Analytical Model for Mitigating Primary User Emulation Attack using Hypothesis Testing in Cognitive Radio Networks

Dr. Mahesh Kumar N.[1], Dr. Purushotham U.[2]

[1] Assistant Professor, Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering. Bangalore, Karnataka, India.

[2] Associate Professor, Department of Electronics and Communication Engineering, PES University, Bangalore, Karnataka, India.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: The Cognitive Radio (CR) is the key technology to deal with spectrum scarcity by allowing unlicensed CR users to coexist with existing users in licensed spectrum bands without interfering with binding communications. Cognitive technology provides the spectrum ability to be shared with licensed networks. This radio system can adjust its transmitter and recipient parameters on the basis of interaction with the current conditions in the environment. Due to this flexibility cognitive radios are exploring different types of threats and security attacks. In this paper, we focus primarily on the Primary User Emulation Attack (PUEA) which is a major attack in the cognitive radio network. PUEA is similar to a Denial-of-service attack that can seriously disrupt the spectrum sensing process and deny other legitimate secondary users to access the available spectrum. We proposed a Neyman-Pearson composite hypothesis test (NPCHT) based analytical model to study the impact of PUEA in a fading wireless communication environment. Simulation results show that the proposed techniques can substantially reduce the impact of the malicious attack on the network.

Keywords: Cognitive Radio Network, Primary User Emulation Attack (PUEA), Primary Exclusive Region, Probability Density Function (PDF), Neyman-Pearson composite hypothesis test (NPCHT).

1. Introduction

Recent advances in wireless communication have contributed to the challenge of rising spectrum scarcity. Owing to the growing demand for new mobile technologies, the allocated frequency bandwidth has become increasingly scarce. A significant amount of available frequency spectrum has been used occasionally, causing underutilization of the spectrum. Cognitive Radio technology offers a potential approach to the problems of spectrum scarcity in wireless networks (Mitola, 1999). The CR network facilitates the effective use of the limited frequency range. Licensed users or primary users are classified in cognitive radio jargon as user with a right to use the spectrum band, whereas non-licensed and secondary users are identified as users who can use a spectrum for the moment not used by authorized users without interruption. Around the same time, more attention is paid to the safety issues of cognitive radio as the intrinsic properties of CR networks present new challenges for wireless communications.

In this paper work, we mainly concerted the physical layer attack that is primary user emulation (PUE) attack, which is a sever attack and can degrade the performance of the CR network. In a CR network, the authorized user is being referred to as the primary user (PU) to have the highest priority over unauthorized users, which are being called as secondary the users (SU) for utilizing the band of frequencies. Hence, some of the secondary users are taking advantage of this opportunity by imitating as the authorized user characteristics, to utilize a frequency band with priority over other users (Chen *et.al.*, 2008)-(Rajesh Sharma *et.al.*, 2015). This scenario is referred as PUEA, which is pictorially illustrated in the figure 1.

One of the most extreme attacks is a primary user emulation attack (PUEA), whose objective focuses on the layers of physical CR and MAC. In this attack the malicious node deludes other secondary users by mimicking the transmission features of the incumbent user (PU). It produces a negative threat to the incumbent user, and thwarts other secondary users' use of idle frequency bands. Furthermore, the emulation of the incumbent user signal in multiple channels extends the SU handoff, leading to reduced network performance (Chen *et.al.*, 2008)-(Marinho *et.al.*, 2015). The malicious user (PUE attacker) mimic as a PU and other legitimate SUs considered, this as incumbent primary user. Then they send false statistics to the Fusion Centre, these can increase the probability of false detection.

The rest of the paper is organized as follows: In section II, we gave the comprehensive study of the literature survey. In the section III, we present the system model and all assumptions made to formulate the problem and

derive an analytical model of the problem, the PDF of received signal and also use the Neyman-Pearson's Composite Hypothesis Test for investigation. In Section IV presented the simulation results followed by conclusion and future work in section V.

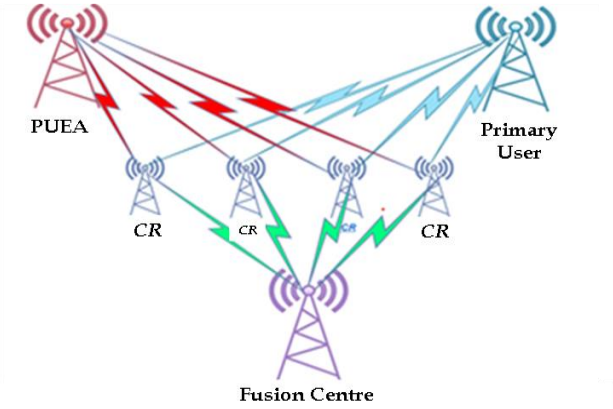

Figure 1. PUE Attack

Ruilang Chen *et.al.* (2016), authors proposed a transmitter verification technique using DRT and DDT. These methods employ a position verification scheme to differentiate licensed users and malicious user transmitters. Lianfen Huang *et.al.* (2010), they proposed joint position verification method is proposed to enhance the positioning accuracy using TDoA and FDoA methods. The combination of energy detection technique and localization technique using TDoA proposed by authors Fan Jin *et.al.* (2015), in this work, the authors used multiple thresholds for each secondary user to detect a PUE attack. A. Alahmadi *et.al.* (2013), in this work the authors used a reliable Advanced Encryption Standard (AES) DTV technique for mitigating PUE attack. In this method, they used symmetric-key techniques between transmitters and receivers.

The authors led by N. Goergen *et.al.* (2010) presented a watermarking technique to prevent PUE attacks by using applying watermark signals at the physical layer in CRN. In the method suggested by Z. Yuan *et.al.* (2012), each secondary user must compute the local function and compatibility function, calculate the message, exchange messages and measure belief to the neighboring user before convergence takes place. The PUE attacker is then detected and the features of the attacker's signal are transmitted to all secondary users on the network. Mahesh Kumar N. *et.al.* (2020), proposed a spectrum sensing techniques based on Energy detection, Matched filter and feature detection methods to detect the PUEA.

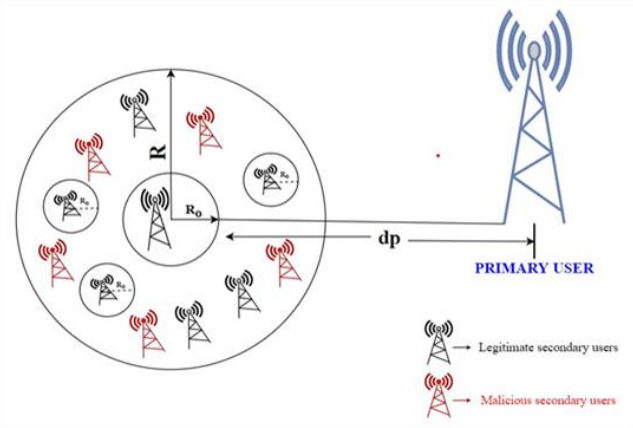

Figure 2. Simple System model of CR Networks in Circular grid fashion of R radius and consists legitimate SU and malicious SUs.

