Amirkabir University of Technology
(Tehran Polytechnic)
Vol. 47, No. 2, Fall 2015, pp. 1- 8

Amirkabir International Journal of Science& Research
(Electrical & Electronics Engineering)
(AIJ-EEE)

Secure Collaborative Spectrum Sensing in the Presence of Primary User Emulation Attack in Cognitive Radio Networks

A.A. Sharifi [1*], M. Sharifi [2] and M.J. Musevi Niya [3]

1- PhD. Student, Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
2- MSc. Student, Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran
3- Associate Professor, Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran

ABSTRACT

Collaborative Spectrum Sensing (CSS) is an effective approach to improve the detection performance in Cognitive Radio (CR) networks. Inherent characteristics of the CR have imposed some additional security threats to the networks. One of the common threats is Primary User Emulation Attack (PUEA). In PUEA, some malicious users try to imitate primary signal characteristics and defraud the CR users to prevent them from accessing the idle frequency bands. The present study investigates a new CSS scheme in the presence of a smart PUEA, which is aware of idle frequency channels and transmits its fake signal in a way that CR users are not easily able to discriminate between the received signal from the PU and PUEA. The idea is based on the Bayes risk criterion. More precisely, the sensing results of the CR users are summed up in the Fusion Center (FC) and compared with the optimum threshold that minimizes the Bayes risk. We also discuss practical limitation issue that need to be considered when applying the proposed method. Simulation results are provided to indicate the superiority of the proposed method against PUEA compared with conventional method.

KEYWORDS

Cognitive Radio, Cooperative Spectrum Sensing, Primary User Emulation Attack, Optimum Threshold, Bayes Risk.

* Corresponding Author, Email: a.sharifi@tabrizu.ac.ir

1- INTRODUCTION

Cognitive Radio (CR), which enables secondary user's access to licensed frequency bands, is a promising technology to boost spectrum resource utilization efficiency in upcoming communication networks [1]. A CR user is permitted to use licensed spectrum, provided that it does not interfere with any Primary User (PU). This requirement makes free spectrum exploration be a crucial function in CR networks. Several approaches have been investigated to monitoring the spectrum usage of PU that is so-called Spectrum Sensing [2], [3].

Local spectrum sensing at each CR node may not be as accurate as it should be because of communication channel fading, deep shadowing effects or hidden station problem. To deal with these problems, Collaborative Spectrum Sensing (CSS) was introduced where a Fusion Center (FC) exploits the available spatial diversity by employing multiple CR users' local information [3]. Moreover, the FC makes more reliable decision. But, sensing process suffers from two major security threats [4]; Spectrum Sensing Data Falsification (SSDF) attack and Primary User Emulation Attack (PUEA). In the first case, malfunction CR users or some malicious attackers may send incorrect sensing information to the FC and degrade the accuracy of the CSS process, leading to great error in detection of idle and busy channels. In the second case, one or more malicious users imitate and transmit similar primary signal on the sensing period. This may leads to the prohibition of CR users accessing to the idle channel which results in great false alarm probability.

The PUEA is a more active attacking approach to the spectrum sensing process of the CR networks. Recently, the PUEA has attracted considerable studies in literature [4-9]. In [4], the authors proposed a localization-based transmitter verification scheme to defend against PUEA. To this end, they exploited the received signal power and explored the location of primary transmitter and then determined whether the received signal was from PU or PUEA. However, this method is ineffective when the PU is considered as a mobile transmitter. In [5], an analytical model for the probability of successful PUEA based on energy detection was proposed and a lower bound on the probability of a successful PUEA is obtained using Markov inequality. In [6], Wald's Sequential Probability Ratio Test (WSPRT) was presented to detect PUEA based on the received signal power. In [7], a CSS model was proposed for PU detection in the presence of PUEA. In this approach, the decision whether the PU is present or absent is based on the energy detection method, but the attacker is assumed to be always present in wireless channel, which is not practical assumption from the energy consumption point of views. The authors of [8] introduced a smart PUEA to overcome this weakness. They have considered a PUEA in which malicious users choose their attack strategy in a smart manner so as to impose more destructive effect. The authors of [9] used weighted vector of CR's energy at FC and maximized the average cognitive signal to interference plus noise ratio. In [10] the hard combination method has been considered and voting rule exploited to choosing final decision. Then, the researchers explore the optimized number of samples used for decision making and find appropriate detection threshold so as to minimize total error probability.

