Security Aspects in Cognitive Radio Networks

Detection and Mitigation of Primary User Emulation Attacks

Mahmod Ammar, Nick Riley, Meftah Mehdawi, Anwar Fanan, Mahsa Zolfaghari

School of Engineering
University of Hull
Hull, UK
E-mails: {M.A.Ammar@2011, N.G.riley, M.A.Mehdawi@2010, A.M.Fanan@2012, M.Zolfaghari@2009}.hull.ac.uk

***Abstract*—Cognitive Radio Networks (CR) is an advanced growing technique and a promising technology for the upcoming generation of the wireless networks. Deployment of such networks is hindered by the vulnerabilities that these networks are exposed to, in this paper we focus on security problems arising from Primary User Emulation Attacks (PUEA) in CR networks. We study the impact of this attack on CR networks, detection and defense approaches. We have setup the system model using Matlab software; the Neyman-Pearson composite hypothesis test NPCHT is used to obtain the hypothesis test and detect the PUEA. Simulation results proved that using NPCHT it is possible to keep the probability of successful PUEA low, and this depends on the threshold values; the number of malicious users in the system can significantly increase the probability of false alarm in the network, Also it shows that there is a range of network radii in which PUEA are most successful.**

Keywords-Cognitive Radio (CR); Primary User Emulation Attack (PUEA); Probability Density Function (PDF); Neyman Pearson composite hypothesis test (NPCHT);

I. INTRODUCTION

Spectrum sensing and spectrum sharing are important functionalities of CR which enables the secondary users to monitor the frequency spectrum and detect vacant channels to use [1]; it is also important to address the security and reliability issues in the CR. An example of CR networks is the usage of unused spectrum (white spaces) in the television band where the TV transmitter becomes a primary transmitter, i.e., the TV receivers are primary receivers or licensed users and while the other users who are not TV subscribers but wish to use the spectrum in the TV band for their own communication becomes secondary transmitters/receivers.

The essential purpose of spectrum sensing employment in a CR network is to identify empty spectral bands (white spaces) and once these white spaces have been identified, CR nodes opportunistically utilize these unoccupied bands of spectrum by wirelessly operating across them while simultaneously avoiding interference with the primary users [2]. In a CR network, primary users possess the priority to access the spectrum band, while the secondary users must always give up access of the spectrum band over to the primary users and ensure that no interference is caused. Subsequently, if a primary user begins to transmit across a frequency band occupied by a secondary user, the secondary user is ideally required to vacate that specific spectral band immediately. But when there is no active primary user communication in the spectrum, all other users enjoy equal right to access the unoccupied spectrum band. For a secondary user to gain equal rights as the primary user, the secondary user may tend to modify the air interface so as to mimic the primary user's characteristics causing the secondary user to behave maliciously. The resultant effect of this is that the other secondary users will identify the malicious user as a primary user there by vacating the occupied spectrum band for the malicious user believing that it is a primary user. In this way, the malicious user gets access to the primary user's spectrum band. In literature, this kind of attack against CR networks is considered as a Primary User Emulation Attack (PUEA) [3].

Therefore, we can define PUEA as an attack in CR networks where the malicious user pretends to be the primary user to obstruct idle channels by transmitting a similar signal as the primary user [3]. Masquerading of a primary user allows threat identifies the malicious masquerading of a primary user like a digital TV broadcaster. The malicious attacker may mimic the primary user characteristics in a specific frequency band (e.g., white space band), so that the legitimate secondary users erroneously identify the attacker as an incumbent and they avoid using that frequency band; the attacker primary focus is to disrupt the secondary user's transmissions by making contact with it as many times as possible, each time the jammer does this it forces the secondary users to change channels as they cannot differentiate it from a primary user. The presence of PUEA causes a number of troubles for CR networks. A PUEA can be launched while the spectrum is being sensed or detected by using cyclostationary, energy or matched filter detection signal features [4].