An analytical approach based on Fenton's approximation and Markov's inequality was discussed in the study by S. Anand, *et.al.* (2008), the feasibility of PUEA in CRNs for the fading Wireless environment. This was used to create a lower limit on the probability of productive PUEA. Jin, Anand & Subbulakshmi (2009) devised some composite hypothesis checks based on Neyman-Pearson and sequence likelihood ratio check Wald's were used for the identification of PUEA. In order to calculate the power and density function of probability, the Neyman-

Pearsons composite hypothesis test was used to study PUEA's impact on the network in the article by Z. Jin, *et.al.* (2014). Mahesh Kumar N. *et.al.* (2020), proposed a detection approach based on transmitter location and modulation technique using Received Signal Strength and cyclostationary feature detection. In this work, we proposed a Neyman-Pearsons Composite Hypothesis Test based mathematical model to study the effect of PUEA on the CRNs.

3.1 Probability Density Function of the Received Signal

1. There is no coordination or cooperation between each secondary user in the network. Each secondary user can independently analyze the presence of malicious users. The effect of PUE attack is equal to all the user in the network.
2. There are Mu malicious users who are geometrically distributed with a mean E_m in the network.
3. All the SUs in the network are apart of d_p distance from the primary users.
4. Both secondary users and MUs are uniformly distributed in the circular gird fashion of radius R, as illustrated in Fig. 2.
5. Each secondary user origin at the axis (r_0, θ_0) of a radius R_0 termed as an exclusive range from the SU. There is no malicious users are present within this radius.
6. All the users in the network have prior knowledge of the primary user transmitter location.
7. The PU transmits with high power denoted as P_t and malicious user power is denoted as P_m. we consider $\boldsymbol{P_t >> P_m}$ and $\boldsymbol{d_p >> R}$.
8. Considered the path loss and log-normal shadow effects (in dB) between transmitter and receiver while traversing the signal. The shadow effect is considered at the SU from the primary user with mean zero and variance σ^2_p and from a malicious user with mean zero and variance σ^2_m. We assumed that the path loss component from the primary user is 2 and from a malicious user is 4. The power density function (PDF) is considered as log-normally distribution values.
9. The effect of PUE attack is identical to all the user in the network because there is no communication between the SUs. We assume that the secondary user lies at the origin (x , y coordinates are 0 , 0) and primary user coordinates are (d_p, θ_p). The position of the primary user will differs at each secondary users.
10. We analyze the Probability density function (PDF) of the received signal at any one SU in the network.

In order to find a hypothesis test using Neyman-Pearson criteria, it is vital to obtain the probability density function of the received signal at the SU due to broadcast by the PU and MUs. We considered M malicious users located at origin (r_j, θ_j) where M is randomly distributed variable and $M \geq j \geq 1$. Then the probability of mass function of M is given by

$$P_r\{M = k\} = (1-P)^{k-1} p; \quad k = 1, 2, 3, ... \tag{1}$$

where $p = 1/E_m$. Each malicious users are uniformly scattered in the angular region within R_0 and R. Hence r_j and θ_j are coordinates of the j^{th} malicious user. The probability density function of r_j, $p(r_j)$ is given by equation (2) as

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

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

The received power at the SU from the PU transmitter $P_r^{(p)}$ is expressed by the Eqn. (3) as

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

where G_p^2 is gain of the primary transmitter = $10^{\frac{\xi_p}{10}}$ & $\xi_p \sim N\left(0,\sigma_p^2\right)$ & $p^{(pr)}(\gamma)$ can be expressed using Eqn. (4) as

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

where γ is RV (Random variable) and $A=\frac{\ln(10)}{10}$. The mean of the primary user is modelled by the Eqn. (5) as

$$\mu_p=10\log_{10}\left(P\right)_t-20\log_{10}\left(d_p\right) \tag{5}$$

Then the total received power at the SU from all malicious user (MU) is expressed as Eqn. (6) as,

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

where d_j and $G_j^2=10^{\varepsilon_j/10}$ are the distance and shadowing between the j^{th} MU and the legitimate SU respectively.

$$\mu_j=10\log_{10}\left(P_m\right)-40\log_{10}\left(d_j\right) \tag{7}$$

$P_r^{(m)}$ can be estimated as normally log distributed variable and mean and variance can be expressed by using Fenton's approach. The conditional probability (probability density function of $P_r^{(m)}$) of the location of all malicious user can be expressed by the equation (8) as

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

where r is the vector with elements $r_1, r_2, \ldots\ldots, r_M$ and $\hat{\mu}_M$ and $\hat{\sigma}_M^2$ are expressed as equations (9) and (10) as

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

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

The probability density function of the received power from all M malicious users, $p^{(m)}(x)$, can be achieved by averaging Eq. (8) over $r_1, r_2, \ldots\ldots, r_M$ and is written using the Eqn. (11) as

$$p^{(m)}\left(\chi\right)=\int_{R_0}^{R}\prod_{j=1}^{M}p_\chi^M\left|\left(\chi\,|\,r\right)p\left(r_j\right)dr_j\right. \tag{11}$$

where $p\left(r_j\right)$ defined in equation (2) and eq (11) is roughly evaluated by log normally distributed random variable with parameters μ_x & can σ_x^2 be expressed using the Eqns. (12) & (13) as

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

and

$$\sigma_x^2 = \frac{1}{A^2}\left(\ln E\left[p_r^{(m)}\right]^2\right) - 2\ln E\left[p_r^{(m)}\right] \tag{13}$$

From equations (12) and (13), the equation (11) can be written as

$$p^{(m)}(\chi) = \frac{1}{Ax\sigma_x\sqrt{2\pi}}\exp\left\{-\frac{\left(10\log_{10}(x)-\mu_x\right)^2}{2\sigma_x^2}\right\} \tag{14}$$

$E\left[p_r^{(m)}\middle|r\right]\&E\left[p_r^{(m)^2}\middle|r\right]$ can both be evaluated using the Fenton's approximation analysis.

Here, $E\left[p_r^{(m)}\middle|r\right]\&E\left[p_r^{(m)^2}\middle|r\right]$ are obtained by averaging $E\left[p_r^{(m)}\middle|r\right]\&E\left[p_r^{(m)^2}\middle|r\right]$ over r_1, r_2, ……. , r_M. So, the average probability of $p_r^{(m)}$, can be written as

$$\begin{aligned} E\left[p_r^{(m)}\middle|r\right] &= e^{A\mu_M + A^2\sigma_M^2} + e^{A\left(\mu_j - \frac{A}{2}\sigma_M^2 + \frac{A}{2}\sigma_M^2 + \frac{1}{A}\ln(M)\right) + \left(\frac{1}{2}A^2\sigma_M^2\right)} \\ &= e^{A\mu_j + \frac{A^2}{2}\sigma_M^2 + \ln(M)} \end{aligned} \tag{15}$$

$$E\left[p_r^{(m)}\middle|r\right] = M\, e^{A\mu_j}.e^{\frac{A^2}{2}\sigma_M^2} \tag{16}$$

$$E\left[p_r^{(m)}\middle|r\right] = M\; p_m d_j^{-4}.e^{\frac{A^2}{2}\sigma_M^2} \tag{17}$$

where $\mu_j = \left\{10\log_{10}(p_m) - 40\log_{10}(d_j)\right\} = 10\log_{10}\left(p_m.d_j^{-4}\right)$ & $e^{A\mu_j} = p_m * d_j^{-4}$

