INVESTIGATION OF PUEA IN COGNITIVE RADIO NETWORKS USING ENERGY DETECTION IN DIFFERENT CHANNEL MODEL

[1]Walid. R. Ghanem, [2]Mona Shokair and [3]MI Dessouky

[1, 2, 3] Department of electronic and electrical communication, Faculty of electronic engineering, Menouf, Egypt

ABSTRACT

Primary User Emulation Attack (PUEA) is one of the major threats to the spectrum sensing in cognitive radio networks. This paper studies the PUEA using energy detection that is based on the energy of the received signal. It discusses the impact of increasing the number of attackers on the performance of secondary user. Moreover, studying how the malicious user can emulate the Primary User (PU) signal is made. This is the first analytical method to study PUEA under a different number of attackers. The detection of the PUEA increases with increasing the number of attackers and decreases when changing the channel from lognormal to Rayleigh fading.

KEYWORDS:

Cognitive Radio, Primary User Emulation Attacks (PUEA), energy detector.

1. INTRODUCTION

Cognitive Radio Networks (CRNs) are a new technology that uses the unused spectrum to enable much higher spectrum efficiency. The concept of cognitive radio is introduced in [1-6], where secondary (unlicensed) users utilize the licensed frequencies while the primary user (licensed) user is absent. To make this utilization, sensing process is needed to know the situation of the primary user. If the secondary user senses that primary user do not transmit, they can use the channel to transmit, otherwise, secondary user detect the presence of the primary user it stops transmitting. Some problems will be found during this process. One of these problems is made due to many attacks such as a denial of service attack, false sensing data report attack, and primary user emulation attack. The last one of attack is a serious problem, which is presented by R. Chen in [7]. When the primary user does not use the spectrum, a malicious user or attacker sends a signal whose characteristics emulates that of the primary user therefore the secondary user may think that this signal is from the primary user and thus prevented from accessing the CRNs. Recently, Primary user emulation attack (PUEA) has been studied in many researches. R. Chen proposed to use the location of the primary user to identify the primary user emulation attack [7]. S. Annand made an analytical model based on Fenton's approximation and Markov inequality [8]. Z. Jin et al. Presented a Neyman–Pearson composite hypothesis test [9] and a Wald's sequential probability ratio test [10] to detect PUEA. Z. Chen showed how the attacker emulated the primary user signal to confuse the secondary user and use an advanced strategy called variance detection to mitigate the effect of an attacker using the difference between the communication channel of PUEA and primary user [11]. C. Chen et al made a joint position verification method to enhance the positioning accuracy [12]. Moreover, C. Chen et al discussed

the cooperative spectrum sensing model in the presence of PUEA and established a scheme to maximize the detection probability of PU [13]. Feijng Bao et al studied the PUEA with the motion secondary users in cognitive radio network and using a hybrid method based on Energy Detection (ED) and Variance Detection [14]. ED is one technique from some techniques depending on the sensing which is the basis of cognitive radio network.

Another technique such as matched filters (MF), cyclostationary detection, covariance detection, Eigen value based detection, wavelet edge detection. All existing PUEA detection used ED due to its simplicity and have no prior information about the detecting signal.

In this paper, analytical method is used to study PUEA under a different number of attackers when the attack strategy is used by each attacker, which hasn't done before. In this system, no cooperation is considered between the attackers. Therefore, each attacker wants to fool the SU with transmitting a signal whose characteristics mimics the primary user signal. The victim user (SU) receives signals from PU and the attacker and makes its decision.

The remainder of this paper is structured as follows. In Section 2, the problem formulation is introduced. In Section 3, an analytical model for energy detection strategy against primary user emulation attacks for many numbers of attackers under the strategy used by each attacker. The numerical and simulation results will be made in Section 4. Finally, conclusions will be done in Section 5.

2. PROBLEM FORMULATION

2.1. SYTEM MODEL

The network model shown in Fig 1. where the attackers and secondary user (victim) are located in circular grid. The primary user is a TV tower located at a distance of dp from the CRN and all users position is fixed in the network. Each attacker wants to fool the victim by transmitting a signal whose characteristic emulates that of the primary user. The victim listens to the channel to distinguish between the signal coming from the primary user or the attacker.

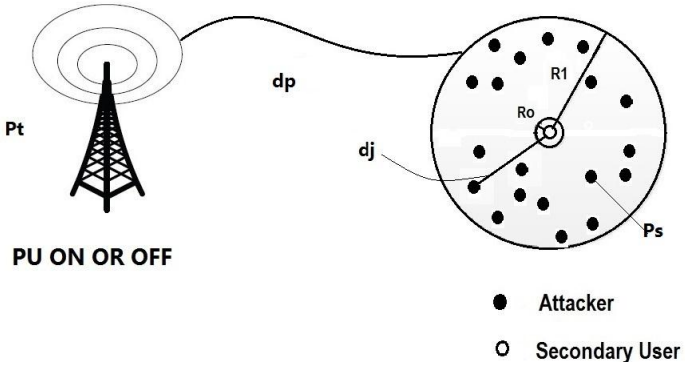


Fig. 1 System model of the CRN [8]

The following assumptions are considered for proposed model specification:

1. d_J is the distance between the J^{th} attacker and the victim, the target region in which each Attacker wants to fool the victim is a loop of radius R_o and R_1.
2. The primary transmitter located at a distance of d_P from the Cognitive Radio network.