We can classify the protection techniques against these types of threats in the following categories: (i) protection techniques based on reputation and trust of the CR nodes [5], (ii) identification of the masquerading threat though signal analysis [6], (iii) authentication of the CR node through cryptographic techniques [7], and (iv) geolocation database of primary users [8].

The remainder of this paper is organized as follows. In Section II, the model design and simulation setup are Introduced. Section III describes the model analysis and probability density function of the received signal. Our simulation results, conclusion and future work are discussed in Section IV and section V, respectively.

 ISBN: 978-1-61208-403-9

A. *Objective of adversarial attackers*

The objectives of an attacker have a direct correlation with the way the attacks are launched, and therefore, they determine the nature of attacks [9][10].

1) *Selfish attacks*: The attacker's motive is to acquire more spectrum for its own use by preventing others from competing for the channels and unfairly occupying their share. In this type of attack, adversaries will defy the protocols and policies only if they are able to benefit from them [11][12].

2*) Malicious attacks:* The attacker's only objective is to create hindrance for others and does not necessarily aim at maximizing own benefits. They do not have any rational objective and identify protocols and policies to just induce losses to others [13].

B. *Impact of PUE attacks on CR Networks*

The presence of PUE attacks causes a number of troubles for CR networks. The list of potential consequences of PUE attacks is:

- Bandwidth waste: The ultimate objective of deploying CR networks is to address the spectrum under-utilization that is caused by the current fixed spectrum usage policy. By dynamically accessing the spectrum "holes", the SUs are able to retrieve these otherwise wasted spectrum resources [14].
- QoS degradation: The appearance of a PUE attack may severely degrade the Quality-of-Service (QoS) of the CR network by destroying the continuity of secondary services [14].
- Connection unreliability: If a real-time secondary service is attacked by a PUE attacker and finds no available channel when performing spectrum handoff, the service has to be dropped. This real time service is then terminated due to the PUE attack. In principle, the secondary services in CR networks inherently have no guarantee that they will have stable radio resource because of the nature of dynamic spectrum access. The existence of PUE attacks significantly increases the connection unreliability of CR networks. Also the Hidden Node Problem (HNP) can cause unreliable connection; the most common approach against HNP is based on collaborative sensing to identify the incorrect spectrum perception of the affected CR node. This is the approach adopted in standard IEEE 802.22 [15], where decision rules (e.g., voting algorithm) are used to correct errors in the spectrum sensing function. In a similar way, this approach is also described by Prasad [16], even if the term distributed spectrum sensing is used.
- Denial of Service: Consider PUE attacks with high Attacking frequency; then the attackers may occupy many of the spectrum opportunities. The SUs will have insufficient bandwidth for their transmissions, and hence, some of the SU services will be interrupted. In the worst case, the CR network may even find no channels to set up a common control channel for delivering the control and this is called Denial of Service in CR networks.

II. MODEL DESIGN AND SIMULATION SETUP

In our scenario, all secondary and malicious users are distributed in a circular grid of radius R, as shown in Fig. 1.

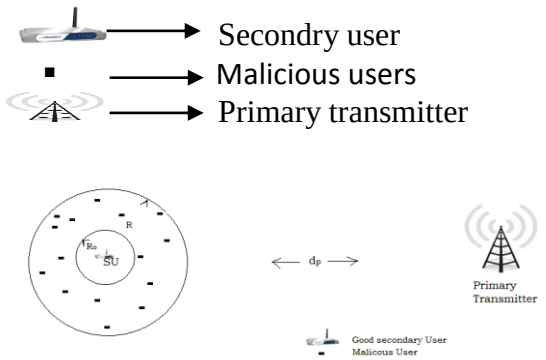

Figure 1. CR Network Model

A primary user (e.g., a TV tower), is located at some distance from all the users, the secondary users are randomly and uniformly distributed within a network radius from the primary transmitter. In order to detect the white spaces or the return of the primary, the secondary users measure the received power, if the received power is below a specified threshold then the spectrum band is considered to be vacant (white space). If the received power is above the specified threshold, then based on the measured power, a decision is made as to whether the received signal was transmitted by a primary transmitter or by a set of malicious users [17]. We design a Neyman-Pearson Composite Hypothesis Test (NPCHT) to obtain a criterion for making this decision. To perform the analysis, the assumptions below are taken:

- The distance between primary transmitter and all the users is d*p*=120Km.
- There are M malicious users in the system. M is a geometrically distributed random variable.
- The locations of malicious users are uniformly distributed in the circular grid of radius R=500m as our simulation shows in Fig. 2 when M=30.The received power at the secondary user from each of the malicious user is Independently and Identically Distributed (IID). This is valid due to the symmetry of the system and the fact that the malicious users presented uniformly in an annular region between the centered at (0, 0) and radii (R_0, R), if the received power is not IID, then the SU will use another power control scheme.

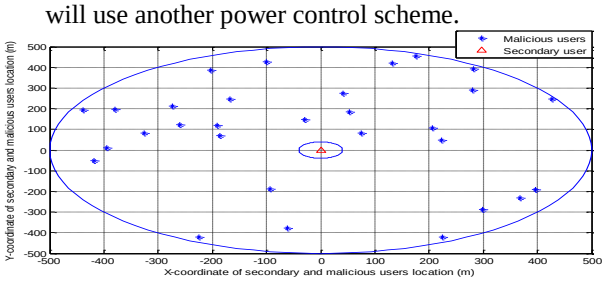

Figure 2. Simulation result of malicious users distributed randomlly around the secondary user located at coordinate (0,0).

- The primary transmits at a power Pt =120 KW while the malicious users transmit at a power Pm=

5W. All the values of the system parameters we have used are in Table I below.

- The primary transmitter co=ordinates are fixed at a point (rp, θp) and this position is known to all the users in the grid.
- The secondary user co-ordinates (r, θ), no malicious users are present within a circle of radius R0=40m known as "exclusive distance from the secondary user" centered at (r, θ).in case of this condition is not met then the received power at the secondary due to transmission from any subset of malicious users present within a distance R0 from the secondary becomes too large to create PUEA [17].

TABLE I. SYSTEM PARAMETERS FOR OUR SIMULATION

Parameter	Value
Dp: Distance between primary transmitter and other users	120 Km
R : Radius of the circular grid	500 m
R0: Radii of annular region	40 m
M : Number of malicious usres in the system	10,15,30
Pt : Primary transmition power	120 KW
Pm : Malicious transmition power	5 W
σp: : Variance of Primary users	8 dB
σm : Variance of Malicious users	5.5 dB

- The transmission from primary transmitter and malicious users undergo path loss and log normal shadowing with mean 0 and variance σ^2p and σ^2m, respectively [18].
- The path loss exponent chosen for transmission from primary transmitter is 2 and from malicious user are 4.

III. MODEL ANALYSIS AND PROBABILITY DENSITY FUNCTION OF THE RECEIVED SIGNAL:

First, we have to obtain the Probability Density Function (PDF) of the received power at the secondary user due to transmission by the primary and by the malicious users in order to obtain a hypothesis test using Neyman-Pearson composite hypothesis test NPCHT [18].

A. Probability Density Function of the Received Signal

One of the applications of the probability density function of the received power is using it in Neyman Pearson's Composite Hypothesis Test NPCHT or any other statistical test to identify intruders and impostors in CR networks and also investigate the impact of PUEA in the network.

We consider M malicious users located at co-ordinates (rj, θj) $1 \leqslant j \leqslant M$. Since the position of the jth malicious user is uniformly distributed in the annular region between R0 and R, rj and θj are statistically independent ∀ j. The pdf of rj , p(rj) ∀ j is given by

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

where θj is uniformly distributed in $(-\pi,\pi)$ ∀j [19]. The received power at a secondary user from the primary transmitter, $p_r^{(p)}$ is given by

$$p_r^{(p)} = P_t d_p^{-2} G_p^2 \quad (2)$$

where $G_p^2 = 10^{\varepsilon p/10}$ and $\varepsilon_p = N(0, \sigma_p^2)$, as mentioned in Section II. Since P_t and d_p are fixed, the pdf of $p_r^{(p)}$, $P^{\Pr(\gamma)}$, follows a log-normal distribution and can be written

