AUT Journal of Electrical Engineering

AUT J. Elec. Eng., 51(1) (2019) 39-44
DOI: 10.22060/eej.2019.14147.5209

Investigation of Always Present and Spectrum Sensing Based Incumbent Emulators

A. A. Sharifi

Department of Electrical Engineering, University of Bonab, Bonab, Iran

ABSTRACT: Cognitive radio (CR) technology has been suggested for the effective use of spectral resources. Spectrum sensing is one of the main operations of CR users to identify the vacant frequency bands. Cooperative spectrum sensing (CSS) is used to increase the performance of CR networks by providing spatial diversity. The accuracy of spectrum sensing is the most important challenge in the CSS process since the sensing performance is vulnerable to security attacks. Primary user emulation attack (PUEA) is one of the most important attacks, where a malicious attacker sends the signal similar to the signal of the legitimate primary user (PU) and deceives the CR sensors to avoid them from accessing the spectrum holes. In this paper, we investigate two different strategies for the attacker. Always present (AP) and spectrum sensing (SS) based strategies. In the AP scenario, the PUEA, without performing spectrum sensing, continuously sends its fake signals. In SS based PUEA, the attacker senses the spectrum to identify the spectrum holes and then only sends its signals in idle frequency bands. Assuming the attack strategy, we estimate normalized attack power factor (NAPF) to obtain an optimal value of the energy detection threshold. The parameter NAPF is the ratio of the average emitted power of the attacker to the average power of the PU transmitter. The obtained results verify the superiority of the proposed energy detection approach compared to the existing conventional methods.

Review History:

Received: 1 March 2018
Revised: 9 November 2018
Accepted: 11 March 2019
Available Online: 11 March 2019

Keywords:

CR, PUEA
NAPF
AP
SS

1- Introduction

Cognitive radio (CR) network is a new technology in wireless communications, trying to resolve the spectrum scarcity [1]. In a CR network, two different types of users are present; primary users (PUs) and secondary users. The former is called licensed users and the latter, which is also referred to as the CR users, is called unlicensed users [2]. The CR users frequently monitor the frequency spectrum and identify the presence of licensed PU signals. This producer is named spectrum sensing. If the CR users are convinced by the absence of the PU signals, they can opportunistically use the vacant frequency bands for communications; otherwise, the CR users detect the presence of the PU signals, they immediately switch to another available spectrum band by performing spectrum handoff. In this way, the CR users are forced to use the spectrum holes without interfering with the PU signals [2]. Due to noise, multipath fading, shadowing, and hidden station problems, the local spectrum sensing of each sensor is not reliable [3]. Cooperative spectrum sensing (CSS) has been reported to address these issues, where some CR users collaborate with each other to sense the PU channels [4]. Although the CR network performance is improved by the CSS process, it is vulnerable to security threats [5]. One of the most common threats is primary user emulation attack (PUEA), where a malicious user tries to deceive the CR users by imitating the PU signal characteristics to prevent the CR sensors from accessing the idle frequency bands or convincing the CR users to leave the spectrum [5]. Several defense strategies have been reported recently [6-15].

In [6], the location information of the licensed PU transmitter was used to discriminate between the PU and PUEA signals. The authors in [7] have proposed Wald's sequential probability ratio test (WSPRT) to detect the PUEA. Their work is based on analytical modeling of the received CR users' power. The modified Neyman-Pearson (N-P) or log-likelihood ratio test (LLRT) was proposed in [8] and [9]. To improve the CSS performance and mitigate the impact of PUEA, the important attack parameters were estimated and then applied in LLRT. In [10] and [11] an intelligent PUEA was considered. In [10], the authors demonstrated that the intelligent behavior of an attacker results in a more harmful effect on spectrum sensing procedure. In [11], attack-aware threshold selection approach was reported. Four-level hypotheses were considered and optimal thresholds that minimize the total sensing error probability were obtained. In [12], an always present PUEA in a CR network was investigated. The spectrum sensing measurements of different CR users were combined at the FC and the combining weights were optimized with the aim of increasing the detection probability of PU signals under the limitation of a predefined false alarm probability. The effect of the channel estimation errors on the detection probability was also investigated. In [13], the game theory approach was suggested to defend against PUEA. Nash-equilibrium (NE) of the game was obtained and indicated that the NE depends on the attacker's strategy. The analysis of statistical characteristics for the received power of the CR users was proposed in [14] to discriminate between PU and PUEA signals. The authors have considered three efficient scenarios: always present, probabilistic and adverse attacks. An optimal weighted CSS was introduced in [15]. The optimal weights were calculated by maximizing the CR sensors' throughput while protecting the PU from interference with the PUEA.