The equation (17) can be written as

$$E\left[p_r^{(m)}\middle|r\right] = M\; p_m d_j^{-4}.e^{\frac{A^2}{2}\sigma_M^2} \tag{18}$$

Integrating Eq. (18) over r_1, r_2, ……. , r_M :

$$E\left[p_r^{(m)}\right] = \int_{R_0}^{R} M_p\left(r_j\right) P_m d_j^{-4} e^{A^2\sigma_M^2/2} dr_j \tag{19}$$

$$E\left[p_r^{(m)} \right] = M\, P_m e^{A^2\sigma_M^2/2} \int_{R_0}^{R} \frac{2r_j}{R^2 - R_0^2} d_j^{-4} dr_j \tag{20}$$

Since secondary user is at position (0,0), $d_j = r_j$:

$$E\left[p_r^{(m)} \right] = M\, P_m e^{A^2\sigma_M^2/2} \int_{R_0}^{R} \frac{2r_j}{R^2 - R_0^2} d_j^{-4} dr_j \tag{21}$$

$$E\left[p_r^{(m)} \right] = \left(\frac{M\, P_m e^{A^2\sigma_M^2/2}}{R^2 - R_0^2} \right).2\left[\frac{1}{2}\left(\frac{1}{R^2} - \frac{1}{R_0^2} \right) \right] = \frac{M\, P_m e^{A^2\sigma_M^2/2}}{R^2 - R_0^2} \left[\frac{R^2 - R_0^2}{R^2 R_0^2} \right] \tag{22}$$

$$E\left[p_r^{(m)} \right] = \frac{M\, P_m e^{A^2\sigma_M^2/2}}{R_0^2 R^2} \tag{23}$$

$$E\left[\left(P_r^{(m)} \right)^2 \right] = \frac{M P_m^2 e^{2A^2\sigma_m^2}}{3R_0^6 R^6} \cdot \left[\left(\frac{R^6 - R_0^6}{R^2 - R_0^2} \right) + \frac{3(M-1) R^2 R_0^2}{e^{A^2\sigma_m^2}} \right] \tag{24}$$

From the above analysis, the received power at the SU from the PU transmitter is derived in Equation (3) and the received power at the SU from the MUs is derived in Equation (6) and their respective PDFs, Equation (4) and Equation (14) have been derived.

3.2. Impact of PUEA investigation using Neyman-Pearson Composite Hypothesis (NPCH) Test

Neyman-Pearson Composite Hypothesis Test can be used to distinguish between two hypotheses:

- H_1 - Primary User transmission, which indicates only PU signal is present.
- H_2 - Malicious user transmission, which indicates that PU signal is absent only malicious user signal is present.

In this hypothesis test, each legitimate SU can make out two types of errors that is the probability of false alarm and probability of miss detection as shown in Figure 3. In the Figure 3, where the probability density functions of the received signal can be identified with and without the primary signal. If we want to keep the likelihood of missed detections very low, the likelihood of false alarms increases and this would lead to low spectrum usage. On the other hand, a low probability of false alarms would result in a high probability of missed detection which increases the primary user interference. This trade-off must be looked into carefully.

- **False alarm:** The SU makes a decision that the transmission is due to a PU but the MU is actually communicating.
- **Miss detection:** The SU makes a decision that the transmission is due to a MU but the PU is actually communicating.

The NPCH test calculates the PDF of received power at the SUs due to the PU transmitter and also the PDF of received power at the SUs due for the MUs and the division gives the decision variable *T* as

$$T = \frac{p^{(m)}(x)}{p^{(pr)}(x)} \tag{25}$$

where $p^{(pr)}(x)$ the probability density function of the received power at the SU receiver from the PU transmitter following a log normal distribution and $p^{(pr)}(x)$ is the probability density function of received power at the SU receiver from malicious users following a log normal distribution. The value of *T* is compared

with predefined threshold and the SU makes the following decision which is made based on the following the measure:

$$\begin{aligned} T \geq \lambda\, D_1 &: \text{Primary User Transmission} = H_1 \\ T \geq \lambda\, D_2 &: \text{Malicious User Transmission} = H_2 \end{aligned} \tag{26}$$

The SU may take the decision of D_2 when H_1 is true and D_1 when H_2 is true. These errors based on the decision rule, which is associated with the probability. The probability of miss detection and probability of false alarm are given by the equations (27) and (28) as

$$P_r\{D_2 \mid H_1\} = \int_{T \geq \lambda} p^{(r)}(x).dx = \alpha \tag{27}$$

$$P_r\{D_1 \mid H_2\} = \int_{T \geq \lambda} p^{(m)}(x).dx \tag{28}$$

where λ the constraint of the probability and both equations is can also be represented in a shorthand form as:

$$T \underset{D_1}{\overset{D_2}{\gtrless}} \lambda \tag{29}$$

Form equation (29), NPCH test allows us to decide any one probability either probability of false alarm or probability of miss detection.

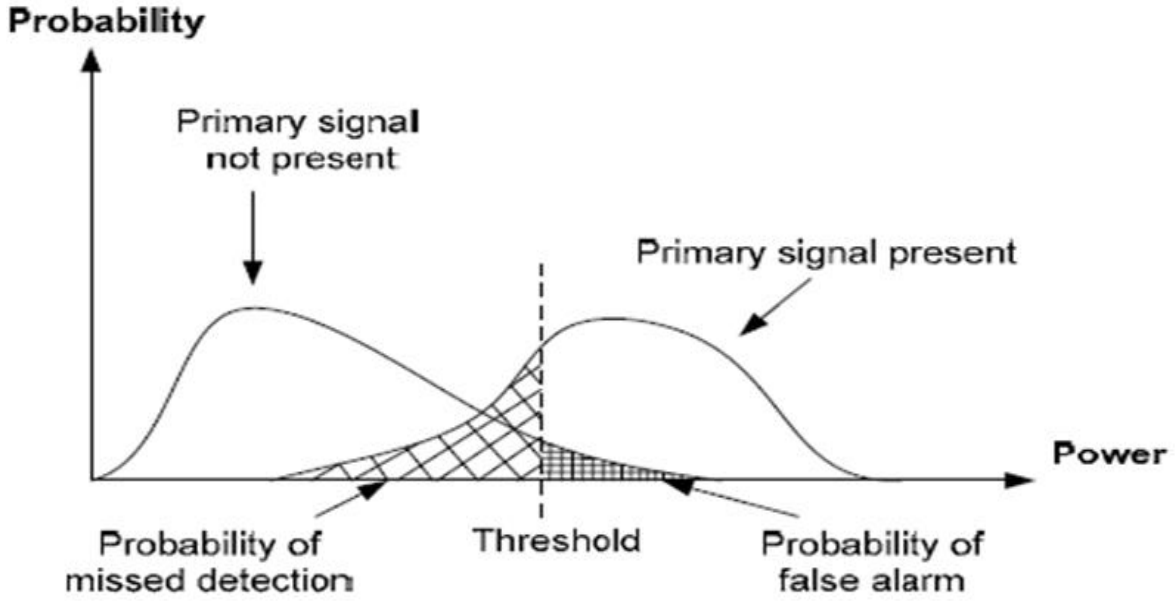

Figure. 3. The probability density functions of the received signal

4 Simulations Results

Here, in the Section-4, experimental outcomes are portrayed in order to prove the effectiveness of the mathematical model which is being developed by us and also analysis the impact of malicious user mainly PUEA in the CRN. All the simulation is performed for the developed model using MATLAB 2018a platform. Figure 2 shows that, a simple model of CRN, SUs deployed in the circular grid (R) network with R = 1 km, R_0 = 30 m. The primary user transmitter is located at a distance D_p = 100 km from the secondary users.

