

Physical Layer Security in Cognitive Radio Networks

Detection and Mitigation of Primary User Emulation Attacks

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

Abstract—Cognitive Radio Networks (CR) is an advanced growing technique and a promising technology for the upcoming generation of the wireless networks in order to efficiently utilize the limited spectrum resources and satisfy the rapidly increasing demand for wireless applications and services. 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 present a comprehensive introduction to primary user emulation attacks, from the attacking rationale and its impact on CR networks, to detection and defense approaches. We have setup the system model using Matlab software, we have used the Neyman-Pearson composite hypothesis test NPCHT to obtain the hypothesis test and detect the PUEA. In order to secure CR networks against PUE attacks, we considered the power received at the secondary receiver.

Simulation results proved that using the NPCHT it is possible to keep the probability of success of PUEA low depends on the threshold value. 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; Probability Density Function (PDF); Primary User Emulation Attack (PUEA);

Nomenclature-

PU Primary User
SU Secondary User
P_t Primary User transmitting Power
P_m Malicious User transmitting power
d_p Distance between the primary transmitter & others
R Radius of the circular grid
R_o Radii of annular region
M number of malicious usres in the system

I. INTRODUCTION

THE Spectrum sensing and spectrum sharing are important functionalities of cognitive radio which enables the secondary users to monitor the frequency spectrum and detect vacant channels to use [1], it's also important to address the security and reliability issues in the cognitive radio.

An example of Cognitive radio network is the usage of unused spectrum (white spaces) in the television band where the TV transmitter becomes a primary transmitter, 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 cognitive radio network is to identify empty spectral bands (white spaces) and once these white spaces have been identified, Cognitive radio nodes opportunistically utilize these unoccupied bands of spectrum by wirelessly operating across them while simultaneously avoiding interference with the primary users [2]. In a cognitive radio 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 cognitive radio networks is considered as a Primary User Emulation Attack (PUEA) [3].

Therefore, we can define Primary User Emulation Attack (PUEA) as an attack in cognitive radio 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]. The presence of PUE attack 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]. Among these, the energy based detection is more popular and easier to implement.

Mahmod Ammar, School of Engineering, University of Hull, Hull, UK,(E-mail: M.A.Ammar@2011.hull.ac.uk)

Nick Riley, School of Engineering, University of Hull, Hull, UK.
Meftah Mehdawi, School of Engineering, University of Hull, Hull, UK.
Anwar Fanan, School of Engineering, University of Hull, Hull, UK.
Mahsa Zolfaghari, School of Engineering, University of Hull, Hull, UK.

• *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 [5], [6].

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 [7], [8].

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 [9].

• *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[10].
- 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[10].
- 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.

The rest of the paper is organized as follows. In section II, we present the system model and all assumptions made to formulate the problem. Section III gives a detailed explanation of the Probability Density Function of the Received Signals and detection approach. Section IV, presents discussion and test results while section V concludes the paper and set the future work.

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 below

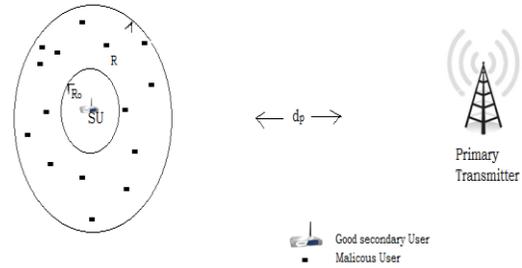
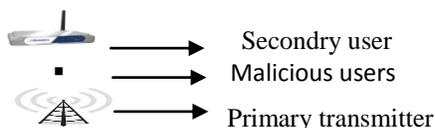


Fig. 1 Cognitive Radio Network Model

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[11]. We design a NPCHT to obtain a criterion for making this decision. To perform the analysis, the assumptions below are taken:

- The distance between primary transmitter & all the users is $dp=120\text{Km}$.
- There are M malicious users in the system.
- The locations of malicious users are uniformly distributed in the circular grid of radius $R=500\text{m}$ as our simulation shows in fig. 2 below when $M=30$.