Most of the previous research, to mitigate the destructive effect of PUEA, have been conducted based on assumption that the physical location or unique properties of the PU transmitter is known for CR users or the FC. But, an appropriate strategy capable of accurate PU detection, without requiring any prior information about location and properties of PU signal, is extremely important. Therefore, we propose a new CSS method that requires no prior information about physical location and properties of PU signal. First, each CR user performs its own spectrum sensing and sends its measurements to the FC. Then, the mean value of sensing reports is calculated to estimate the attack parameter. The obtained attack parameter, including probability of PUEA presence in a desired spectrum hole is used to determine the optimal thresholds that minimize the Bayes risk.

2- SYSTEM MODEL

The considered system model is a centralized CR network including a PU transmitter, N collaborative CR users, an FC and a PUEA. Each CR user independently conducts its spectrum sensing and then local measurements are sent to the FC to take the global decision about the presence or absence of the licensed PU signal. The network model is shown in Fig. 1.

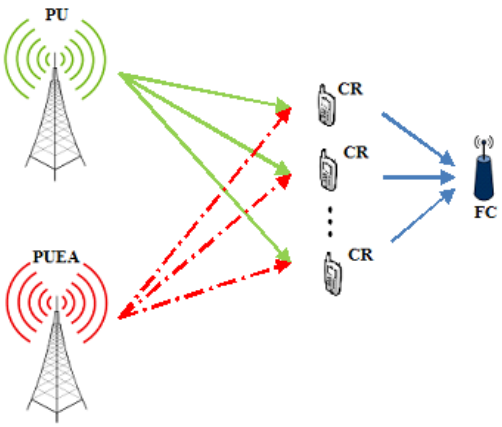

Fig. 1. Network Layout

We assume that the energy detection scheme is used for local spectrum sensing [11]. The PUEA is able to perform spectrum sensing to identify the spectrum holes and transmit the fake signal to disrupt the CR network operation. We further assume that the attacker is able to distinguish exactly between occupied and unoccupied frequency bands allocated to the PU.

Based on the presence or absence of the PU and PUEA, there are three possibilities which can be expressed as:

$$\begin{cases} \text{only Noise} & \text{under } H_0 \\ \text{PU + Noise} & \text{under } H_1 \\ \text{PUEA+ Noise} & \text{under } H_2 \end{cases}$$

The first state H_0 occurs when the CR users receive only noise. Moreover, the channel is neither occupied by the PU nor by PUEA. The second state H_1 happens when the PU transmits over the channel while the PUEA is absent. If the PU is absent and PUEA transmits the fake signal, the CR users receive only the PUEA signal plus noise, as stated by the third hypothesis H_2. We assume that two hypotheses H_1 and H_0 indicate the presence and absence of PU signal, respectively. Similarly, the presence and absence of the PUEA signal are denoted by E^{on} and E^{off}, respectively. Based on the above mentioned assumptions, the probability of each hypothesis H_k, denoted by π_k, is determined as

$$\begin{aligned} \pi_0 &= P(H_0) = P(H_0, E^{off}) = P(E^{off} \,|H_0) P(H_0) \\ \pi_1 &= P(H_1) = P(H_1, E^{off}) = P(E^{off} \,|H_1) P(H_1) \\ \pi_2 &= P(H_2) = P(H_0, E^{on}) = P(E^{on} \,|H_0) P(H_0) \end{aligned} \quad (1)$$