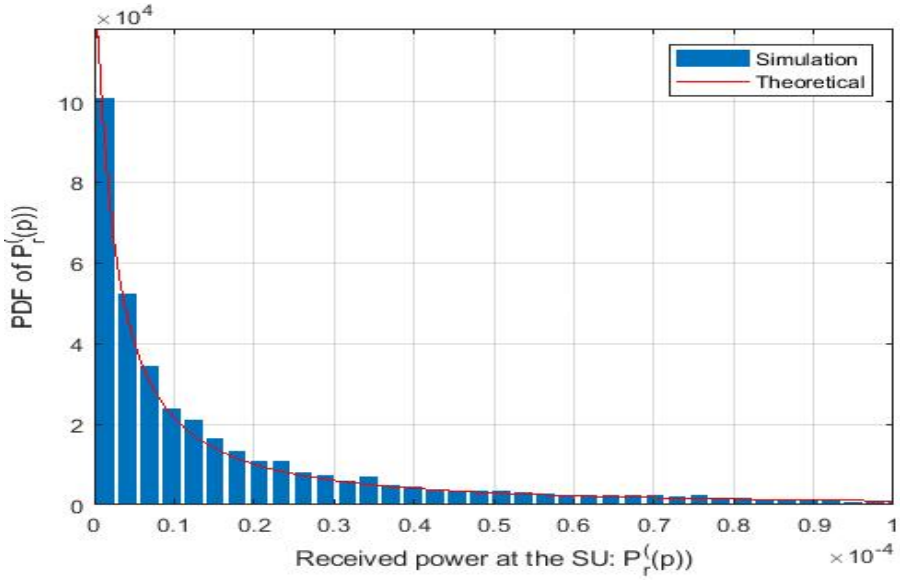

Figure 4. Probability density functions of received power at the secondary user receiver due to PU: $P_r^{(p)}$

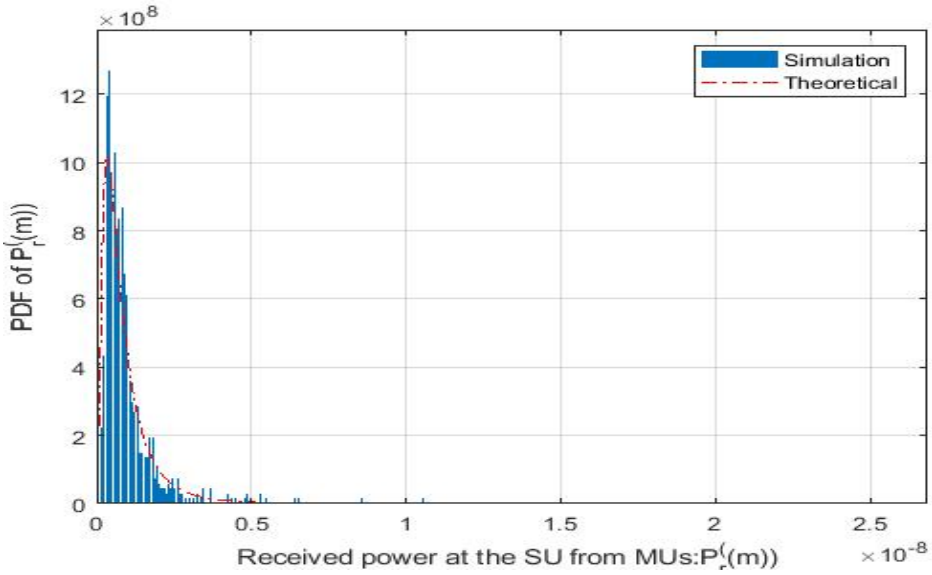

Figure 5. Probability density function of received power at the secondary receiver due to MU: $P_r^{(m)}$

The transmitting power of the PU transmitter is set to be 100 kW and secondary users (both Legitimate user and malicious user) transmitting power is set to 4 W as devised by Jin *et.al.* (2009). The variances of the PU (σ^2_p) and MU (σ^2_m) transmissions are taken to be 8 dB and 5.5 dB, respectively. The number of MUs are assumed to be randomly distributed around the circular grid. The simulation testing time is set to 10000. The results are carried out by using Matlab 2018a, as well as the theoretical models are shown in figure 2, the PDFs of the received power from the PU transmitter and malicious user transmitter at the SUs as illustrated in figure 4 and figure 5. Both the figures show that the PDFs of the received power from the PU transmitter and malicious user transmitter at the secondary user differ from each other using the NPCH test.

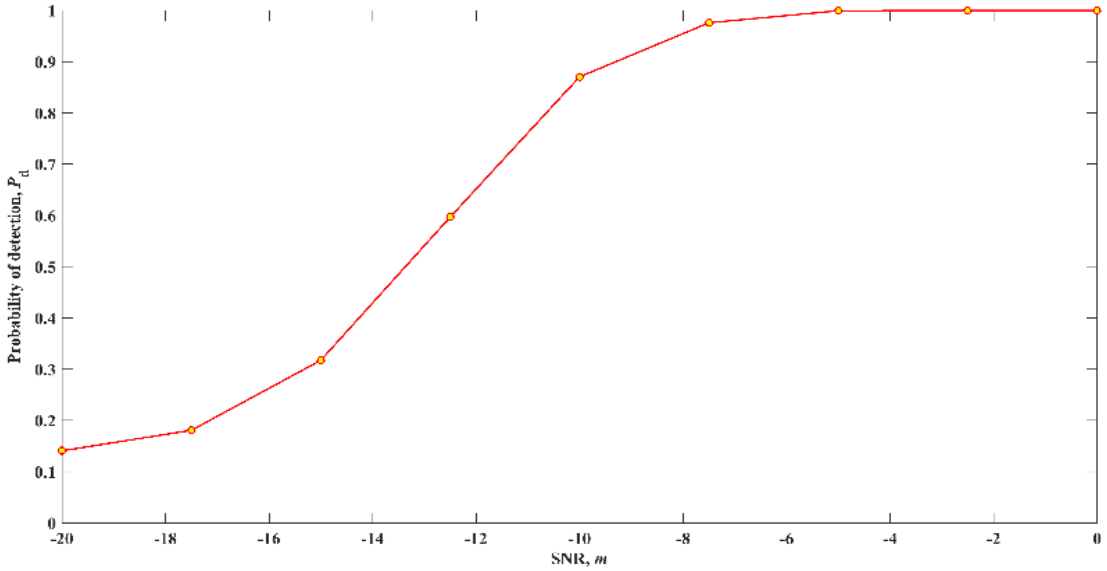

Figure 6. Probability of detection v/s SNR using Energy detection.