3. The primary user transmits a power of P_t and each attacker transmit an adaptive power of $P_{s.}$

4. The signal from primary and the attacker undergoes path loss and, lognormal, or fading.

5. At the victim the free space propagation model is considered for the signal from primary and two ray ground model for the signal from the attacker, respectively. The received signal at victim from the primary is proportional to d_P^{-2}, and from the attacker is proportional to d_J^{-4} [9].

6. The shadowing random variable for the primary transmitter is[15]

$$G_p = 10^{\beta P/10} = e^{a\beta P} \tag{1}$$

where $a=\frac{\ln 10}{10}$ and $\beta_p \approx N(0,\ \sigma_P^2)$ follows a normal distribution with zero mean and variance equal to σ_P^2 .

7. The shadowing random variable for the attacker is [15]

$$G_s = 10^{\beta_S/10} = e^{a\beta_S} \tag{2}$$

Where $a=\frac{\ln 10}{10}$, $\beta_S \equiv N(0,\ \sigma_s^2)$ follows normal distribution, with zero mean and variance equal to σ_s^2 .

8. NO cooperation is consumed between the attackers.

2.2. Performance Metrics Parameters

This section discusses the metric parameter for the modal performance measurement. Most existing work on cognitive sensing focuses on performing a hypothesis testing to decide the presence of the primary user [11]. In this paper, the interaction between the attacker and the victim are discussed. As a result, in our work a victim (or a defender) performs a hypothesis testing to decide whether a signal is from the primary user or from the attacker,
As shown in the following two hypotheses [11].

Ho: the signal is from the primary user
H1: the signal is from the attacker

In the hypothesis testing, two matrices are used to demonstrate the performance of strategies taken by the attacker and the victim [11].

Probability of false positives (PFP) or (probability of false alarm (PFA)):

When the signal is from the primary user, the probability that the victim falsely identifies as the signal from the attacker is expressed as [14],

$$P_{FP} = \Pr(\mathrm{H}_1 \setminus H_0) \tag{3}$$

If this case happens, the victim will attempt to access the network and cause interference to the primary user. Then the victim may be punished as an attacker user. Hence the victim may use a strategy to make PFP (PFA) as small as possible while the attacker want to make PFP (PFA) as large as possible [11].

Probability of false negatives (PFN) or the probability of misdetection (PMD):
When the signal is for the attacker, the probability that the victim falsely classifies it as from the primary user is defined as [11],

$$P_{FN} = \Pr(H_0 \setminus H_1) \tag{4}$$

If this case happens, the victim will vacate the spectrum unnecessarily or give up accessing the network, although the spectrum band is vacant, and the attacker launches a successful PUEA and take the spectrum resource.

Another widely matrices is the probability of detection (PD) [14].

$$P_D = 1 - P_{FN} = \Pr(H_1 \setminus H_1) \tag{5}$$

The victim should take a strategy to make P_{FN} (P_{MD}) as small as possible where the attacker aims to make P_{FN} or probability of miss detection (P_{MD}) as large as possible.

3. ANAYLTICAL MODEL

3.1. The attack strategy

In this part we describe by the equation the attack strategy used by the attacker. Each attacker wants to fool the victim (SU) by transmitting a signal whose characteristics emulates that of the primary user to make P_{FN} and P_{FP} as large as possible, in [11] a mean-field approach is used to derive a solution of P_s and this method focus on the average of the received power Ignoring fluctuations this approach describe in Fig.2. Where an attacker receive a power from the primary user and transmit the emulating power to the secondary user.

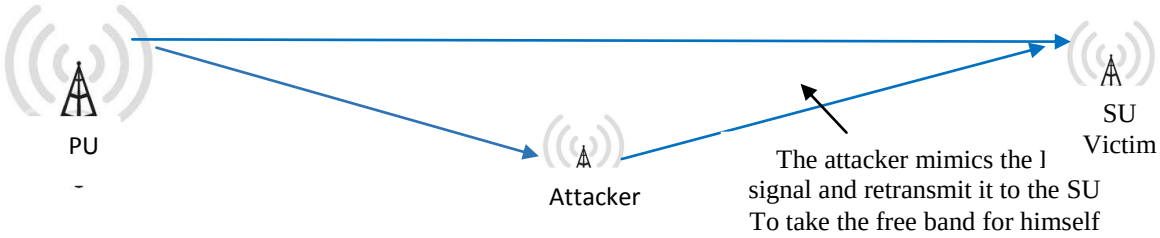


Fig.2 The attacker strategy

The received power at the victim from primary user, $P_r^{(v)}$, is denoted as follows[9]:

$$P_r^{(v)} = P_t \; d_p^{-2} G_p = P_t \, d_p^{-2} e^{\alpha \beta p} \tag{6}$$

Where G_p is the shadowing random variable from the primary user to the victim
The received power at victim from each of the j[th] attacker is given as [9],

$$P_r^{(sj)} = Ps_j \, d_{sj}^{-4} G_s = Ps_j \, d_{sj}^{-4} e^{\alpha \beta_s} \tag{7}$$