Let the parameter α (called attack strength through the study) be the conditional probability regarding the presence of the fake PUEA signals in the hypothesis H_0, (i.e. $\alpha = P(E^{on} \,|H_0)$). Thus, the above equation can be simplified to

$$\begin{aligned} \pi_0 &= (1-\alpha) P(H_0) \\ \pi_1 &= P(H_1) \\ \pi_2 &= \alpha P(H_0) \end{aligned} \quad (2)$$

By considering the three-level hypotheses, the received signal at the i th sample of the j th CR user, x_j^i, can be formulated as

$$x_j^i = \begin{cases} n_j^i & H_0 \\ \sqrt{\gamma_j}\, p_j^i + n_j^i & H_1 \\ \sqrt{\lambda_j}\, e_j^i + n_j^i & H_2 \end{cases} \quad (3)$$

where n_j^i is the Additive White Gaussian Noise (AWGN) at the j th CR user. The parameters $\sqrt{\gamma_j}\, p_j^i$ and $\sqrt{\lambda_j}\, e_j^i$ are the received PU and PUEA signal with the powers γ_j and λ_j, respectively. We assume that the noise at each sample (n_j^i), the PU signal (p_j^i), and PUEA signal sample (e_j^i) are independently and identically distributed Gaussian random variables with zero mean and unit variance. We further assume that the CR users experience independent Rayleigh fading channels with the same average SNRs. This condition is relevant for CR network which is geographically far from the PU and PUEA transmitters. Thus, γ_j and λ_j vary from (observation) period to period while their Probability Density Functions (PDFs) are identically as exponential distribution with the average values $\bar{\gamma}$ and $\bar{\lambda}$, respectively. The parameter ρ is also defined as $\rho = \bar{\lambda} / \bar{\gamma}$. As mentioned in equation (3) and with regard to the above assumptions, the received signal, x_j^i, is a Gaussian distributed as [10],

$$x_j^i \sim \begin{cases} \mathcal{N}(0,1) & H_0 \\ \mathcal{N}(0, \gamma_j + 1) & H_1 \\ \mathcal{N}(0, \lambda_j + 1) & H_2 \end{cases} \quad (4)$$

Moreover, M samples are used for local energy detection at each CR user during one detection interval. The observed energy of the j th user, E_j, is given by

$$E_j = \sum_{i=1}^{M} \left| x_j^i \right|^2 \sim \begin{cases} a_j & H_0 \\ (\gamma_j + 1) b_j & H_1 \\ (\lambda_j + 1) c_j & H_2 \end{cases} \quad (5)$$

where the random variables a_j, b_j and c_j follow a central Chi-square distribution with M degree of freedom. But, according to central limit theorem, if a large number of samples are considered (i.e. $M > 10$), these random variables can be assumed to be Gaussian distributed.

In conventional Equal Gain Combining (EGC) scheme [12], in the absence of the PUEA, all of the

sensing reports are summed up and compared with a predefined threshold to determine the channel status. The output signal at the FC is

$$Y = \sum_{j=1}^{N} E_j \underset{H_0}{\overset{H_1}{\gtrless}} \eta \tag{6}$$

where η is the global threshold and determined by the target false alarm or miss detection probability. In the presence of the PUEA, the decision statistics Y is a Gaussian distributed as

$$Y \sim \begin{cases} \mathcal{N}(\mu_0, \sigma_0^2) & H_0 \\ \mathcal{N}(\mu_1, \sigma_1^2) & H_1 \\ \mathcal{N}(\mu_2, \sigma_2^2) & H_2 \end{cases} \tag{7}$$

where one can easily verify that

$$\begin{aligned} &\mu_0 = MN\ ,\ \ \sigma_0^2 = 2MN \\ &\mu_1 = MN\,(\bar{\gamma}+1),\ \ \sigma_1^2 = 2MN\,(\bar{\gamma}+1)^2 \\ &\mu_2 = MN\,(\bar{\lambda}+1),\ \ \sigma_2^2 = 2MN\,(\bar{\lambda}+1)^2 \end{aligned} \tag{8}$$

An appropriate spectrum sensing rule is analyzed by considering the attacker. As mentioned before, the PUEA sends fake signals in the radio environment to defraud CR users and consequently prevents them from accessing idle frequency bands. The conditional PDFs of decision statistics Y under four hypotheses H_0, H_1, and H_2 are shown in Fig. 2.

