of the distributions of sums of lognormal variates," *IEEE Transactions on Information Theory*, vol. 16, no. 3, pp. 299–302, May 1970.

[18] D. Schleher, "Generalized gram-charlier series with application to the sum of lognormal variates," *IEEE Transactions on Information Theory*, vol. 23, no. 2, pp. 275–280, Mar. 1977.

[19] S. C. Schwartz and Y. S. Yeh, "On the distribution function and moments of power sums with lognormal components," *Bell System Technical Journal*, vol. 61, pp. 1441–1462, Sep. 1982.

[20] N. C. Beaulieu, W. L. Hopkins, and P. J. Mclane, "Interception of frequency hopped spread spectrum signals," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 5, pp. 853–870, Jun. 1990.

[21] N. C. Beaulieu, A. A. Abu-Dayya, and P. J. McLane, "Comparison of methods of computing lognormal sum distributions and outages for digital wireless applications," *Proceedings, IEEE International Conference on Communications (ICC'1994)*, vol. 3, pp. 1270–1275, May 1994.

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

[23] M. Abramowitz and I. Stegun, *Handbook of mathematical functions with formulas, graphs and mathematical tables*, 9th ed. Dover, 1972.

[24] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[25] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attack in large wireless sensor networks," *Proceedings, IEEE Military Communications Conference (MILCOM'2006)*, Oct. 2006.

[26] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," *Proceedings, IEEE International Conference on Commununications (ICC'2008)*, pp. 3406–3410, May 2008.

[27] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," *Proceedings, IEEE Conference on Computer Communications (INFOCOM'2008)*, pp. 1876–1884, Apr. 2008.

[28] "IEEE P802.16-Revd/D3-2004: Draft amendment to IEEE standard for local and metropolitan area networks c Part 16e: Air interface for mobile wireless access systems c Medium access control (MAC)modifications and additional physical-layer (PHY) specifications for 2c11 GHz," Jan. 2004.

[29] "IEEE standards for wireless LAN medium access control (MAC) and physical layer (PHY) specifications, p802.11," Nov. 1997.