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

where $A = \frac{\ln 10}{10}$ and $\mu_p = 10\log_{10} p_t - 20\log_{10} d_p$

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

$$P_r^{(m)} = \sum_{j=1}^{M} p_m d_j^{-4} G_j^2 \quad (4)$$

where dj is the distance between the jth malicious user and the secondary user and G^2_j is the shadowing between the jth malicious user and the secondary user.

B. Detecting PUEA using Neyman-Pearson Criterion

We have used the two hypotheses in Neyman-Pearson decision criterion, which are given as below:
M1 : Primary Transmission in progress
M2 : Emulation attack in progress
In this hypothesis test, there are two types of errors that secondary user can make [20]:
False alarm: The secondary makes a decision that the transmission is due to primary but the malicious user is transmitting.
Miss Detection: The secondary makes a decision that the transmission is due to malicious user but the primary is transmitting.
In our simulation, the power of the received signal is measured in order to calculate the decision variable which is given by the ratio of $\Lambda = P^{m}(\chi) / P^{\Pr}(\chi)$
where $P^{\Pr}(\chi)$ and $P^{m}(\chi)$ is the pdf of received power from the primary and from all malicious users respectively. Λ is then compared with predefined threshold and the secondary decides the following

$\Lambda \leq \lambda \Longrightarrow$ D1: Primary transmission

$\Lambda \geq \lambda \Longrightarrow$ D2: PUEA in progress

First, secondary user may decide D2 when M1 is true, and second secondary user may decide that D1 when M2 is true. Each of these errors has a probability associated with it which depends on the decision rule and condition densities [14]. Miss Probability: P{D2|M1}= Probability of making decision D2 when M1 is true.
False Alarm Probability: P{D1|M2}=Probability of making decision D1 when M2 is true.

 ISBN: 978-1-61208-403-9

C. *Decision Rule*

In Fig. 3, we plot the decision rule showing Miss Probability and Probability of false alarm under Gaussian distribution. It shows the two conditional densities of the power received by the good secondary user from primary and malicious transmitters.

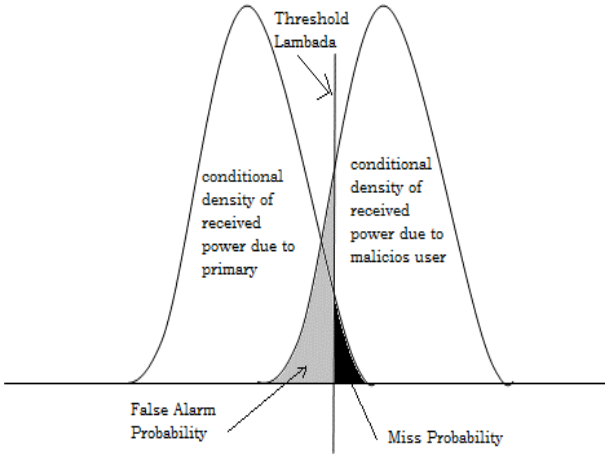

Figure 3. The Decision Rule

We compare the decision rule with the threshold value; Lambda (λ) and the miss probability and probability of false alarm are calculated accordingly [21].

IV. RESULTS AND ANALYSIS

In this section, we present the results obtained using Matlab simulation and also the theoretical results for the similar setup for the probability density function of the received power at the secondary user due to the primary transmitter and the received power at the secondary user due to the malicious users.

Also, we determined the performance of the network for PUE attack in terms of probability of miss detection and false alarm, in addition to the relationship between the false alarm probability (i.e., the probability of successful PUEA) and the network Radius R.

In our simulation, we have used the following system parameters, as shown in Table II.