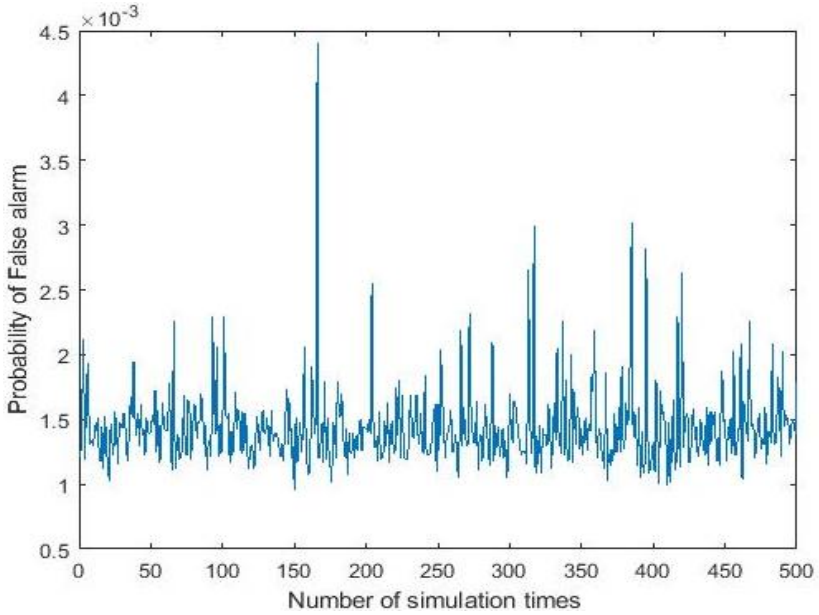

Figure 7. Probability of False Alarm, M = 10, R= 500 m, R_0 = 30m.

Figure 6 illustrates the probability of detection for different SNR with 10 malicious user. We vary the SNR form 0 to –20 dB. This figure shows that probability of detection is very poor for low SNR using Energy detection technique. We considered SNR = 0 dB to calculate Probability of false alarm and probability of miss detection in this work. Figures 7 and figure 8, illustrates the plot for the probability of False alarm and the probability of Miss Detection respectively. The number of malicious users, in this case, is set to be MU = 10, the radius of outer region R = 500 m, Radius of primary exclusive region R_0 = 30 m. The transmitting power of the primary user transmitter and malicious user transmitter is taken as P_t = 100 KW and P_m = 4 w respectively. Variances of the primary user (σ^2_p) and malicious user (σ^2_m) transmissions are taken to be 8 dB and 5.5 dB, respectively. The simulation time is set to be 500 times and the threshold value (λ) = 2.

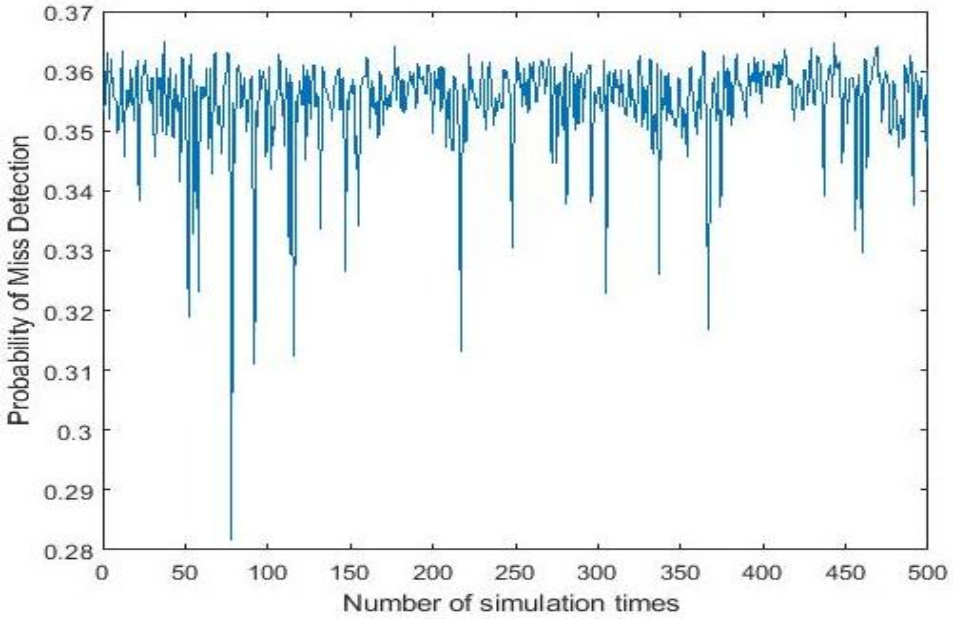

Figure 8. Probability of Miss Detection. M = 10, R= 500m, R_0 = 30 m.

Figures 9, 10, 11 and 12 shows the probability of errors rate (probability of false alarm and miss detection rate) at different numbers of malicious users. The radius of outer region R = 500 m, Radius of primary exclusive region R_0 = 30 m. The transmitting power of the primary user transmitter and malicious user transmitter is taken as P_t = 100 Kw and P_m = 4 w respectively. The threshold values is set to 2. The probability of errors (P_f and P_m) are observed for different values of outer radius (R = 300 m and R = 800 m) with same number of malicious users (MU = 15).

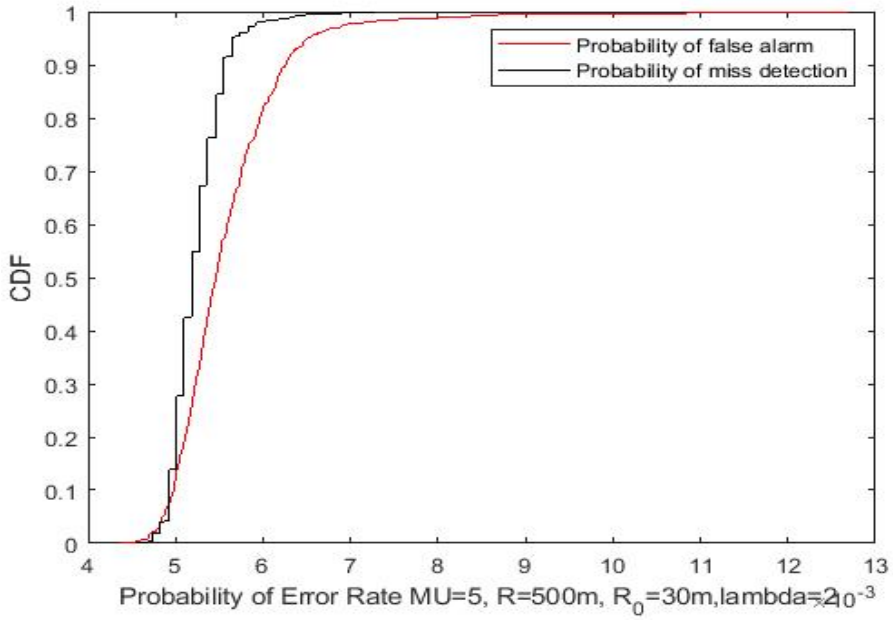

Figure 9. Probability of Errors rate malicious user (MU=5), R = 500 m.