Where G_s is the shadowing random variable from the primary user to the j[th] attackers?
The Moment generating function $\Phi(t)$ of a random variable β is expressed as [15],

$$\Phi(t) = E(e^{t\beta}) = e^{\frac{1}{2}\sigma^2 t^2} \quad (8)$$

The mean of $P_r^{(v)}$ that given by (3) and $P_r^{(s)}$ that given by (4)

$$E(P_r^{(v)}) = P_t d_p^{-2} E(G_p) = P_t d_p^{-2} E(e^{a\beta p}) = P_t d_p^{-2} e^{\frac{1}{2}a^2\sigma p^2} \quad (9)$$

$$E(P_r^{(sj)}) = P_{sj} d_{sj}^{-4} E(G_s) = P_{sj} d_{sj}^{-4} E(e^{a\beta s}) = P_{sj} d_{sj}^{-4} e^{\frac{1}{2}a^2\sigma s^2} \quad (10)$$

The attacker emulates the primary user signal under the condition of $E(P_r^{(sj)}) = E(P_r^{(v)})$ [11]
Thus the power of each attacker is expressed as,

$$P_{sj} = P_t \frac{d_{sj}}{d_p} e^{\frac{1}{2}a^2(\sigma_P^2 - \sigma_s^2)} \quad (11)$$

3.2. The Energy Detection Defense Model

In this part the mathematical analysis of probability of false Positive (P_{FP}) that is given by (1) and probability of false negative that given by (2) will be made.
The energy detection is used to defense the PUEA as follows [11]:

$$\text{IF} \mid p_r - u_r \mid \leq k\sqrt{\sigma_r^2}: \quad \text{The signal from the primary user } (H_0) \quad (12)$$

$$\text{IF} \mid p_r - u_r \mid > k\sqrt{\sigma_r^2}: \quad \text{The signal from the malicious user } (H_1) \quad (13)$$

Where P_r is the received power at the victim , and k (k > 0) is a constant that controls the threshold of determination and is called the threshold factor.

The mean of the received signal is given by

$$u_r = E(P_r^{(v)}) = P_t d_p^{-2} e^{\frac{1}{2}a^2\sigma_P^2} \quad (14)$$

The variance of the received power from primary user is given by:

$$\sigma_r^2 = Var(P_r^{(v)}) = P_t^2 \, d_p^{-4} e^{a^2\sigma_P^2} (e^{a^2\sigma_P^2} - 1) \quad (15)$$

Therefore the root mean square is given by

$$\sigma_r = u_r\sqrt{e^{a^2\sigma_P^2} - 1} = u_r c \quad (16)$$

Where $c = \sqrt{e^{a^2\sigma_P^2} - 1}$

When the received signal is from the primary user is given by (3),

$$P_r^{(v)} = P_t\, d_p^{-2} G_p = P_t\, d_p^{-2} e^{a\beta p} \tag{17}$$

From the determination criteria from (12) and (13), the probability of false positives can be calculated as [11]:

$$p_{FP} = pr(|p_r^{(v)} - u_r| \geq k\,\sigma_r) \tag{18}$$

$$p_{FP} = pr(p_r^{(v)} > (1+kc)u_r) + pr(p_r^{(v)} < (1-kc)u_r) \tag{19}$$

When $kc < 1$

$$p_{FP}=pr(\frac{\beta_P}{\sigma_P} > \frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1+kc)) + pr(\frac{\beta_P}{\sigma_P} < \frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1-kc)) \tag{20}$$

$$p_{FP}=1+Q(\tfrac{1}{2}a\sigma_p + \tfrac{1}{a\sigma p}\ln(1+kc)) - Q(\tfrac{1}{2}a\sigma_p + \tfrac{1}{a\sigma p}\ln(1-kc)) \tag{21}$$

If $kc \geq 1$,

$$p_{FP}=pr(\frac{\beta_P}{\sigma_P} > \frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1+kc)) = Q(\frac{1}{2}a\sigma_p + \frac{1}{a\sigma_p}\ln(1+kc)) \tag{22}$$

Where $Q(\tau) = \int_{\tau}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}} dx$

Note that P_{FP} only depends on σ_p and k and independent on P_t, d_p and α.

On the other hand, when the signal from the attacker,

The Probability of false negative is defined as,

$$P_{FN} = \Pr(|p_r^{(s)} - ur| \leq k\,\sigma_r) \tag{23}$$

$$P_{FN}=\Pr(1-kc \leq \frac{P_r^{(s)}}{ur} \leq 1+kc) \tag{24}$$

Where

$$P_r^{(s)} = \sum_{j=1}^{M} P_{sj} d_j^{-4} G \tag{25}$$

Where P_{sj} the power from the j attacker and dj is is the distance between the j attacker and the victim, G is the shadowing between each attacker and victim. Since there is no cooperation between the attackers therefore each attacker wants to conflict the SU with transmitting power with mean equal to the mean of the primary signal.