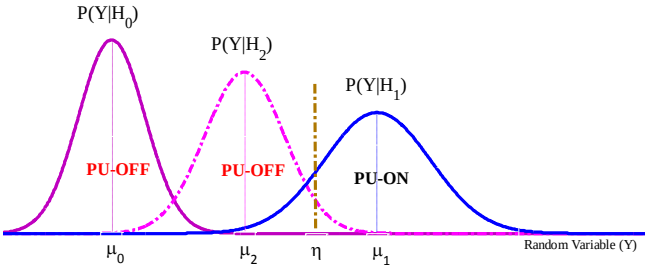

Fig. 2. The conditional PDFs of decision statistics

As shown, when two average SNR values $\bar{\gamma}$ and $\bar{\lambda}$ are the same ($\mu_1 = \mu_2$), two curves $P(Y|H_1)$ and $P(Y|H_2)$ exactly coincide and the optimum threshold η can be calculated.

Let $Q_{fa}(\eta)$ be the probability of global false alarm in CSS. Then we have

$$\begin{aligned} Q_{fa}(\eta) &= P\left(D^{on}|H_0\right) \\ &= P\left(D^{on}|H_0, E^{on}\right)P\left(E^{on}|H_0\right) \\ &+ P\left(D^{on}|H_0, E^{off}\right)P\left(E^{off}|H_0\right) \\ &= P\left(D^{on}|H_2\right)\alpha + P\left(D^{on}|H_0\right)(1-\alpha) \end{aligned} \tag{9}$$

Accordingly, the probability of global miss detection, denoted by $Q_m(\eta)$, is defined as

$$Q_m(\eta) = P\left(D^{off}|H_1\right) \tag{10}$$

where D^{on} means that the FC's decision is the presence of PU signal and D^{off} means that the global decision declares the absence of the PU signal.

To evaluate the performance of CSS in the presence of a malicious PUEA and compare it to conventional energy detection, in which the PUEA is not considered we use Bayes risk function. More precisely, we use the Bayes risk criterion to choose the optimal value of threshold η that minimizes the Bayes risk. Assuming that correct detection occurs in no additional cost, the Bayes risk is defined [13] as

$$\begin{aligned} \Re(\eta) &= \sum_{i=0}^{1}\sum_{j=0}^{1} P(\text{Decision} = H_i\,|H_j)\pi_j C_{ij} \\ &= Q_{fa}(\eta)\pi_0 C_{fa} + Q_m(\eta)\pi_1 C_m \end{aligned} \tag{11}$$

where C_{fa} and C_m are the costs of the false alarm and miss detection events, respectively.

3- OPTIMUM THRESHOLD CALCULATION

In this section, the optimal threshold selection approach is applied to find the hold hypothesis.

Let's begin the case that there is no PUEA signal ($\alpha = 0$) to derive the optimal detection threshold. In the absence of PUEA signals, the state H_2 does not occur ($\pi_2 = 0$). Hence, the Bayes risk is defined as:

$$\Re(\eta) = P(Y > \eta|H_0)\pi_0 C_{fa} + P(Y < \eta|H_1)\pi_1 C_m \tag{12}$$

The optimum thresholds η^* to achieve the minimum Bayes risk is obtained as

$$\frac{\partial \Re(\eta)}{\partial \eta} = 0 \Rightarrow \eta^* = \frac{\mu_0\sigma_1^2 - \mu_1\sigma_0^2 + \sqrt{\Delta}}{\sigma_1^2 - \sigma_0^2} \qquad (\sigma_1^2 \neq \sigma_0^2) \tag{13}$$

where

$$\Delta = \left[\mu_0\sigma_1^2 - \mu_1\sigma_0^2 \right]^2 + (\sigma_1^2 - \sigma_0^2)\left[\mu_1\sigma_0^2 - \mu_0\sigma_1^2 + 2\sigma_0^2\sigma_1^2 \ln(\frac{\sigma_1\pi_0 C_{fa}}{\sigma_0\pi_1 C_m}) \right] \quad (14)$$