Corresponding author, E-mail: sharifi@bonabu.ac.ir

In this paper, we investigate a CSS process in the presence of a PUEA. Each CR user independently senses the frequency band and then sends its sensing measurement to the FC. The measurement is the received energy of the CR user from the PU signal or the PUEA. The FC makes the global decision about the status of the PU transmitter by using an optimal threshold selection approach in equal gain combining (EGC) scheme. We have considered two different scenarios: Always present (AP) and spectrum sensing (SS) based emulators. In the AP attack, the emulator permanently sends fake signals in the radio environment. In SS based PUEA, the attacker senses its environment and searches the vacant frequency bands to transmit its fake signals. Assuming the attack strategy, we estimate normalized attack power factor (NAPF) to obtain an optimal value of the energy detection threshold. The parameter NAPF is defined as the ratio of the average emitted power of the attacker to the average power of the PU transmitter. Computer simulation results confirmed the superiority of the proposed method.

The rest of the paper is presented as follows: In section two, the system model, and the CSS process are described. Section three explains the estimation of the attack power factor. In section four, numerical results are provided. Finally, section five concludes the paper.

2- system model and cooperative spectrum sensing

In this part, we explain the suggested system model and briefly review the energy detection scheme for cooperative sensing. In the presented system model, we consider a wireless CR network with N number of CR users and a malicious PUEA. A malicious PUEA emulates the features of the PU signal to deceive the CR sensors to convince that the PU transmission is in progress. The proposed system model is shown in Fig. 1

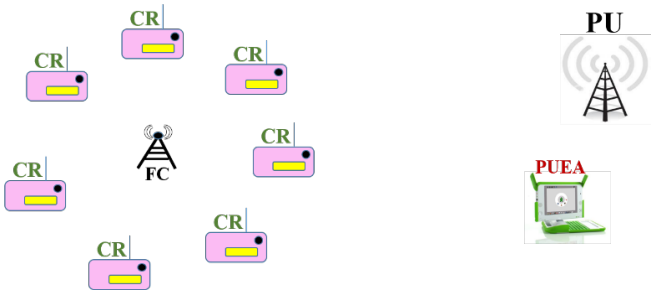

Fig. 1. Network layout

In the proposed network model, a malicious PUEA is relatively located near the PU transmitter to sense the primary spectrum; consequently, the spectrum sensing error either caused by multipath fading or shadowing is ignored for the attacker. We also assume that the emulator is able to change its transmission power level. As mentioned before, two different strategies are investigated for the PUEA; AP and SS-based strategies. In AP attack, the malicious PUEA continuously sends its fake signals in the channel. In SS-based PUEA, the attacker performs spectrum sensing to identify vacant frequency bands and then only sends its signals in unoccupied frequency bands. The transmission process of the legitimate PU, AP-PUEA, and SS-PUEA are presented in Fig. 2.

The presence and absence of PU signal are respectively denoted by PU^{on} and PU^{off}. Similarly, E^{on} and E^{off} specify the presence and absence of the malicious PUEA signal, respectively.

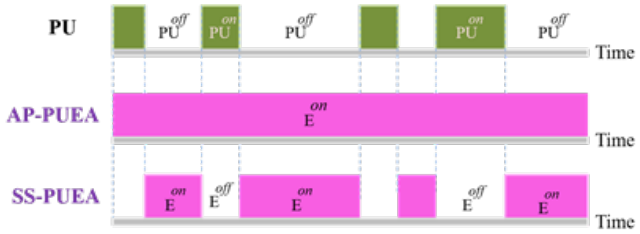

Fig. 2. The transmission process of the PU, AP-PUEA, and SS-PUEA

We adopt that each sensor uses an energy detector for its local spectrum sensing. Spectrum sensing is a binary hypothesis between H_0 and H_1 which includes the hypotheses of the absence and presence of the PU signal, respectively. In the presence of the PUEA, two different AP and SS-based attack strategies can occur. In AP-PUEA scenario, the hypotheses can be written as:

$$\begin{cases} H_0: & \text{PUEA+ Noise,} \\ \widehat{H}_1: & \text{PU + PUEA+ Noise,} \end{cases}$$