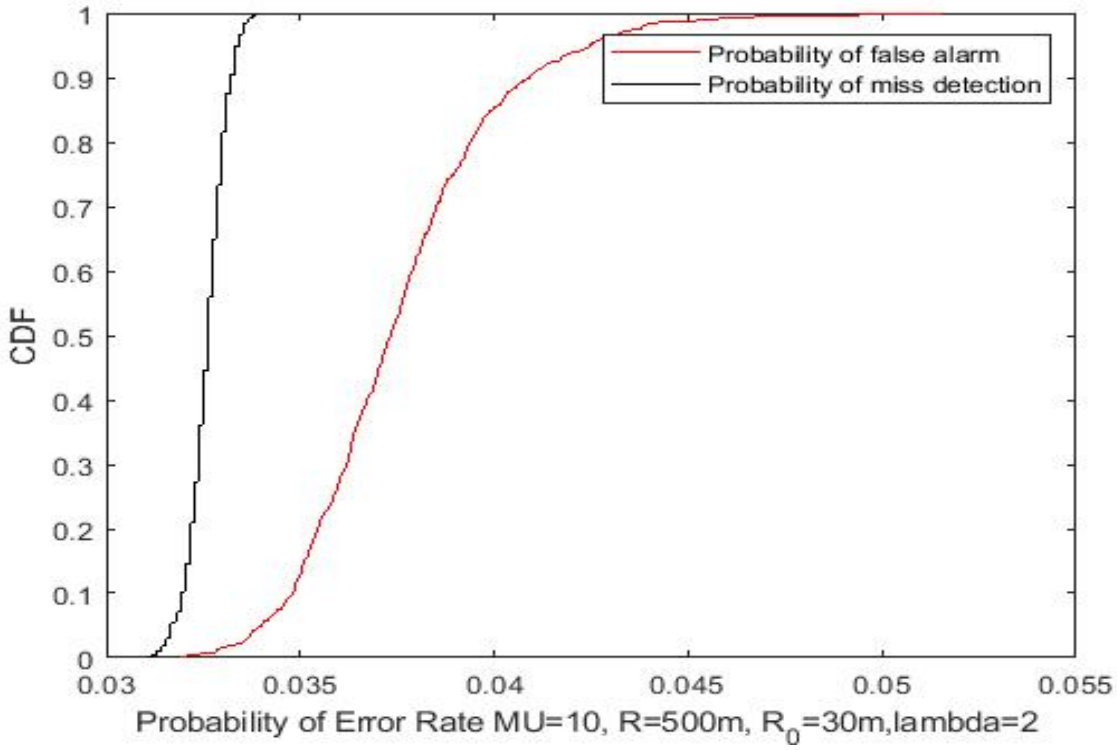

Figure 10. Probability of Errors rate malicious user (MU = 10), *R* = 500 m.

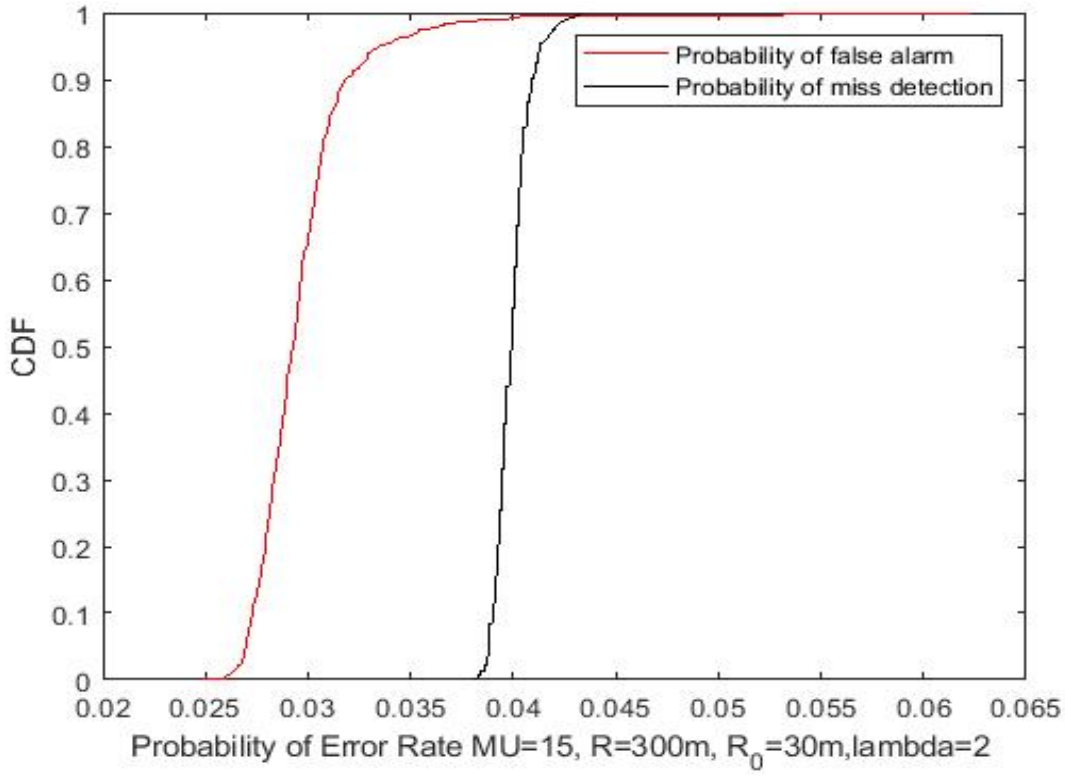

Figure 11. Probability of Errors rate malicious user (MU=15), *R*=300m.