TABLE II. SYSTEM SIMULATION PARAMETERS

Parameter	dp	R	Ro	M	Pt	Pm	σp	σm
Value	120 KM	500 m	40 m	15	120 KW	5 W	8 dB	5.5 dB

We can see from Fig. 4 and Fig. 5 that the results of the probability density function using simulations considerably match with the one derived mathematically.

There is a slight mismatch and the reason behind this is duo that the theoretical derivation is for ideal setup and over an unlimited duration of time while the simulation testing times are limited in number and also have random effects as per the simulation settings.

It is clear that the probability density functions of the received power at the secondary user from the primary transmitter differ from the received power at the secondary user from the malicious user.

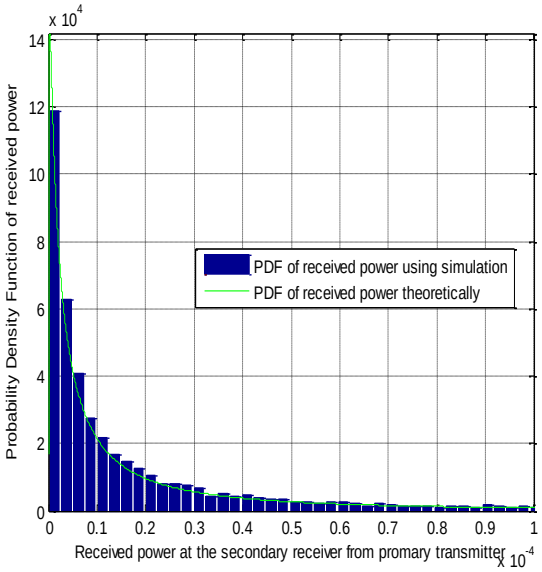

Figure 4. PDF of the received power deu to the primary transmitter

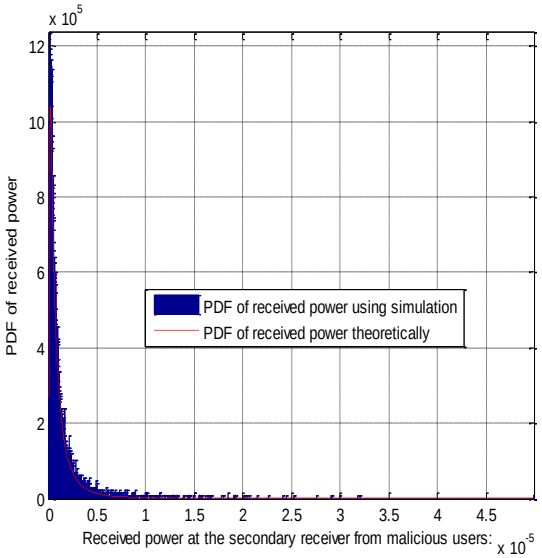

Figure 5. PDF of the received power due to the malicious users

Based on the PDF which we have achieved in our simulation and Neyman Pearson's Composite Hypothesis Test NPCHT approach, we have obtained the probability of successful PUEA (False Alarm),

Fig. 5 shows the relationship between the false alarm probability (i.e., the probability of successful PUEA) and the network Radius R, we set the threshold value λ at 2. It is observed that the probability of false alarm rises and then falls down with increasing value of R and also there is a value of R for which the probability of false alarm is maximum; this is as expected because:

Case 1- for a given R0, if R is small, the malicious users are closer to the secondary user and the total received power from all the malicious users is likely to be larger

 ISBN: 978-1-61208-403-9

than that received from the primary transmitter, thus decreasing the probability of successful PUEA.

Case 2- for large R, the cumulative received power at the secondary from the malicious users may not be sufficient to successfully launch PUEA.

We have done the simulation with different values of M, as shown in Fig.6; our results prove that when the PDF is used with NPCHT, the number of malicious users in the system has a significant impact on the network causing the secondary users suffer from degradation in the quality of their communication due to the transmission from the malicious users.