Thus

$$P_{sj} = P_t \frac{d_{sj}}{d_p} e^{\frac{1}{2}a^2(\sigma_p^2 - \sigma_s^2)} \tag{26}$$

$$\frac{p_r^{(s)}}{u_r} = \frac{\sum_{j=1}^{M} P_t \left(\frac{d_{sj}^{\,4}}{d_p^{\,2}}\right) e^{\frac{1}{2}a^2(\sigma_p^2-\sigma_s^2)} d_{sj}^{\,4} e^{a\beta_j}}{P_t\, d_p^{-2}} = \sum_{j=1}^{M} e^{-\frac{1}{2}a^2\sigma_s^2} e^{a\beta_j} \tag{27}$$

$$p_{FN} = pr(1-kc \le \sum_{j=1}^{M} e^{-\frac{1}{2}a^2\sigma_s^2} e^{a\beta_j} \le 1+kc) \tag{28}$$

By taking Ln for both sides.

$$p_{FN} = pr(\frac{1}{2}a^2\sigma_s^2 + \ln(1-kc) \le a\sum_{j=1}^{M}\beta_j \le \ln(1+kc) + \frac{1}{2}a^2\sigma_s^2) \tag{29}$$

$$p_{FN} = pr(\frac{1}{2}a^2\sigma_s^2 + \ln(1-kc) \le a\sum_{j=1}^{M}\beta_j \le \ln(1+kc) + \frac{1}{2}a^2\sigma_s^2) \tag{30}$$

Where $\beta_j \cong N(0,\sigma_s^{\,2})$, the sum of normal variable is also normal with mean zero and variance equal to $\sum_{j=1}^{M}\beta_j = \beta_T$ where β_T is the normal value with mean equal zero and variance $= M\sigma_s^{\,2}$.

The probability of false negative can be expressed as

$$p_{FN}=pr(\tfrac{1}{2}a^2\sigma_s^2 + \ln(1-kc) \le a\beta_T \le \ln(1+kc) + \tfrac{1}{2}a^2\sigma_s^2) \tag{31}$$

by dividing by $\sqrt{M}.\sigma_s$

$$p_{FN}=pr(\frac{a\sigma_s^2}{2\sqrt{M}} + \frac{\ln(1-kc)}{a\sigma_s.\sqrt{M}} \le \frac{\beta_T}{\sqrt{M}.\sigma_s} \le \frac{\ln(1+kc)}{a\sigma_s\sqrt{M}} + \frac{a\sigma_s^2}{2\sqrt{M}}) \tag{32}$$

The probability of false negative as a function of false negative

$$p_{FN}=Q(\frac{a\sigma_s^2}{2\sqrt{M}} + \frac{\ln(1-kc)}{a\sigma_s.\sqrt{M}}) - Q(\frac{\ln(1+kc)}{a\sigma_s.\sqrt{M}} + \frac{a\sigma_s^2}{2\sqrt{M}}) \tag{33}$$

When kc≥1

The probability can be given by,

$$p_{FN}=pr(\frac{\beta_T}{\sqrt{M}.\sigma_s} \le \frac{\ln(1+kc)}{a\sigma_s.\sqrt{M}} + \frac{a\sigma_s^2}{2\sqrt{M}}) \tag{34}$$

The final expression of the probability of false negative is given by

$$p_{FN}=1-Q(\frac{\ln(1+kc)}{a\sigma_s.\sqrt{M}} + \frac{a\sigma_s^2}{2\sqrt{M}}) \tag{35}$$

Note that P_{FN} is depending on σ_p, σ_s and k and M the number of malicious users. It is independent on P_t, d_p, d_j and α.

3.3. Energy Detection Scheme

Figure 3 shows the ED defense scheme, first the system will be initialize by defining the primary user, secondary user, the attacker and also the channel models that used. These channels are AWGN and Rayleigh fading. Then the SU performs spectrum sensing to distinguish that the signal from the primary user or attacker and that based on some threshold that define above in (12), (13).

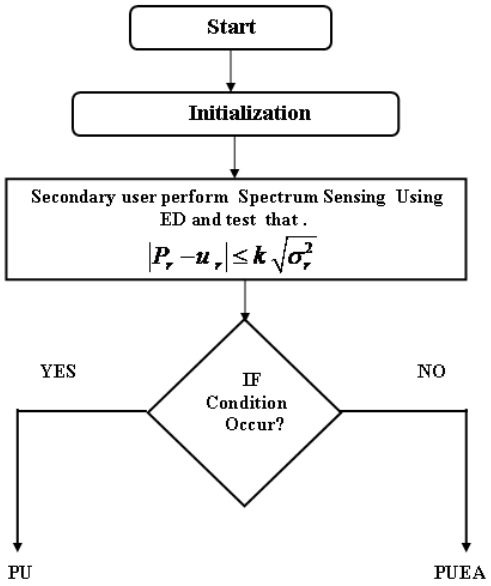


Fig.3 Flow chart of ED method defense strategies

4. SIMULATION RESULTS

The values of the system simulation parameters are listed in Table 1 [14].

Table 1 SIMULATIONS PARAMETER.

Parameter	Value	Parameter	Value
d_p	10Km	R_o	30m
P_t	100KW	R_1	500
σ_p^2	8,4	σ_s^2	4,8,12

In this section, The simulations for the proposed models shown if Fig.1 will be validated and the simulation parameter given in table 1. First, consider a system with fixed primary user at a distance of d_p from the CRN, and transmit power P_t The shadowing random variable from the primary transmitter is given by equation (1)

The target region of the victim is loop with inner radius R_o and outer radius R_1=, the attackers located at any distance $R_o \le R \le R_1$ and each attacker transmit with adaptive power P_s that give by (8) ,the shadowing random variable from the attacker is given by (2) , the victim is using energy detection method. The Rayleigh fading channel from the primary user to the CRN is considered to be a two paths channel. The P_{FA} with P_D is plotting with the variability of the threshold value k, we use monte carol with 100000 run times for every value of the threshold value

Figure 4 gives the probability density functions (PDFs) of signal power received by the victim when the primary user and the attacker transmitting under the lognormal channel model. The attacker applies the advanced strategy that is explained above from this figure we conclude that, when the number of attackers increase, the PDF of the received signal will differ from that of the primary user signal and the mean of the received signal is differ, thus the performance detection increases and the secondary user easy identifies the signal that from PU or from the attacker.