In the presence of the PUEA, the Bayes risk is defined as

$$\Re(\eta) = p(Y > \eta | H_0)\pi_0 C_{fa} + p(Y > \eta | H_2)\pi_2 C_{fa} + p(Y < \eta | H_1)\pi_1 C_m \quad (15)$$

Thus, the optimum thresholds η^* is obtained as

$$\frac{\partial \Re(\eta)}{\partial \eta} = 0 \Rightarrow -\pi_0 C_{fa} \, \mathrm{F}(\eta^*, \mu_0, \sigma_0) - \pi_2 C_{fa} \mathrm{F}(\eta^*, \mu_2, \sigma_2) + \pi_1 C_m \mathrm{F}(\eta^*, \mu_1, \sigma_1) = 0 \quad (16)$$

where $\mathrm{F}(.)$ is the PDF of normal distribution given by $\mathrm{F}(x, \mu, \sigma) = (1/\sigma\sqrt{2\pi})\exp(-(x-\mu)^2/2\sigma^2)$. From the above equation, the optimum threshold η^* is calculated by numerical method.

4- PRACTICAL CONSIDEARTION

In the previous sections, we investigated collaborative sensing in the presence of a PUEA theoretically, without considering practical limitations. For instance, to find the hold hypothesis, the FC needs to get the α value according to (2). There might be several different methods for FC to get the parameter α but here, we propose a method based on the mean value of received sensing reports. Two parameters m and mathematical expectation of m are defined as

$$m = \frac{1}{N}\sum_{j=1}^{N} E_j \quad , \quad \mathrm{E}(m) = \frac{1}{N}\sum_{j=1}^{N} \mathrm{E}(E_j) \quad (17)$$

By considering three different hypotheses H_0, H_1, and H_2 we have

$$\mathrm{E}(E_j) = \mathrm{E}(E_j | H_0)\pi_0 + \mathrm{E}(E_j | H_1)\pi_1 + \mathrm{E}(E_j | H_2)\pi_2 = M\pi_0 + M(\gamma_j + 1)\pi_1 + M(\lambda_j + 1)\pi_2 \quad (18)$$

and

$$\mathrm{E}(m) = M\pi_0 + M(\bar{\gamma} + 1)\pi_1 + M(\bar{\lambda} + 1)\pi_2 \quad (19)$$

Considering the equation (2), the value of attack strength α is estimated as

$$\hat{\alpha} = (\mathrm{E}(m) - \psi_1)/\psi_2 \quad (20)$$

where two parameters ψ_1 and ψ_2 are defined as

$$\psi_1 = MP(H_0) + M(1+\bar{\gamma})P(H_1) \quad , \quad \psi_2 = M\bar{\lambda}P(H_0)$$

5- SIMULATION RESULTS AND DISCUSSIONS

We provide the simulation results of the analytical discussion in previous sections. In the proposed system model there are 12 CR users ($N = 12$) that use energy detection by $M = 30$ sample number in a detection interval. The channels are assumed to be Rayleigh fading. Moreover, prior probabilities $P(H_0)$ and $P(H_1)$ are assumed to be 0.8 and 0.2, respectively. Two parameters C_{fa} and C_m are set to 0.3 and 0.7, respectively. All parameters are constant unless otherwise specified.

Results are obtained through Monte-Carlo simulations over 10^4 runs. Throughout the simulations, we have depicted that there is not any PUEA signals labeled by "EGC (No Attack)" curves and the case that there is PUEA signals and the FC is not aware of the fake signals labeled by "Conventional" curves.

