Mitigating Primary User Emulation Attacks Using Analytical Model

Ishu Gupta and O. P. Sahu

Abstract Cognitive radio has been a widely studied area to increase the efficiency of the spectrum. Most of the present work focuses on sensing techniques but very less work has been done for security in Cognitive Radio Networks (CRNs). Primary User Emulation Attack (PUEA) is a very prominent Denial of Service (DoS) attack that degrades the performance of the network to a large extent. This paper deals with an analytical model which depends on Neyman–Pearson Composite Hypothesis Test (NPCHT) to determine whether a PUEA is present in CRN. Log-normal shadowing and Rayleigh fading have been taken for the signals received from the primary transmitters as well as the attackers. The movement of good secondary user has been assumed in vertical direction ranging from an angle of $(-\pi/4)$ to $(\pi/4)$ with respect to primary transmitter. The performance of the system model has been evaluated by plotting the Receiver Operating Characteristic (ROC) curve. Variation in miss detection and false alarm probabilities has been studied for different angles. Results demonstrate that the likelihood of successful PUEA increments with the increasing distance between the good secondary user and primary transmitter.

Keywords Dynamic spectrum access · Cognitive radio · Primary user emulation attacks · Probability of false alarm · Probability of miss detection

1 Introduction

With increasing use of the multimedia applications, the demand for spectrum is continuously increasing. However, the spectrum available is very limited as well as costly. Hence, there is a need to utilize the spectrum very judiciously. The presently adopted

I. Gupta (✉) · O. P. Sahu
Department of Electronics and Communication Engineering, National Institute of Technology, Kurukshetra, Kurukshetra 136119, Haryana, India
e-mail: ishugupta2203@gmail.com

O. P. Sahu
e-mail: ops_nitk@yahoo.co.in

K. Ray et al. (eds.), *Engineering Vibration, Communication and Information Processing*, Lecture Notes in Electrical Engineering 478,
https://doi.org/10.1007/978-981-13-1642-5_20

Static Spectrum Allocation (SSA) policy leads to underutilization of spectrum [1]. J. Mitola suggested the Dynamic Spectrum Allocation (DSA) method to solve this problem [2]. Later, quantification of Mitola's work was done by Haykin [3]. Cognitive radio is a technology that is widely studied nowadays and can possibly eliminate the SSA problem in future. Spectrum sensing is a very crucial task to practically implement this technology. Various spectrum sensing methods have been discussed in [4]. Among all, energy detection has been widely adopted and accepted method for sensing of spectrum, because it does not require any prior knowledge regarding the features of the primary signal and is computationally simple to implement [5]. Most of the present work in Cognitive Radio Technology focuses on spectrum sensing and its optimization. However, for successful implementation for any technology, its security aspects need to be taken into account. A comprehensive survey on different security attacks and their detection has been presented in [6]. This paper focuses on one such Denial of Service (DoS) attack named Primary User Emulation Attack (PUEA) [7]. In such an attack, an adversary tries to imitate the characteristics of primary user so as to fool the good secondary user regarding the usage of channel. The good secondary user believing that channel is being used by the Primary User leaves the spectrum and hence making the use of DSA method trivial. The malicious users can use the channel for their own purpose. Various studies have been conducted on detection and elimination of this attack. The impact of PUEA on Cognitive Radio Networks has been studied in [8]. PUEA can be classified into two types—always on and smart [9]. Always on PUE attacks emulate the primary signal anytime without taking into account whether the primary signal is transmitting or not whereas smart PUE attackers take into account the transmission characteristics of primary signal. The impact of smart PUE attackers is more severe than always on PUE attackers. This paper focuses on always on PUEA.

This paper presents an analytical model for PUEA in which secondary users are assumed to move in a vertical direction. Effect on the probability of miss detection and false alarm has been considered for varying distances between real secondary user and primary user. The first analytical model was presented in [10], where the use of Markov inequality and Fenton's approximation was done so as to get a lower limit for the likelihood of successful PUEA. In [11], WSPRT is used for detection of PUEA by first formulating the probability density function (pdf) for the received power at the good secondary user from the malicious users. Jin et al. [12] compares the Wald's Sequential Probability Ratio test (WSPRT) and NPCHT for identification of PUEA using the same analytical model. It was found that WSPRT offers less likelihood of successful PUEA as compared to NPCHT because it allows two thresholds for both probability of false alarm and miss detection. This paper presents a similar model using NPCHT with the difference being that the good secondary user is allowed to move in a vertical direction that allows the study of probability of false alarm as well as miss detection with changing distance between the real secondary user and primary user. The simulated results match with the theoretical results that probability of successful PUEA increases with increasing distance between primary transmitter and the good secondary user.