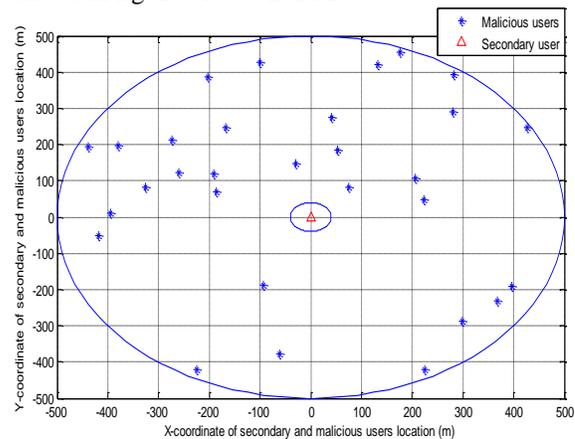


Fig. 2 Simulation result of malicious users distributed randomly around the secondary user located at coordinate (0,0).

- The primary transmits at a power $P_t = 120\text{ KW}$ while the malicious users transmit at a power $P_m = 5\text{ W}$. All the values of the system parameters we have used are in Table 1 below.
- The primary transmitter co-ordinates are fixed at a point (r_p, θ_p) 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 $R_0=40\text{m}$ 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 R_0 from the secondary becomes too large to create PUEA [11].

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
R ₀ : Radii of annular region	40 m
M : Number of malicious users in the system	10,15,30
P _t : Primary transmission power	120 KW
P _m : Malicious transmission power	5 W
σ _p : Variance of Primary users	8 dB
σ _m : 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_p^2 and σ_m^2 , respectively [12].
- 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 NPCHT.

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 cognitive radio networks and also investigate the impact of PUEA in the network.

We consider M malicious users located at co-ordinates (r_j, θ_j) $1 \leq j \leq M$. Since the position of the j^{th} malicious user is uniformly distributed in the annular region between R_0 and R, r_j and θ_j are statistically independent $\forall j$. The pdf of r_j , $p(r_j) \forall j$ is given by

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

While θ_j is uniformly distributed in $(-\pi, \pi) \forall j$ [13]. The received power at a secondary user from the primary transmitter, $P_r^{(p)}$ is given by $P_r^{(p)} = P_t d_p^{-2} G_p^2$

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

as

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

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

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

Where d_j is the distance between the j^{th} malicious user and the secondary user and G_j^2 is the shadowing between the j^{th} malicious user and the secondary user.

B. Detecting PUEA using Neyman-Pearson Criterion

We have used the two hypothesis 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 [14]:

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 $\Lambda = P^m(\chi) / P^{\text{Pr}}(\chi)$

Where $P^{\text{Pr}}(\chi)$ 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

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

$\Lambda \geq \lambda \implies D2$: 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.

In terms of conditional densities these probabilities can be expressed as

$$P\{D2|M1\} = \int_{\Lambda \geq \lambda} p^{(\text{Pr})}(x) dx$$

$$P\{D1|M2\} = \int_{\Lambda \leq \lambda} p^{(m)}(x) dx$$

C. Decision Rule

In Fig. 3 below 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. We compare the decision rule with the threshold value; Lambda (λ) and the miss probability and probability of false alarm are calculated accordingly[15].

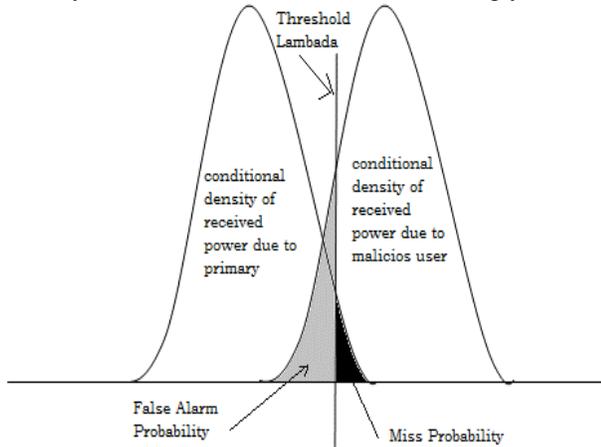


Fig. 3 the Decision Rule

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 Table 2.

TABLE II
SYSTEM SIMULATION PARAMETERS

Parameter	d_p	R	R_0	M	P_t	P_m	σ_p	σ_m
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 result 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.