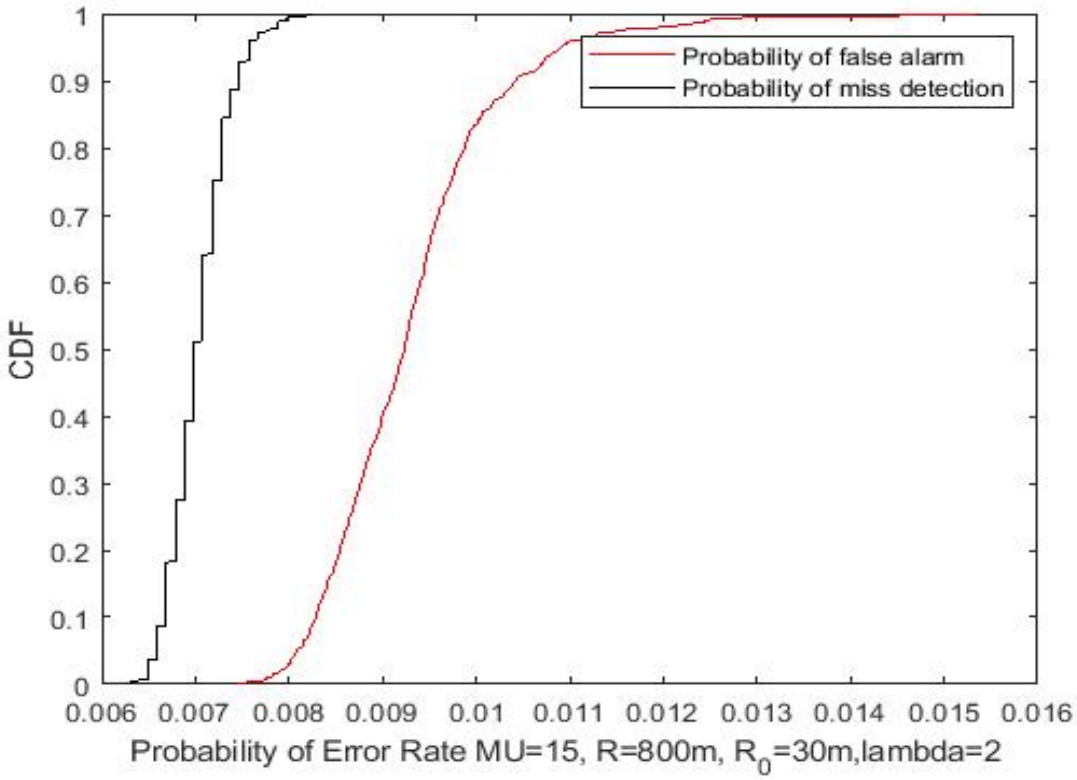

Figure 12. Probability of Errors rate malicious user (MU=15), R = 800 m.

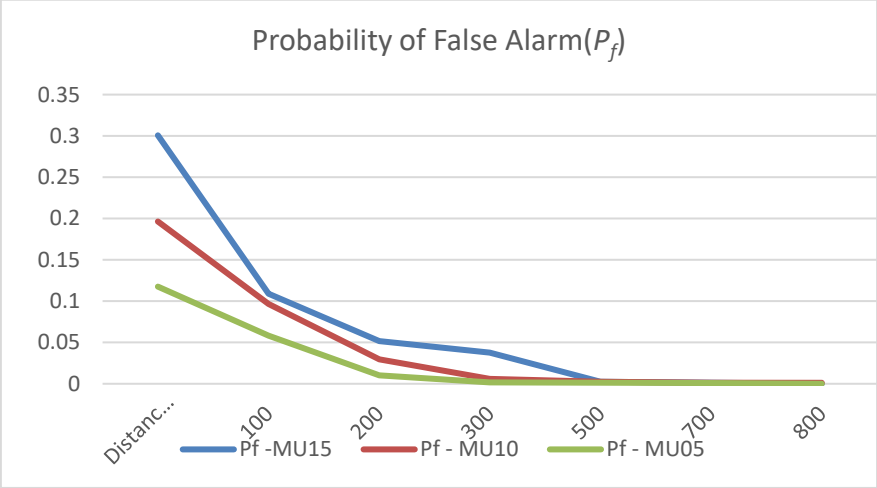

Figure 13. Probability of False Alarm with respect to various radius of the angular region (R) and number of malicious users.

The probability of errors (P_f and P_m) are observed and tabulated as shown in table 1, at a different number of the malicious user (MU = 5, 10, and 15) and the radius of outer region R various from 100 m to 1000 m and the radius of primary exclusive region R_0 = 30 m as illustrated in the figures 13 and figure 14. When angular region (R) is 100m and malicious users are 5, the probability of false alarm is 0.1176. If we vary the number of malicious users from 5 to 10 or 15, the probability of false alarm increases to 0.1964 and 0.3007 respectively. It is observed that the probability of false alarm increases as the more malicious users present in the network. As we increase the radius of the outer region can reduce the effect of the PUEA on the network.

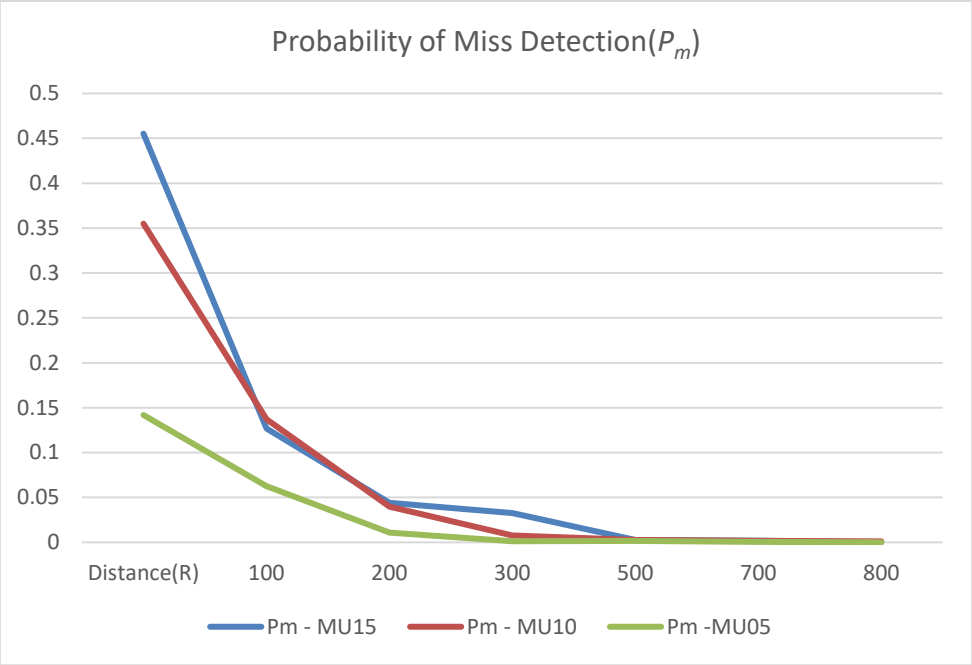

Figure 14. Probability of Miss Detection with respect to various radius of the angular region (*R*) and number of malicious users.

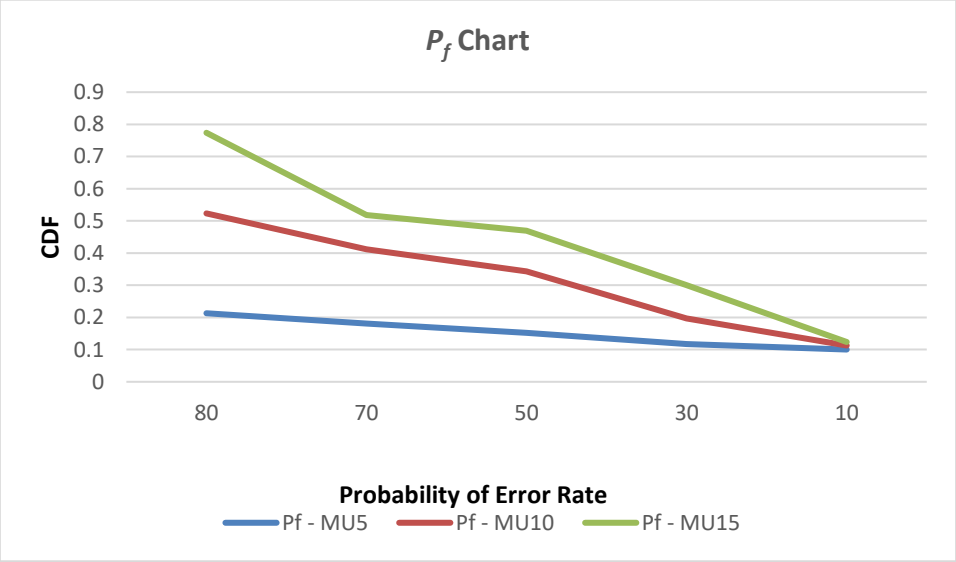

Figure 15. Probability of false Alarm at different number of malicious user present in the Network.