Fi
I
th
lo
1t

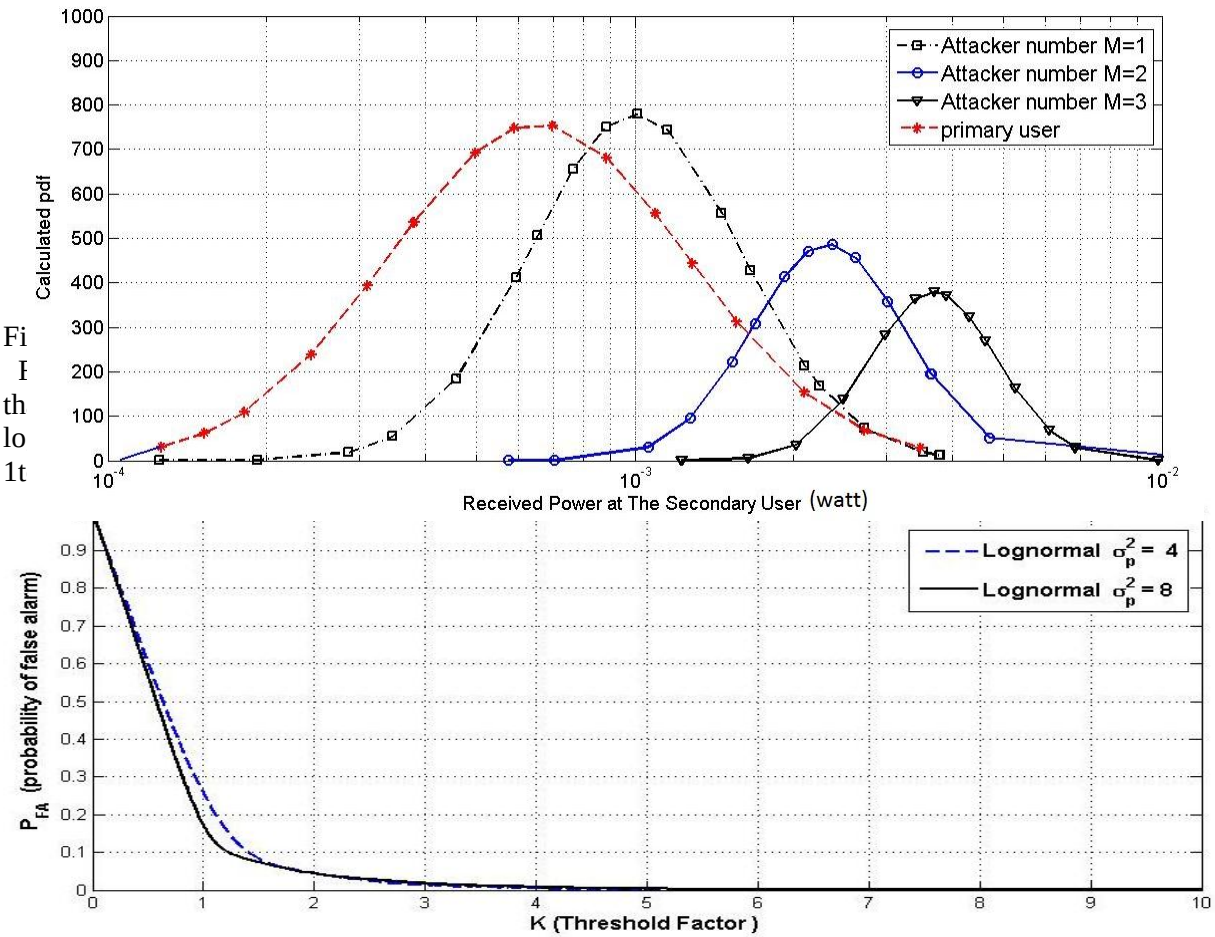


Fig.5 The impact of k on the probability of false alarm (P_{FA}), when $\sigma_p^2 = 8$, $\sigma_p^2 = 4$ under lognormal channel

Fig.6 gives the relation between the threshold factor k and the probability of detection (P_D) that give by equation (5), when the PUEA method is depend on the energy detection method under lognormal at different number of attackers and different variance of the channel. By varying the threshold factor value k from 0 to 10 the probability of detection decrease from 1 to 0. The simulation results shows that increase the number of attackers increase the probability of detection(P_D) , also change the variance from $\sigma_s^2 = 4$ to $\sigma_s^2 = 8$ decrease the detection probability.