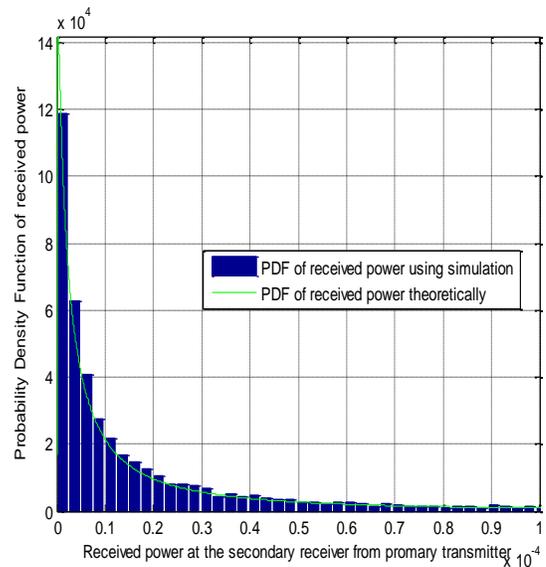


Fig. 4 PDF of the received power deu to the primary transmitter

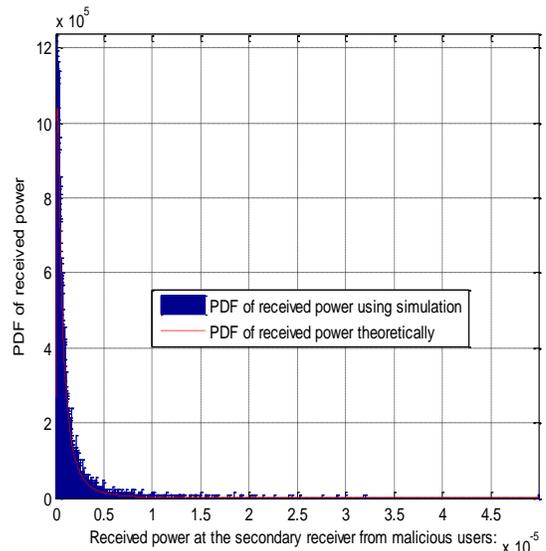


Fig. 5 PDF of the received power due to the malicious users

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

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 below 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 R_0 , 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 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 below, 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.

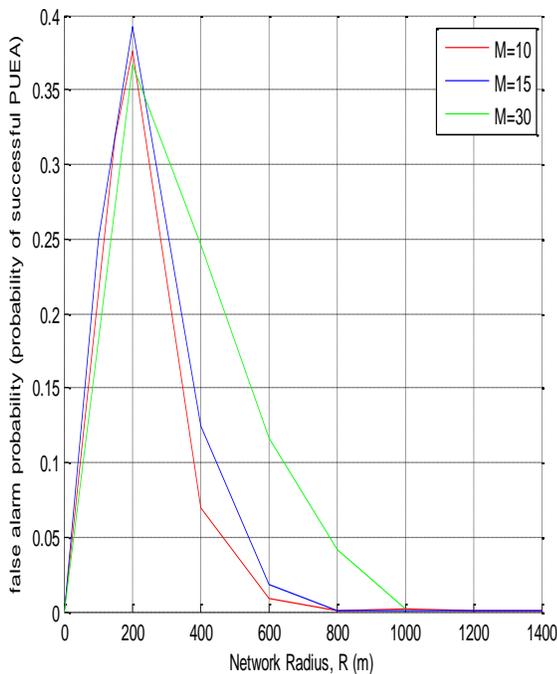


Fig. 6 false alarm probability vs. network Radius R

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. $\lambda=2$. 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 $R_0=40m$, primary transmitter power $P_t=120Kw$, malicious transmitter power $P_m=5w$, $\sigma_m = 5.5dB$, $\sigma_p = 8dB$.

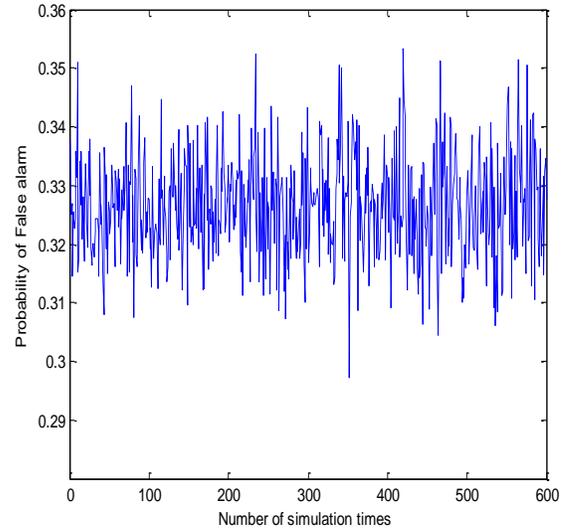


Fig. 7 probability of successful PUEA (False e Alarm)