Figure 15, illustrate the probability of false alarm at different malicious users (MU = 5, 10 and 15) present in the network with varying their transmitting range(primary exclusive region R_0) from 10 m to 80 m at constant radius of outer region R = 100 m. From this graph, we can observed that the probability of false alarm increases if the primary exclusive region and the number of attackers increases. This is because for a large value of R_0, the radius of outer region R tends to be smaller. Therefore, the malicious users become closer to the legitimate secondary users and the total received power from all the malicious users become close to the receiver (legitimate secondary user).

If the radius of outer region R is large, the total received power from the MUs may not be enough to successfully launch a PUEA in the network. From the figure 15, shows that the probability of false alarm is less when the malicious user is low (MU = 5) compare to when more malicious users (MU = 10 or MU = 15) are

present in network. Hence the proper selection of the network defined angular region radius R and the primary exclusive region radius R_0 can reduce the impact of the PUEA in the network.

Table 1. Probability of Errors with respect to various radius of the outer region(R) and number of malicious users.

Number of Malicious Users (MU) =15							
Threshold Value (λ = 2)							
Distance (R) in meters	100	200	300	500	700	800	1000
P_f	0.3007	0.1092	0.0517	0.0376	0.0026	0.0014	0.000105
P_m	0.4552	0.1266	0.0442	0.0326	0.0027	0.0018	0.000100
Number of Malicious Users (MU) = 10							
Threshold Value (λ = 2)							
Distance (R) in meters	100	200	300	500	700	800	1000
P_f	0.1964	0.0967	0.0296	0.0061	0.0024	0.0013	0.0012
P_m	0.3549	0.1372	0.0399	0.0075	0.0025	0.0017	0.0011
Number of Malicious Users (MU) = 5							
Threshold Value (λ = 2)							
Distance (R) in meters	100	200	300	500	700	800	1000
P_f	0.1176	0.0581	0.0101	0.0016	0.0014	0.00093	3.6334e-05
P_m	0.1418	0.0624	0.0108	0.0012	0.0017	0.00070	3.3677e-05

5. Conclusion

The Primary User Emulation attack affects the performance of the spectrum sensing process in the cognitive radio networks by imitating as the licensed user. We proposed an analytical model to study the effect of the probability of errors in terms of the probability of false alarm and probability of miss detection based on the NPCH test by varying the range of the radius. In this proposed work we analyze the impact of the PUEA by varying the distance between the licensed user and secondary users, a radius of the secondary users, and also a number of malicious users present in the network. The simulation results show that the probability of false alarm increases due to the number of malicious users increases. It also increases due to decreases in the outer angular radius of the range and increases the radius of the primary exclusive region. Hence the proper selection of the network defined angular region radius R and the primary exclusive region radius $R0$ can reduce the impact of the PUEA in the network. In the future work will consider two or more primary transmitter to analyze the effect of this attack.

References

1. Mitola III J. and G. Maguire Jr. (1999). Cognitive radio: making software radios more personal. IEEE Personal Communications. 6(4), 13–18.
2. Chen, R., J. Park and J.H. Reed. (2008). Defense against Primary User Emulation Attacks in Cognitive Radio Networks. IEEE Journal on Selected Areas in Communications. 26(1), 25-37.
3. Manesh M.R., & Kaabouch N. (2018). Security threats and countermeasures of MAC layer in cognitive radio networks. Ad Hoc Networks. 70(1), 85-102.
4. Sharma, Rajesh & Rawat Danda B. (2015). Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey. IEEE Communications Surveys and Tutorials. 17(2), 1023 – 1043.
5. Chen, R., J. Park and J. H. Reed (2008). Defense against Primary User Emulation Attacks in Cognitive Radio Networks. IEEE Journal on Selected Areas in Communications. 26(1), pp. 25-37.
6. Jung-Min Jerry Park, Kaigui Bian, Ruiliang Chen. (2010). Chapter 15 - Cognitive radio network security, Cognitive Radio Communications and Networks. Academic Press, ISBN 9780123747150. 431-466.
7. Sharma, Himanshu; Kumar, Kuldip. (2016). Primary User Emulation Attack Analysis on Cognitive Radio. Indian Journal of Science and Technology, ISSN 0974-5645, 9(14), 1-6.
8. Marinho J, Granjal J, Monteiro E. (2015). A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. EURASIP Journal of Information Security. 1(1), 1–14.

9. Ruiliang Chen and Jung-Min Park. (2006). Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks. First IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR), Reston, VA, September. 110-119.
10. Lianfen Huang, Liang Xie, Han Yu, Wumei Wang and Yan Yao (2010). Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio Networks, International Conference on Communications and Mobile Computing (CMC), Shenzhen, China, 2(0), 169-173.
11. Jin, F., V. Varadharajan , U. Tupakula. (2015). Improved detection of primary user emulation attacks in cognitive radio networks. IEEE Telecommunication Networks and Applications Conference (ITNAC). 274-279.
12. Alahmadi, A., M. Abdelhakim, Jian Ren and Tongtong Li. (2013). Mitigating primary user emulation attacks in cognitive radio networks using advanced encryption standard. IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, 3229-3234.
13. Goergen, N., T.C. Clancy and T.R. Newman. (2010). Physical Layer Authentication Watermarks through Synthetic Channel Emulation. 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN), Singapore, 1-7.
14. Yuan, Z., D. Niyato, H. Li, J. B. Song and Z. Han. (2012). Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks. IEEE Journal on Selected Areas in Communications. 30(10), 1850-1860,
15. Mahesh Kumar N., Dr. Siddesh G.K. (2020). Detection of the primary user emulation (PUE) attacks utilizing various spectrum sensing techniques in cognitive radio networks. International Journal of Grid and Distributed Computing, IJGDC. 13(1), ISSN: 2005-4262, 256-271.
16. Anand, S., Z. Jin, and K. P. Subbalakshmi. (2008). An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks. Proceedings of 3rd IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 1-6.
17. Jin, Z., S. Anand, and K.P. Subbalakshmi. (2009). Mitigating Primary User Emulation Attacks in Dynamic Spectrum Access Networks using Hypothesis Testing. ACM Sigmobile Mobile Computing and Communications Review. 13(2), 1-8.
18. Efe Orumwense et.al. (2014). Impact of Primary User Emulation Attacks on Cognitive Radio Networks. International Journal on Communications Antenna and Propagation (I.Re.C.A.P.). 4(1), ISSN 2039 – 5086, 1-10.
19. Mahesh Kumar N., Siddesh G.K. (2020). Simulation of PUE Attack Detection using Transmitter Locations and Modulation Techniques in CRNs. International Journal of Advanced Science and Technology. 29(6s), 2320-2334.
20. Jin, Z., S. Anand, and K.P. Subbalakshmi. (2009). Detecting primary user emulation attacks in dynamic spectrum access networks. Proceedings of the 2009 IEEE international conference on Communications (ICC'09). IEEE Press. 2749–2753.