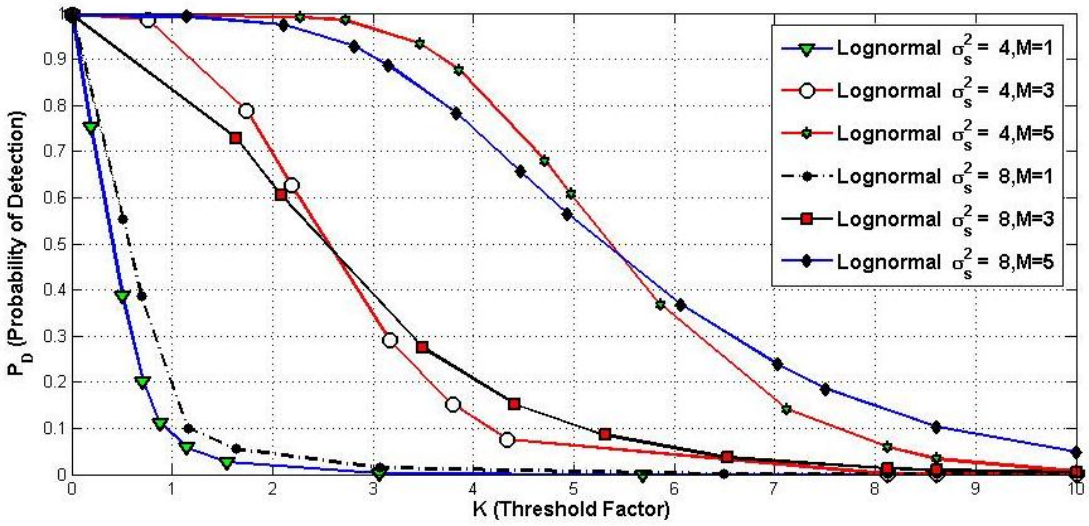
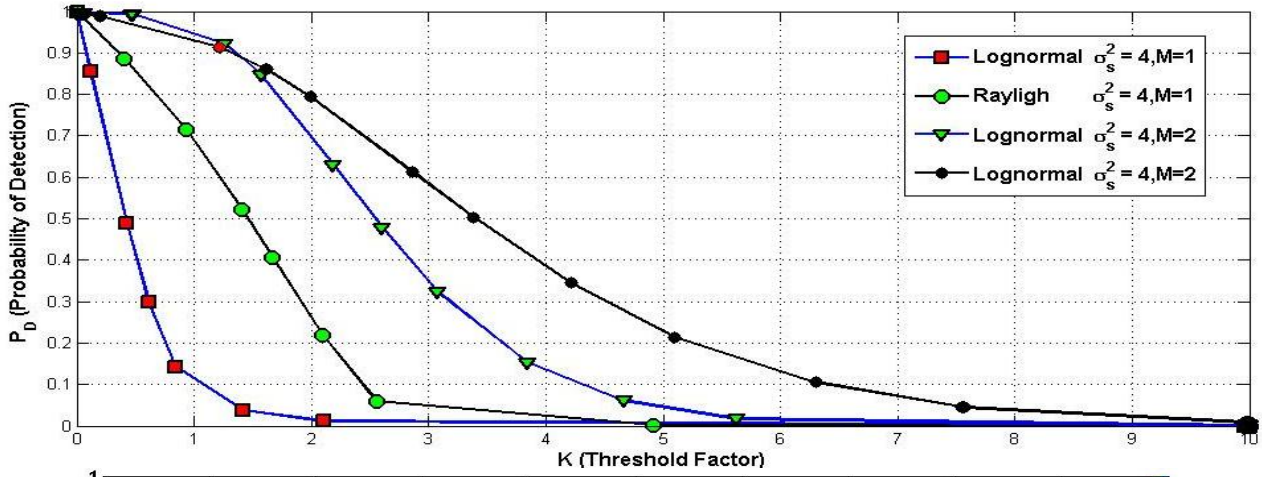
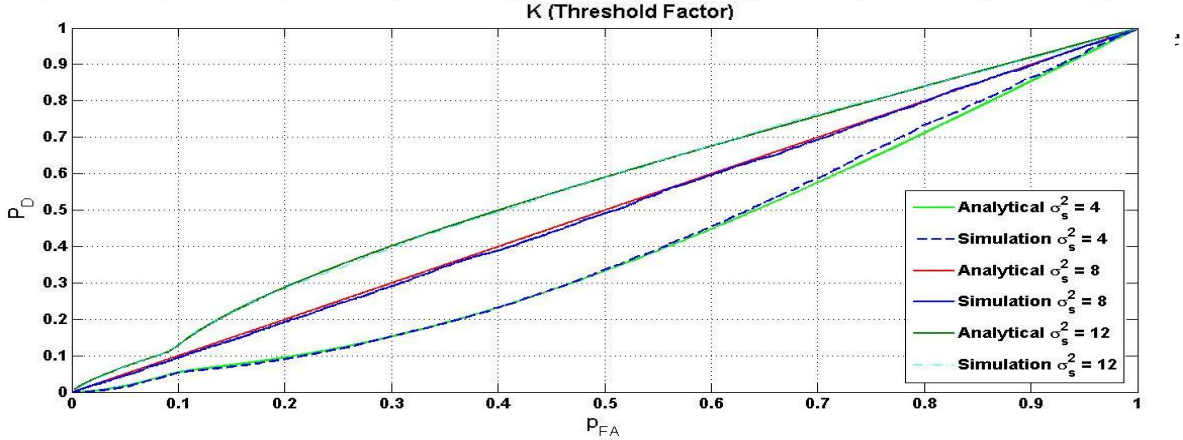


Fig.6 The impact of K on the probability of detection (P_D) when $\sigma_p^2 = 8$.