The rest of the paper is structured as follows. Section 2 discusses the system model. Section 3 presents the analytical model. Section 4 describes the NPCHT approach for detecting PUEA. Results are analyzed in Sect. 5. Conclusion is provided in Sect. 6.

2 System Model

The system model in this paper has one secondary user surrounded by different randomly located malicious users in circular grid around it as given in Fig. 1 [11]. Let the radius of the circular grid be R. One primary transmitter is fixed at a distance greater than or equal to D_p from all the other users. The distance $D_p \gg R$. Energy-based detection technique has been used for detection of PUEA. If the power received at the secondary user exceeds a certain threshold say Λ, then the primary transmission is assumed else malicious transmission is assumed.

Two hypotheses have been taken as null and alternative hypothesis given as follows:

H0: Primary User Transmission. This includes the case when only primary user is transmitting the signal.
H1: Malicious User Transmission. This hypothesis considers the case when malicious and good secondary users are simultaneously transmitting the signal.

Following assumptions have been made for doing analytical study of the system model:

- Total M malicious users along with one good secondary user are present in the CRN.
- Minimum distance of primary transmitter from all other users should be $D_{p.}$
- The primary transmitter power is taken to be $P_{t.}$
- Power of each malicious user is taken to be P_m where $P_m \ll P_t$.

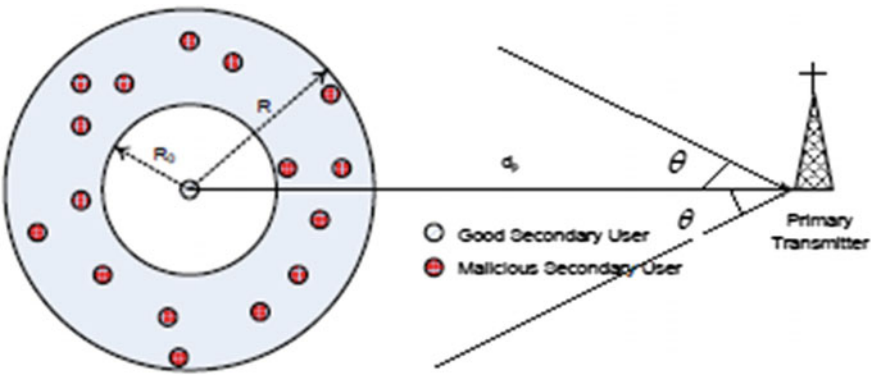

Fig. 1 Typical cognitive radio scenario

- The adversaries are uniformly distributed in a circular region around the good secondary user and their positions are independent to each other.
- The position of primary transmitter is fixed whereas the movement of secondary user is restricted in a vertical direction.
- The position of primary transmitter is known to the good secondary user and the adversaries.
- The incoming signals received from both the primary transmitter as well as malicious users undergo log-normal shadowing, path loss and Rayleigh fading.
- The mean, Δ of the Rayleigh random variable is assumed to be unity.
- The exponent for path loss is assumed to be 2 for propagation from primary transmitter and 4 from malicious users.
- There is an excluded distance R_0 from the good secondary user where there is no malicious user. Such condition is required since if there would be any malicious user present in this region, then the power received from the malicious users will be always higher than the power received from primary transmitter leading to successful PUEA every time.

3 Analytical Model

First of all, the probability density function (pdf) of the signal is analyzed. It is assumed that the good secondary user is fixed at origin (0, 0). It is also assumed that the motion of SU is restricted in a vertical direction ranging from a minimum angle of $-\pi/4$ to maximum angle of $\pi/4$ from primary transmitter. Since $Dp \gg R$, coordinates of primary transmitter can be assumed to be same for all the malicious SUs.

Let the coordinates of the M malicious users be (r_j, Θ_j), where $1 \leq j \leq M$. The pdf of r_j is taken as

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

Θ_j is taken as uniformly distributed in the range $(-\pi, \pi)$.