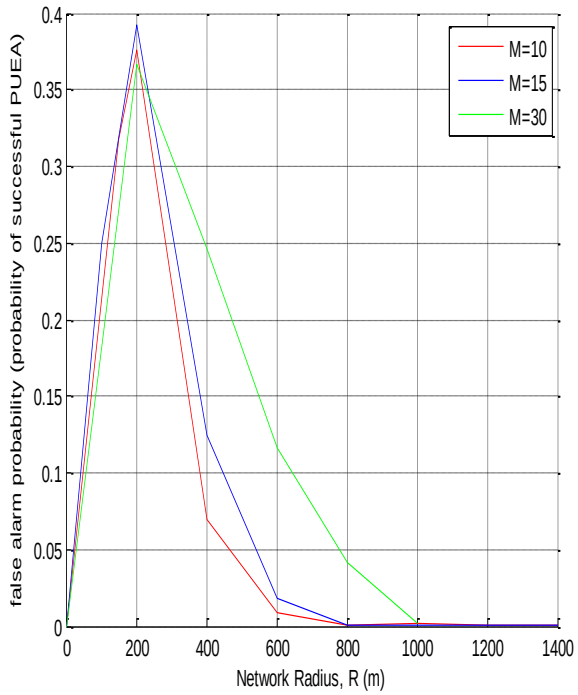

Figure 6. False alarm probability Vs. network Radius R

Fig. 7 and Fig. 8 are the plots for the probability of miss detection vs. the number of simulation times and False alarm vs. the number of simulation times respectively, Probability of miss detection and false alarms are calculated for 600 times of simulations. The threshold value for this simulation is set to 2, i.e. λ=2. The number of malicious users in this case is set to be M=35, the radius of outer region R=400m, Radius of primary exclusive region R0=40m, primary transmitter power Pt=120Kw, malicious transmitter power Pm=5w, σm =5.5dB, σp = 8dB.

As we can see from the experiment, the probability of false alarm (Successful PUEA) is always close to 0.326 (within ±0.04 of this value) for the all number of simulation runs and this is because the high number of malicious which we set at M=35.

The miss detection probability is averaged at 0.187 for the whole 600 runs, as one can see in Fig. 8.

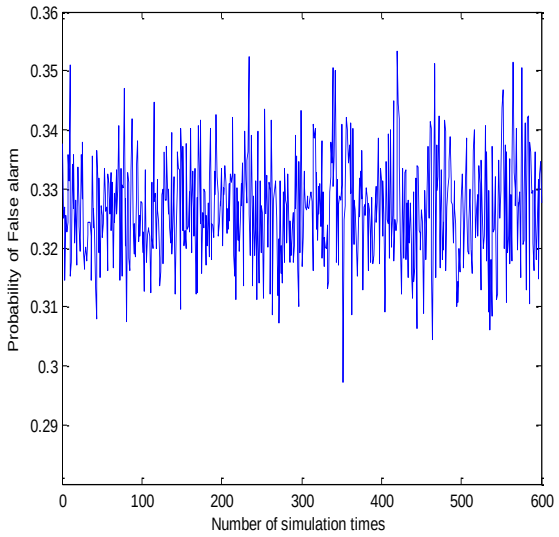

Figure 7. Probability of succefull PUEA (False e Alarm)