Fig.7 shows the relation between the threshold factor k and the probability of detection (P_D) when the PUEA method depends on the energy detection method under lognormal and Rayleigh Fading channel at different number of attackers. The simulation shows that the probability of detection is increased when the channel is changed from Lognormal to Rayleigh under the same number of attackers.





With $\sigma_p^2 = 8$ and different σ_s^2, M=1.

Fig.9 shows the ROCs at a different number of attackers with different channel parameters from the victim to the attacker under the lognormal channel for both the primary user of victim channel and from the attacker to victim channel. The performance detection increases with increasing the number of attackers. The performance detection when $\sigma_p^2 = \sigma_s^2 = 8$ has a bad detection at the same number of attackers. At P_{FA}=0.5 the P_D=0.7 and 1 for the number of attacker M=2 and 3, the probability of detection is increase by 30% when the number of attacker change from 2 to 3.

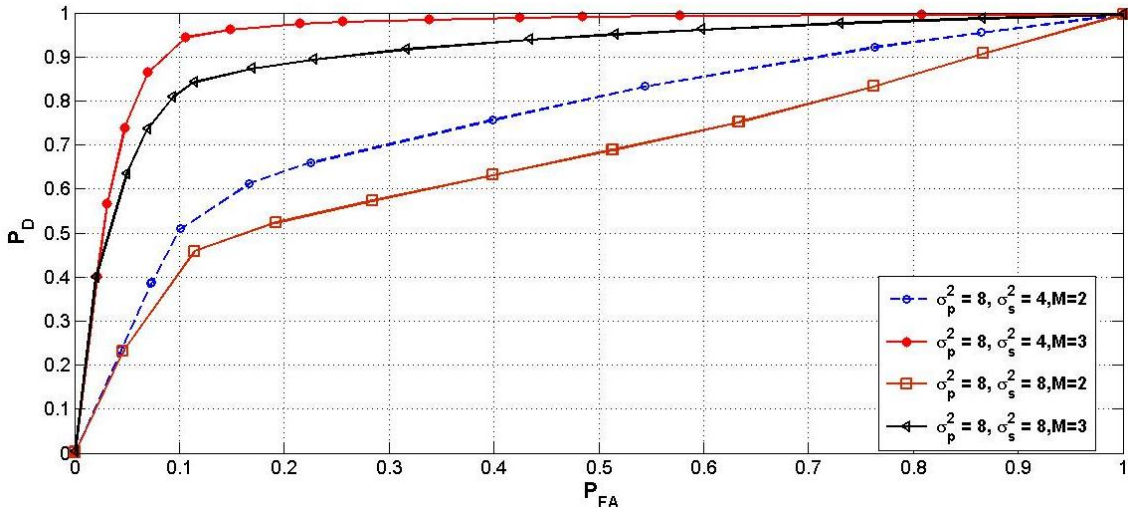
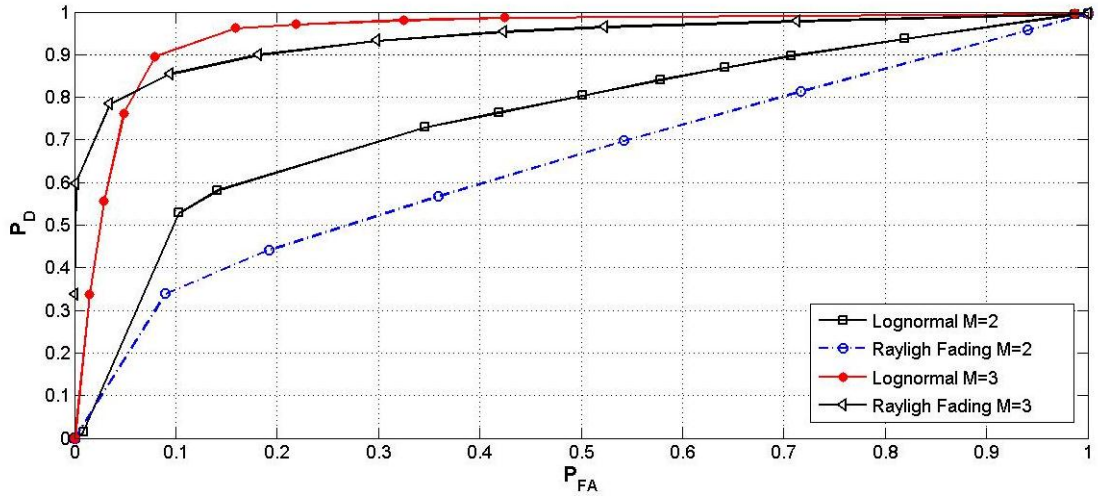


Fig.9 Receiver operating characteristics (ROCs) of energy detection with different channel parameter under a different number of attackers

Fig.10 shows the ROCs of energy detection under lognormal and Rayleigh fading from the primary user to the victim, and lognormal from the attacker to the victim, the performance detection of the victim gives small P_D for the same value of the P_{FA} for the same number of malicious users therefore the detection is worse for the Rayleigh fading channel. At P_{FA} =0.5 the probability of detection equal to 0.65 and 0.8 for Rayleigh and Lognormal at M=2 so the performance decrease by 15% when the channel change from lognormal to Rayleigh fading.