The power transmitted from primary transmitter to the SU can be taken as

$$P_r^{(p)} = P_t G_p^2 \left(\frac{d_p}{\cos(\theta)} \right)^{-2} \tag{2}$$

where $G_p^2 = 10^{\frac{\xi_p}{10}}$ and $\xi_p \sim N(0, \sigma_p^2)$. The corresponding pdf $p^{(P_r)}(\gamma)$ can be defined as log normal distribution which can be written as follows:

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

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

$$\mu_p = 10\log_{10} P_t - 20\log_{10}\left(\frac{d_p}{\cos(\theta)}\right) \tag{4}$$

Since different malicious users are not dependent on each other, their power can be added which can be taken as

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

where G_j^2 is the shadowing between the SUs and jth MU. $G_j^2 = 10^{\frac{\xi_j}{10}}$ and $\xi_j \sim \mathrm{N}\left(0, \sigma_m^2\right)$. All the variables in above equation are log-normally distributed of the form $10^{\frac{\omega_j}{10}}$ and $\omega_j \sim \mathrm{N}\left(\mu_j, \sigma_m^2\right)$. Here

$$\mu_j = 10\log_{10} P_m - 40\log_{10}\left(d_j\right) \tag{6}$$

By approximating the pdf from different malicious users using Fenton's approximation, pdf $p^{(m)}(\chi)$ can be given as

$$p^{(m)}(\chi) = \frac{1}{A\sqrt{2\pi}\sigma_\chi\chi} \exp\left\{\frac{-\left(10\log_{10}\chi - \mu_\chi\right)^2}{2\sigma_\chi^2}\right\} \tag{7}$$

The received power $P_r^{(m)}$ is assumed to be log-normally distributed random given by above equation. Here, μ_χ and σ_χ^2 can be taken as

$$\mu_\chi = \frac{1}{A}\ln\left[\frac{E^2\left[P_r^{(m)}\right]}{\left(\mathrm{var}\left(P_r^{(m)}\right) + E^2\left[P_r^{(m)}\right]\right)^2}\right] \tag{8}$$

$$\sigma_\chi^2 = \frac{1}{A^2}\ln\left[\frac{\mathrm{var}\left(P_r^{(m)}\right) + E^2\left[P_r^{(m)}\right]}{E^2\left[P_r^{(m)}\right]}\right] \tag{9}$$

The values of μ_χ and σ_χ^2 can be substituted in Eq. (7) to get the pdf for the malicious users. Further, the error probabilities, i.e., the probability of miss detection and false alarm can be analyzed by applying Neyman–Pearson criterion as defined in the following section.

4 Neyman–Pearson Criterion for Detection of Puea

In Neyman–Pearson criterion, to take any decision, two hypothesis are assumed which can be defined as follows:

H0: Primary User transmission (Null hypothesis).

H1: Malicious User transmission (Alternative hypothesis).

Any secondary user can undergo two types of errors during sensing of the channel, namely:

- Miss detection: This case corresponds to when the PU is actually transmitting the signal but the SU believes that it to be sent by the malicious user. The probability of detection, P_d is defined as (1-P_m), where P_m is the likelihood of miss detection.
- False alarm: This error corresponds to case when the signal is transmitted by the MU but the good SU assumes the signal to be transmitted by the PU. This leads to interference to the PU and thus PU may impose a penalty to the good SU for further usage of the channel.

The Neyman–Pearson criterion aims at reducing the possibility of successful PUEA assuming a fixed false alarm probability say, α. The condition of fixed false alarm probability has to be imposed because both the error probabilities, i.e., miss detection and false alarm cannot be reduced simultaneously [13]. The ratio of two pdfs is taken and compared with a certain threshold, say Λ, which is taken as

$$\Lambda = \frac{p^{(m)}(x)}{p^{(P_r)}(x)} \tag{10}$$

where x can be taken as the measured power of the signal at SU. The final decision is based on criterion given as follows:

$$\Lambda \begin{cases} \leq \lambda & \text{D1: Primary Transmission} \\ \geq \lambda & \text{D2: Malicious User Transmission} \end{cases} \tag{11}$$

where λ can be obtained by a constraint on probability of miss detection $\Pr\left\{\frac{D2}{H0}\right\}$ which is fixed at a certain value α given by the following expression:

$$\Pr\left\{\frac{D2}{H0}\right\} = \int_{\Lambda \geq \lambda} p^{(P_r)}(x)dx = \alpha \tag{12}$$

Hence, Neyman–Pearson criterion aims at reducing the error probabilities while keeping a constraint as shown in the above equation.