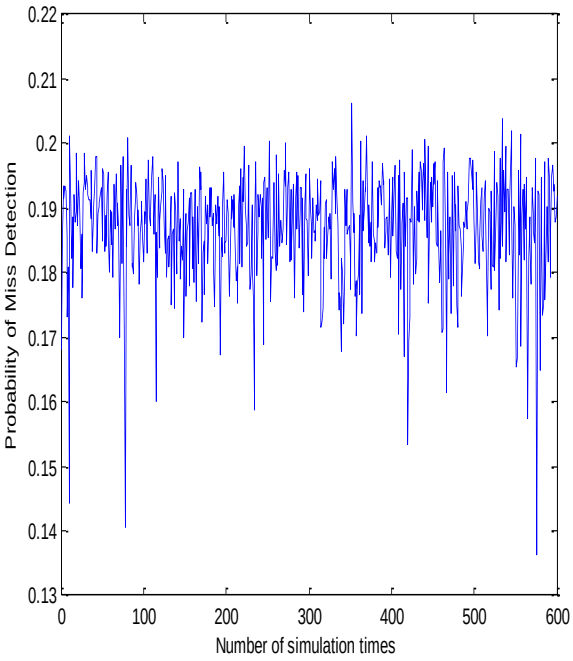

Figure 8. Probability of miss detection

We have done the simulation with different values of λ, as shown in Table III, and we have noted that when λ is decreased, the probability of successful PUEA decreased and the miss detection probability is increased; this is as expected, since NPCHT only allows a threshold to be set on either false alarm or miss detection probabilities.

 ISBN: 978-1-61208-403-9

TABLE III. FALSE ALARM AND MISS DETECTION FOR DIFFERENT VALUES OF λ

Parameter	False Alarm Probability Averaged for 600 runs	Miss Detection Probability Averaged for 600 runs
λ =2	0.326	0.187
λ =1	0.043	0.4182
λ =0.5	0.041	0.43

Finally, we have used the Cumulative Distribution Function (CDF) to describe and show how both the false alarms and miss detection probability appears on the same graph.

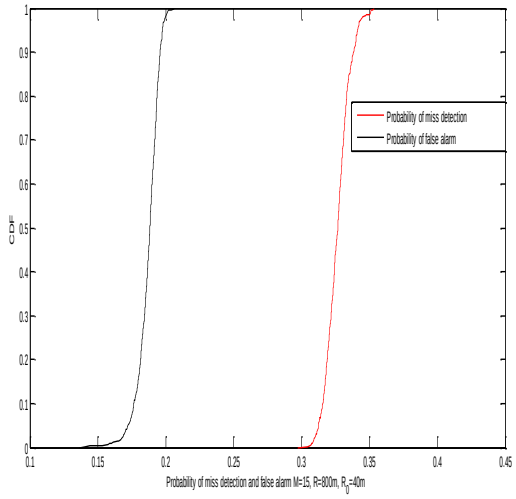

Figure 9. CDF of false alarm and miss detection probabilities

It is clear from Fig. 9 that the CDF plot is non-decreasing and right-continues function as must be meaning that the parameters and assumptions we have taken in our simulation are well-chosen and very close to the real-life values.

V. CONCLUSION AND FUTURE WORK

In this paper, we presented an analytical and experimental approach to obtain the PDFs of received powers at the secondary users due from malicious users and also due from the primary transmitter in a CR network by a set of malicious users.

The PDF obtained was used in Neyman-Pearson Composite Hypothesis Test to show the probability of false alarm in the network. Our results show that number of malicious users in the system has a great impact on the network causing the secondary users to suffer degradation in the quality of their communication due to the transmission from the malicious users. Also we show that there is a range of network radii in which PUEA are most successful.

The future work will be as a second stage of this work; in this stage, we will propose a security algorithm for transmitter verification scheme based on two parameters (distance and received signal power level) in order to identify the primary and malicious users; this kind of mitigation technique for PUEA does not rely on examination of PDF, but rather on localization of signal source.

ACKNOWLEDGMENT

As a research group, we are very thankful to Nick Riley and Kevin S. Paulson in Department of Engineering for their feedback and contributions in this work.

REFERENCES

[1] M. Buddhikot and K. Ryan, “Spectrum management in coordinated dynamic spectrum access,” IEEE DySpan, pp. 299–307, August 2005.

[2] FCC 03-322, “NPRM - Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing CR Technologies,” FCC, December 2003.

[3] Z. Jin, S. Anand, and K. Subbalakshmi, “Detecting primary user emulation attacks in dynamic spectrum access networks,” IEEE International Conference on Communications, Dresden, Germany, no. 4, pp. 13‑18, June 2009.

[4] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, “NeXt generation/dynamic spectrum access/CR wireless networks: A survey,” (Elsevier Journal), on computer Networks, vol. 50, no. 13, pp. 2127-2159, September 2006.