Fig. 3 shows the convergences of attack strength for $\alpha = 0.3$ and 0.7. The estimated values for α is converged to constant values after applying almost 300 rounds of sensing. In the simulation, the initial stage can be set as the first 500 sensing intervals where the attack strength is estimated and then used to find optimum threshold to improve the CSS process in the presence of a malicious PUEA.

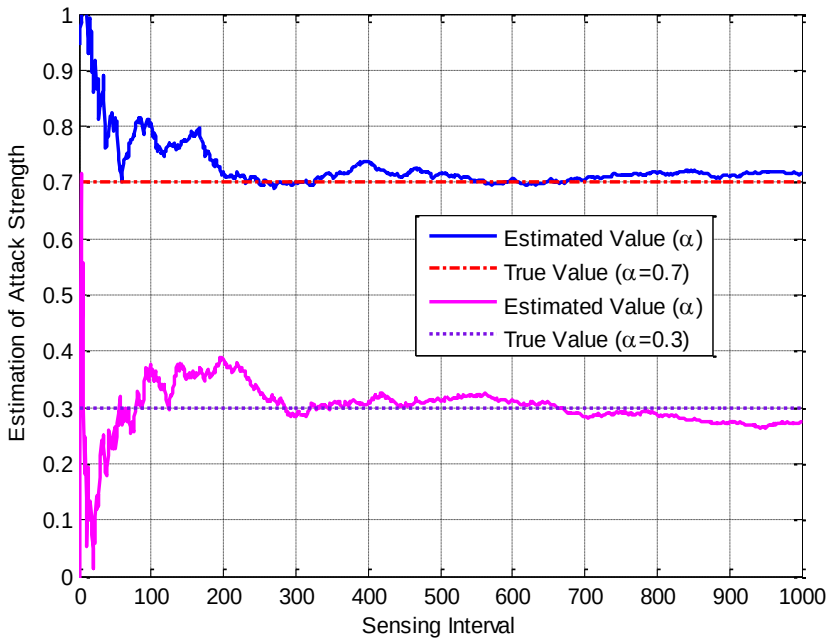

Fig. 3. The convergences of attack strength ($\alpha = 0.3$, 0.7)

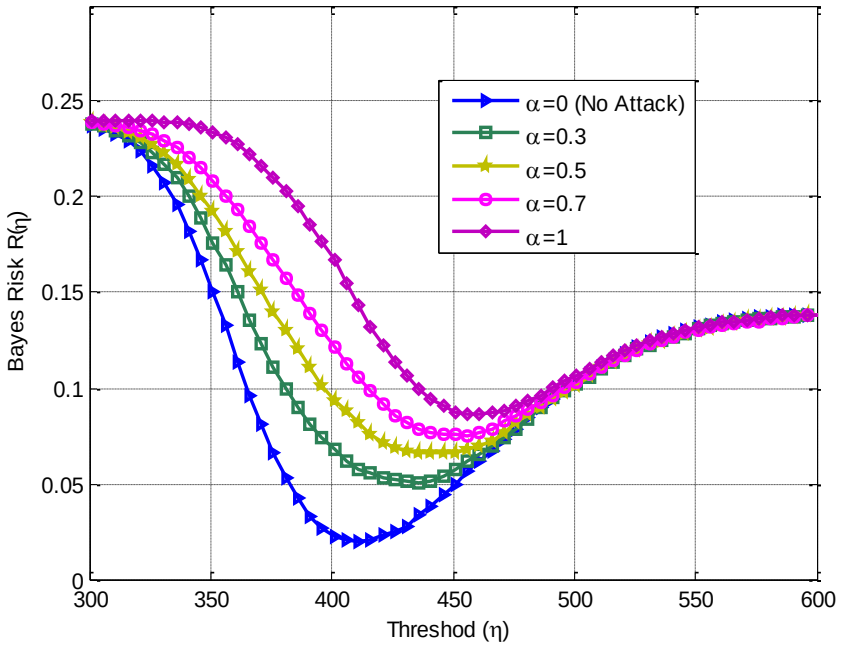

Fig. 4. The Bayes risk versus threshold for several different values of attack strengths