5 Results and Discussion

The proposed work in this paper is simulated by assuming the following system parameters (Table 1).

The simulation is performed for 10,000 times. The performance of the model is illustrated by plotting probability of miss detection verses that of false alarm in Fig. 2. Plot of probability of detection versus that of false alarm, also called ROC is shown in Fig. 3. Finally, variation of probability of false alarm as well as miss detection verses Θ can be analyzed in Fig. 4. The results in Fig. 2 are concordant with the theoretical results that both the errors probabilities cannot be reduced simultaneously and the mean probability of both false alarm as well as miss detection is found to be nearly varying from 0.01 to 0.05.

Similarly, the plot for Receiver Operating Characteristics (ROC) [13], which is generally used as another way for detection of a detector is shown in Fig. 3 and the mean P_d is found to be varying around 0.95–0.99.

Figures 4 and 5 demonstrate how the probability of false alarm and miss detection, respectively, varies with varying angles of the secondary user with the primary transmitter. Change in angles leads to change in distances between primary transmitter and real secondary user and thus, the error probabilities are minimum for $\Theta = 0°$ and maximum for $\Theta = -45°$ and $+45°$. Hence, as the distance between primary transmitter and secondary user increases, the likelihood of false alarm increases and vice versa.

Table 1 System parameters used for simulation

Parameter	σ_p (dB)	σ_m (dB)	D_p (km)	R (m)	R_0 (m)	P_t (kW)	P_m (W)	M	Θ	Δ
Value	8	5.5	100	500	30	100	4	15	$(-\pi/4)$: $(\pi/2048)$: $(\pi/4)$	1