[5] Z. Kun, P. Paweczak, and D. Cabric, ”Reputation-based cooperative spectrum sensing with trusted nodes assistance,” IEEE Communications Letters, vol. 14, no. 3, pp.226-228, March 2010.

[6] T. Yucek, H. Arslan, ”A survey of spectrum sensing algorithms for CR applications,” IEEE Commun. Surveys Tutorials, vol.11, no.1, pp.116-130, First Quarter 2009.

[7] M. Kuroda, R. Nomura, and W. Trappe, ”A Radio-independent Authentication Protocol (EAP-CRP) for Networks of CRs,” 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, (SECON 2007), pp.70-79, 18-21, San Diego, California, USA, June 2007.

[8] D. Borth, R. Ekl, B. Oberlies, and S. Overby, ”Considerations for Successful CR Systems in US TV White Space,” in 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DySPAN 2008), pp. 1-5, 14-17 October 2008.

[9] R. Chen and J. Park, “Ensuring trustworthy spectrum sensing in CR networks,” Proceedings, IEEE Workshop on Networking Technol. for Software Defined Radio Networks (SDR), pp. 110–119, September 2006.

[10] R. Chen, J. M. Park, and J. H. Reed, “Defense against primary user emulation attacks in CR networks,” IEEE Journal on Selected Areas in Communications: Special Issue on CR Theory and Applications, vol. 26, no. 1, pp. 25–37, January 2008.

[11] S. Anand, Z. Jin, and K. P. Subbalakshmi, “An analytical model for primary user emulation attacks in CR networks,” Proceedings, IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks, pp. 35-40, October 2008.

[12] C. N. Mathur and K. P. Subbalakshmi, “Security issues in CR networks,” Chapter: Cognitive Networks: Towards Self-Aware Networks, John Wiley & Sons, Ltd, pp. 271–291, October 2007.

[13] G. Jakimoski and K. P. Subbalakshmi, “Denial-of-service attacks on dynamic spectrum access networks,” IEEE CogNets Workshop, IEEE International Conference on Communications (ICC) 2008, pp. 125-132, May 2008.

[14] S. Bhattacharjeea, S. Senguptab, and M. Chatterjee, ’’Vulnerabilities in CR networks’’ , The International Journal for the Computer and Telecommunications , Vol. 36, pp. 1387-1398 , October 2013.

[15] A. N. Mody, R. Reddy, T. Kiernan, and T.X. Brown, ”Security in CR networks: An example using the commercial IEEE 802.22 standard,” in IEEE Military Communications

 ISBN: 978-1-61208-403-9

Conference (MILCOM 2009), pp. 1-7, 18-21, Boston, MA, USA, 21 October 2009.

[16] N. R. Prasad, "Secure Cognitive Networks," in European Conference on Wireless Technology (EuWiT 2008), pp.107-110, 27-28 , Amsterdam, The Netherlands, October 2008.

[17] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Impact of Primary User Emulation Attacks on Dynamic Spectrum Access Networks," in IEEE Transactions on Communications, vol. 60, no. 9, pp. 2635-2643, December 2012.

[18] Z. Jin, S. Anand, and K.P. Subbalakshmi, "Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing, ACM SIGMOBILE Mob. Comput. Commun. 13 (2), pp. 74–85, November 2009.

[19] T. S. Rappaport, "Wireless communications: principles and practice," Prentice Hall Inc., New Jersey, June 1996.

[20] S. Anand, Z. Jin, and K. P. Subbalakshmi, "An Analytical Model for Primary User Emulation Attacks in CR Networks", Proceedings, IEEE Symposium of New Frontiers in Dynamic Spectrum Access Networks, July 2008.

[21] E. Orumwense, O. Oyerinde, and S. neney, ''Impact of Primary User Emulation Attacks on CR Networks'', International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), vol. 4, no. 1, ISSN 2039 – 5086 February 2014.

 ISBN: 978-1-61208-403-9