Fig. 4 displays the Bayes risk versus threshold η for several different values of attack strengths. The average SNR $\bar{\gamma}$ and parameter ρ are assumed to be -5dB and 0.5, respectively. As shown, for a given value of attack strength it is an optimal value for η that leads to minimum Bayes risk. Thus, we aim to deriving the optimal value for η so as to minimize the Bayes risk.

Fig. 5 depicts the Bayes risk versus attack strength for $\bar{\gamma} = -5\text{dB}$ and $\rho = 0.5$. As shown in the figure, in conventional method (the case that there is a PUEA from which the FC is not aware) with increasing α leads to high Bayes risk, in contrary, by the proposed method increasing α causes a small change in the rate of Bayes risk.

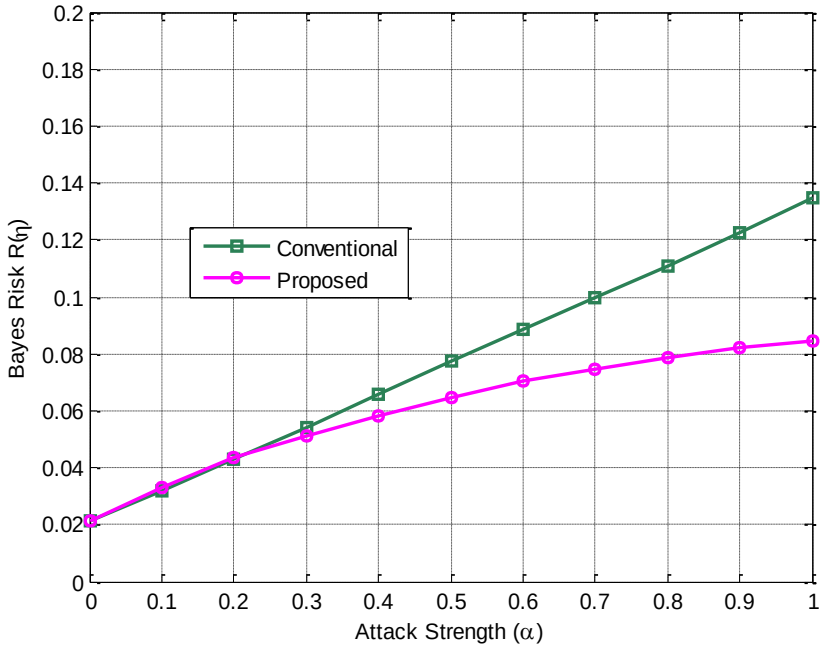

Fig. 5. The Bayes risk versus attack strength

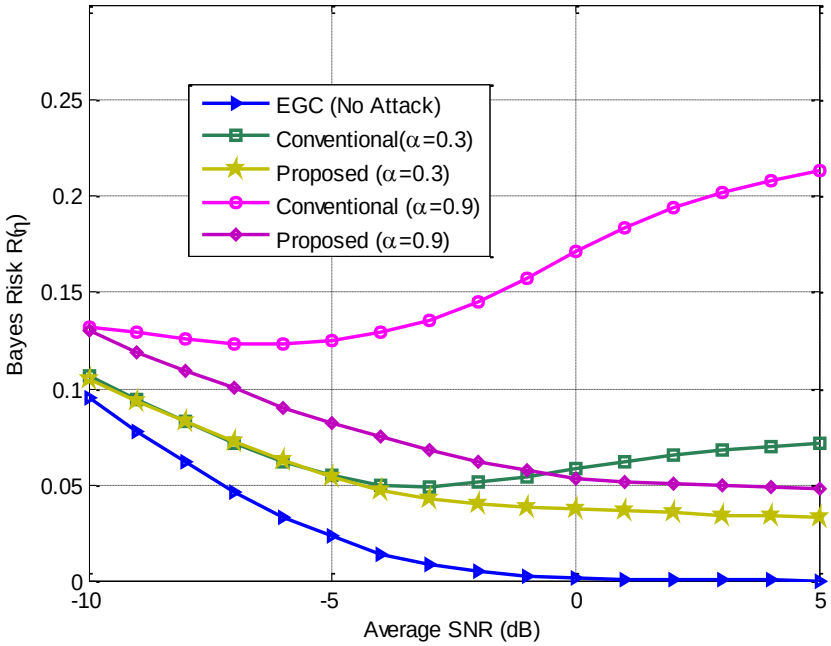

Fig. 6. The Bayes risk versus average SNR $\bar{\gamma}$

Fig 6 shows the Bayes risk versus average SNR ($\bar{\gamma}$) for attack strength 0.3 and 0.9. As shown in the figure, using the proposed method improves the performance of CSS under malicious PUEA signals.

6- CONCLUSION

Collaborative Spectrum Sensing (CSS) was investigated in the presence of Primary User Emulation Attack (PUEA). A new CSS scheme based on optimal threshold selection approach was introduced. As a countermeasure against PUEA, an appropriate defense strategy was proposed which estimated the attack strength, probability of the presence of a PUEA fake signal in the absence of licensed PU signal, and applied to determine the optimal threshold that minimizes the Bayes risk. By the proposed method, less Bayes risk in detection of PU is obtained. The obtained results verified the effectiveness of the proposed scheme compared with conventional method.

REFERENCES

[1] Mitola J, Maguire GQ. Cognitive radio: making software radios more personal. IEEE Personal Communication 1999; **6**(4): 13-18.