The PUEA is one of the major threats to the spectrum sensing in CRN, and it was degrading the performance of the CRN. In this paper, a CRN Network model consists of a primary user, secondary user and many numbers of attackers. Channel models such as lognormal shadowing and Rayleigh fading are used. In this model each attacker applies an attack strategy to fool the victim with emulating the primary user signal. Then the energy detection method is applied to mitigate the effect of the attackers. The analysis and simulation of the system shows that the performance of the detection gives worse when changing the channel from lognormal to Rayleigh fading and get better with the increase number of attackers.

6. REFERANCES

[1] J. Mitola & G. Q. Maguire Jr(1999) " Cognitive Radio: Making Software Radios More Personal", *IEEE Personal Communications*, Vol. 6, No. 4, pp. 13–18.

[2] Hefdhallah Sakran, Mona Shokair, El-Sayed El-Rabaie & Atef Abou El-Azm(2010) "Hard Decision Algorithm for Cooperative Spectrum Sensing in Cognitive Radio Networks*," in Proc. Of the ECSE'10* Conference, Cairo, Egypt.

[3] Hefdhallah Sakran & Mona Shokair(2010) "An Efficient Scheme for Cooperative Spectrum Sensing in Cognitive Radio Networks", *in Proc. Of the AEIC'2010*, Cairo, Egypt, Dec.

[4] Hefdhallah Sakran, Mona Shokair, El-Sayed El-Rabaie & Atef Abou El-Azm(2011) "Three Bits Softened Decision Scheme in Cooperative Spectrum Sensing Among Cognitive Radio Networks," *28th National Radio Science Conference (NRSC),* pp. 183-191, Cairo, Egypt.

[5] Hefdhallah Sakran, Mona Shokair, El-Sayed El-Rabaie, Omar Nasr & Atef Abou El-Azm(2012) "Proposed Relay Selection Scheme for Physical Layer Security in Cognitive Radio Networks," *IEEE IWCMC*, pp. 1052-1056.

[6] Hefdhallah Sakran and Mona Shokair(2010) "An Efficient Scheme for Cooperative Spectrum Sensing in Cognitive Radio Networks" *JAUES*, Vol. 5, No. 3, pp. 579- 587.

[7] R. Chen, J. Park & J. Reed (2006) "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks", *Proc. Of IEEE Workshop Network Technology Software Defined Radio Networks*, pp. 110-119.

[8] S. Anand, Z. Jin, & K. P. Subbalakshmi (2008) "An Analytical Model for Primary User Emulation Attacks in Cognitive Radio Networks",*3rd IEEE Symposium on new frontiers in dynamic spectrum access Networks*, pp.1-6.

[9] Z. Jin, 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. Vol. 13,No.2, pp. 74-85.

[10] Z. Jin and K. P. Subbalakshmi (2009) "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks," Proc. Of ICC 2009, pp. 1-5.

[11] Z. Chen, T. Cooklev and C. Chen and C. Plmalaza-Raez(2009) "Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks", Proc. Of 2009 IEEE 28th International Performance Computing and Communications Conference, pp. 208-215.

[12] C. Zhao, W. Wang, L. Huang, and Y. Yao(2010) " Anti-PUE Attack Based on Joint Position Verification in Cognitive Radio networks", Proc. Of the international conference on communication and mobile computing, pp. 169-173.

[13] C. Chen, H. Cheng & Y. Yao (2011) "Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack", IEEE Trans. Wireless Communication, Vol.10, No.7 pp. 2135–2141.

[14] F. Bao, H. Chen, and L. Xie (2012) " Analysis of Primary User Emulation Attack with Motional Secondary Users in Cognitive Radio Networks", Proc. Of 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC).

[15] S. M. Ross (2007) Introduction to Probability Models, Ninth Edition. Academic Press.

AUTHORS

Walid Ghanem received the B.Sc. degree in communication engineering from Faculty of Electronic Engineering, Menoufia University, Egypt, in May 2011, and he is currently working toward the MSc degree in Electrical communication engineering. His current research interests are cognitive radio networks, Localization, wireless security, encryption and optimization algorithms.

Mona Shokair received the B.Sc., and M.Sc. degrees in electronics engineering from Menoufia University, Menoufia, Egypt, in 1993, and 1997, respectively. She received the Ph.D. degree from Kyushu University, Japan, in 2005. She received VTS chapter IEEE award from Japan, in 2003. She published about 70 papers until 2014. She received the Associated Professor degree in 2011. Presently, she is an Associated Professor at Menoufia University. Her research interests include adaptive array antennas, CDMA system, WIMAX system, OFDM system, game theory , next generation networks and optimization algorithms.

Moawad I. Dessouky received the B.Sc. (Honors) and M.Sc. degrees from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1976 and 1981, respectively, and the Ph.D. from McMaster University, Canada, in 1986. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1986. He has published more than 200 scientific papers in national and International conference proceedings and journals. He has received the most cited paper award from Digital Signal Processing journal for 2008. His current research areas of interest include spectral estimation techniques, image enhancement, image restoration, super resolution reconstruction of images, satellite communications, and spread spectrum techniques.