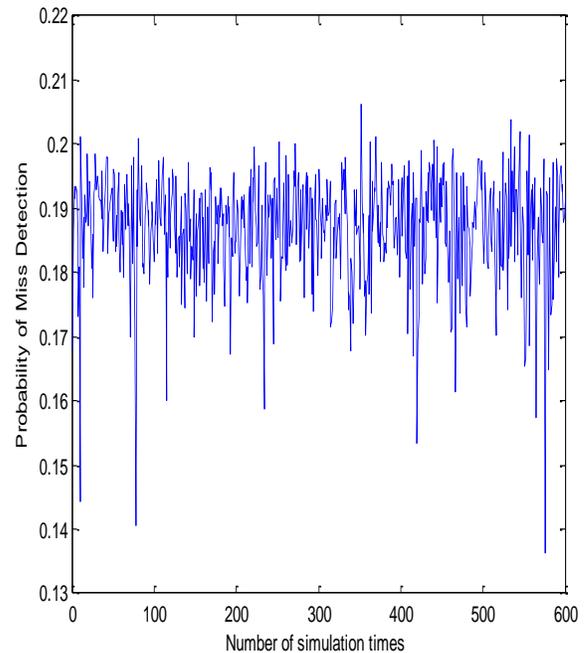


Fig. 8 Probability of miss detection

As we can see from the experimental 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.

We have done the simulation with different values of λ as shown in Table 3 below 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 (Neyman Pearson's Composite Hypothesis

Test) only allows a threshold to be set on either false alarm or miss detection probabilities.

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
$\lambda = 2$	0.326	0.187
$\lambda = 1$	0.043	0.4182
$\lambda = 0.5$	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.

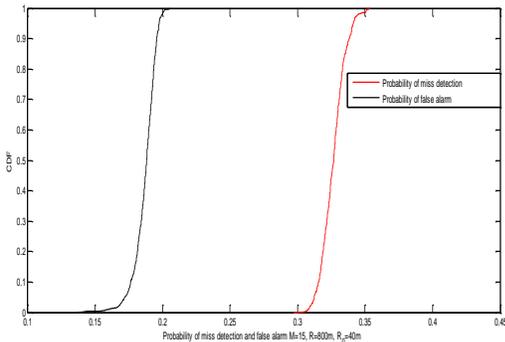


Fig. 9 CDF of false alarm and miss detection probabilities

It is clear from fig. 9 above 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 cognitive radio 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.

VI. 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, K. Ryan, Spectrum management in coordinated dynamic spectrum access, in: Proc. of IEEE DySpan, pp. 299–307, 2005.
- [2] FCC 03-322, “NPRM - Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies,” FCC, Dec. 2003.
- [3] Z. Jin, S. Anand, and K. P. Subbalakshmi, “Detecting primary user emulation attacks in dynamic spectrum access networks,” In Proceedings of the IEEE International Conference on Communications, Dresden, Germany, Jun 2009. No. 4, pp. 13–18, 1999.
- [4] I. F. Akyildiz, W. Y. 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, Sept 2006, pp. 2127-2159,
- [5] R. Chen and J. M. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” Proceedings, IEEE Workshop on Networking Technol. for Software Defined Radio Networks (SDR) 2006, pp. 110–119, Sep. 2006.
- [6] 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. <http://dx.doi.org/10.1109/JSAC.2008.080104>
- [7] 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.
- [8] C. N. Mathur and K. P. Subbalakshmi, “Security issues in cognitive radio networks,” Chapter: Cognitive Networks: Towards Self-Aware Networks, John Wiley & Sons, Ltd, pp. 271–291, 2007.
- [9] 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, May. 2008.
- [10] Shameek Bhattacharjee, Shamik Sengupta, Mainak Chatterjee, “Vulnerabilities in cognitive radio networks” ,The International Journal for the Computer and Telecommunications , Vol. 36, October 2013, .pp. 1387-1398, online <http://www.journals.elsevier.com/computer-communications>, Access date 26-11-2014.
- [11] 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, 2012. <http://dx.doi.org/10.1109/TCOMM.2012.071812.100729>
- [12] Z. Jin, S. Anand, K.P. Subbalakshmi, Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing, ACM SIGMOBILE Mob. Comput. Commun. 13 (2) (2009) 74–85. <http://dx.doi.org/10.1145/1621076.1621084>
- [13] T. S. Rappaport, Wireless communications: principles and practice. Prentice Hall Inc., New Jersey, 1996.
- [14] 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.
- [15] Efe Orumwense, Olutayo Oyerinde, Stanley neny, “Impact of Primary User Emulation Attacks on Cognitive Radio Networks”, International Journal on Communications Antenna and Propagation (I.Re.C.A.P.), Vol. 4, N. 1 ISSN 2039 – 5086 february 2014.