[2] Akyildiz IF, Lee WY, Vuran MC, Mohanty S. NeXt generation/dynamic spectrum access cognitive radio wireless networks: A survey. Computer Networks 2006; 50(13): 2127-2159.

[3] Mishra SM, Sahai A, Brodersen RW. Cooperative sensing among cognitive radios. In Proceedings of the IEEE International Conference on Communications 2006; 1658-1663.

[4] R. Chen, J. Park, Y. Hou, and J. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," IEEE Commun. Mag., vol. 46, no. 4, pp. 50–55, Apr. 2008

[5] Anand S, Jin Z, Subbalakshmi K. An analytical model for primary user emulation attacks in cognitive radio networks. In Proceeding IEEE International Dynamic Spectrum Access Networks 2008; 1-6.

[6] Jin Z, Subbalakshmi k. Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks. IEEE International Conference on Communications 2009; 1–5.

[7] Chen C, Cheng H, Yao Y-D. Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack. IEEE Transactions on Wireless Communications 2011; 10(7): 2135-2141.

[8] Haghighat M, Sadough SMS. Cooperative spectrum sensing for cognitive radio networks in the presence of smart malicious users. International Journal of Electronics and Communications (AUE) 2014; 68(6): 520-527.

[9] Haghighat M, Sadough SMS. Smart primary user emulation in cognitive radio networks: defense strategies against radio-aware attacks and robust spectrum sensing. Transactions on Emerging Telecommunications Technologies 2014.

[10] Saber MJ, Sadough SMS. Optimisation of cooperative spectrum sensing for cognitive radio networks in the presence of smart primary user emulation attack. Transactions on Emerging Telecommunications Technologies 2014.

[11] Digham F, Alouini M, Simon M. On the energy detection of unknown signals over fading channels. In Proceedings of IEEE International Conference on Communications 2003; 5: 3575–3579.

[12] Ma J, Zhao G, Li Y. Soft combination and detection for cooperative spectrum sensing in cognitive radio networks. IEEE Transactions on Wireless Communications 2008; 7(11): 4502-4507.

[13] Varshney PK. Distributed detection and data fusion. Springer-Verlag 1997.