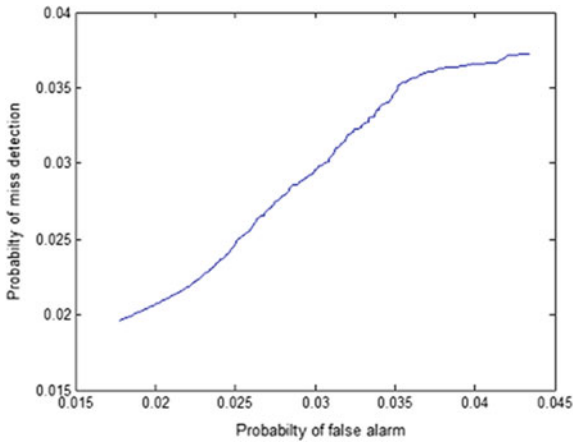

Fig. 2 Probability of miss detection versus false alarm

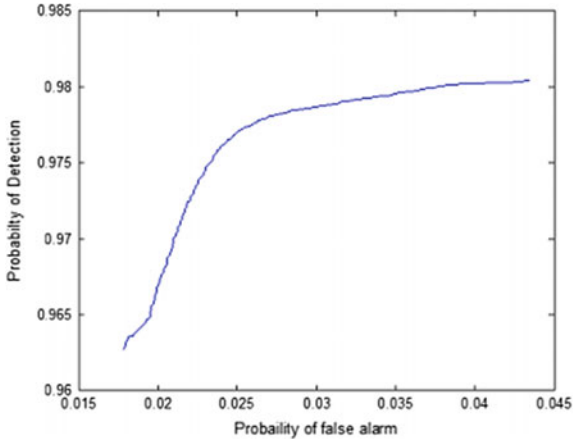

Fig. 3 Probability of detection versus false alarm

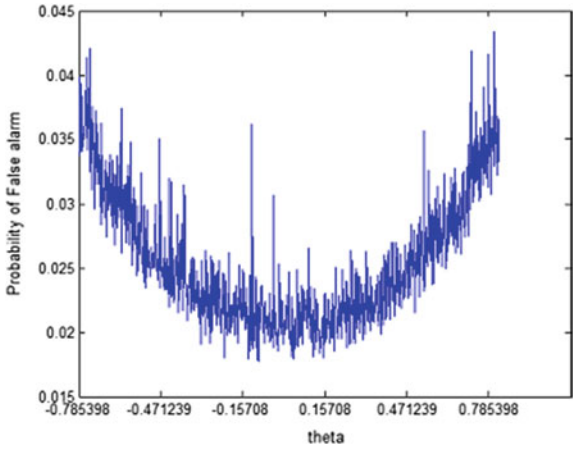

Fig. 4 Probability of false alarm versus angle, ϴ

6 Conclusion

An analytical model for the practical Cognitive Radio Network has been proposed based on Neyman–Pearson criterion and effects on probability of false alarm as well as miss detection has been studied with varying distances between primary transmitter and good secondary user. Movement of secondary user is assumed in a vertical direction ranging from an angle of $-\pi/4$ to $\pi/4$ with the primary transmitter. The simulated results show that error probabilities increments with the increasing distances between primary transmitter and the secondary user. Future work can be based on variable malicious users' power. Other analytical models can be developed that deals with other distributions apart from uniform distributions. Also, different techniques need to be developed that focuses on smart PUE attackers.

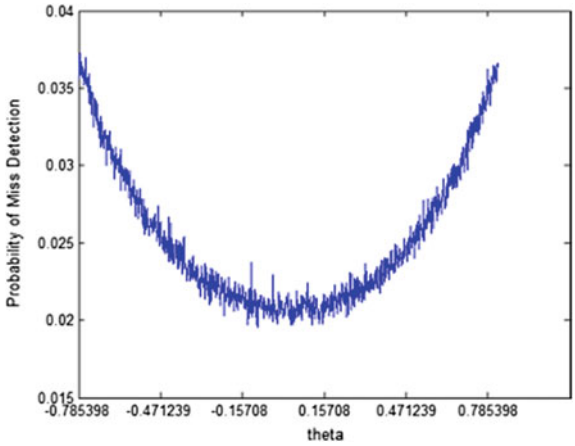

Fig. 5 Probability of miss detection versus angle, ϴ

References

1. Force, S.: Spectrum policy task force report. Federal Commun. Comm. ET Docket 02, **135** (2002)
2. Mitola, J., Gerald, Q.: Maguire.: cognitive radio: making software radios more personal. IEEE Pers. Commun. **6**(4), 13–18 (1999)
3. Haykin, S.: Cognitive radio: brain-empowered wireless communications. IEEE J. Sel. Areas Commun. **23**(2), 201–220 (2005)
4. Yucek, T., Arslan, H.: A survey of spectrum sensing algorithms for cognitive radio applications. IEEE Commun. Surv. Tutor. **11**(1), 116–130 (2009)
5. Umar, R., Sheikh, A.U.H.: A comparative study of spectrum awareness techniques for cognitive radio oriented wireless networks. Phys. Commun. **9**, 148–170 (2013)
6. Fragkiadakis, A.G., Tragos, E.Z., Askoxylakis, I.G.: A survey on security threats and detection techniques in cognitive radio networks. IEEE Commun. Surv. Tutor. **15**(1), 428–445 (2013)
7. Chen, R., Park, J.M., Reed, J.H..: Defense against primary user emulation attacks in cognitive radio networks. IEEE J. Sel. Areas Commun. **26**(1) (2008)
8. Jin, Z., Anand, S., Subbalakshmi, K.P.: Impact of primary user emulation attacks on dynamic spectrum access networks. IEEE Trans. Commun. **60**(9), 2635–2643 (2012)
9. Shrivastava, S.: Security Issues in Cognitive Radios. Diss (2017)
10. Anand, S., Jin, Z., Subbalakshmi, K.P.: An analytical model for primary user emulation attacks in cognitive radio networks. In: 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008. IEEE (2008)
11. Jin, Z., Anand, S., Subbalakshmi, K.P.: Detecting primary user emulation attacks in dynamic spectrum access networks. In: IEEE International Conference on Communications, ICC'09. IEEE (2009)
12. Jin, Z., Anand, S., Subbalakshmi, K.P.: Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing. ACM SIGMOBILE Mob. Comput. Commun. Rev. **13**(2), 74–85 (2009)
13. Kay, S.M.: Fundamentals of Statistical Signal Processing, Volume 2: Detection Theory, Series. Prentice Hall Signal Processing Series, AV Oppenheim, Ed. Prentice Hall PTR (1998)