In SS-PUEA, we have

$$\begin{cases} H_0: & \text{PUEA+ Noise,} \\ \widetilde{H}_1: & \text{PU + Noise.} \end{cases}$$

If the local sensing time is partitioned into M sampling instants, the signal $y_j(m)$ received by the j'th CR user at sampling instants m=1, 2, … , M, in two different scenarios AP-Attack and SS-Attack can be respectively shown as equations (1) and (2) [16].

$$y_j(m) = \begin{cases} \sqrt{\gamma_e}\, x_e(m) h_{e_j}(m) + n_j(m), & H_0, \\ \sqrt{\gamma_p}\, x_p(m) h_{p_j}(m) + \sqrt{\gamma_e}\, x_e(m) h_{e_j}(m) + n_j(m), & \widehat{H}_1. \end{cases} \quad (1)$$

In SS-PUEA strategy,

$$y_j(m) = \begin{cases} \sqrt{\gamma_e}\, x_e(m) h_{e_j}(m) + n_j(m), & H_0, \\ \sqrt{\gamma_p}\, x_p(m) h_{p_j}(m) + n_j(m), & \widetilde{H}_1, \end{cases} \quad (2)$$

where $n_j(m)$ is the additive noise at the jth CR user with zero mean and unit variance. Two parameters $h_{pj}(m)$ and $h_{ej}(m)$, respectively denote the channel coefficients of the PU and the PUEA to the j'th CR user. We also consider block fading channels with constant channel coefficients in each sensing interval. Thus, m can be omitted from $h_{pj}(m)$ and $h_{ej}(m)$. Two parameters $\sqrt{\gamma_p}\, x_p(m)$ and $\sqrt{\gamma_e}\, x_e(m)$ are the PU and PUEA transmitted signals, respectively. $\sqrt{\gamma_p}$ and $\sqrt{\gamma_e}$ are the power coefficients and x_p and x_e are assumed to be independent and identical distributed Gaussian variables with zero means and unit variances. The parameter NAPF (ρ) is also defined as the ratio of the average emitted power by the PUEA to the average transmitted power of the PU, that it is $\rho = \gamma_e / \gamma_p$. Obviously, a greater NAPF (ρ) indicates a more powerful PUEA.

Each CR sensor receives the signal from the M sensing instants. Then, the jth sensor calculates its energy E_j as:

$$E_j = \sum_{m=1}^{M} \left| y_j(m) \right|^2. \quad (3)$$

Based on equations (1) or (2), E_j is the central Chi-square distributed random variable with $2M$ degrees of freedom. With regard to the central limit theorem, for a sufficiently large

number of samples (i.e., M>10), E_j approximately follows a normal distribution. Each CR reports its measured energy to the FC and the FC combines all of the received energies to perform the global decision on spectrum occupancy. The decision statistic is as follows:

$$\Lambda_N = \frac{1}{N}\sum_{j=1}^{N} E_j . \tag{4}$$

The global decision is made at the FC by comparing Λ_N to a decision threshold T. If Λ_N is greater than T, the PU signals' presence is concluded; otherwise, null hypothesis H_0 is concluded. The global detection and false alarm probabilities can be defined as:

$$\begin{aligned} Q_d &= p(\Lambda_N > T \,|H_1), \\ Q_{fa} &= p(\Lambda_N > T \,|H_0), \end{aligned} \tag{5}$$

where the hypothesis H_1 can be either $\widehat{H}_1$ or $\widetilde{H}_1$ hypothesis. The global error probability Q_e at the FC is written as follows:

$$Q_e = Q_{fa}p(H_0) + (1-Q_d)p(H_1). \tag{6}$$

In (4), the decision statistics Λ_N is also a normal distributed random variable. In AP-PUEA scenario, we have

$$\Lambda_N \sim \begin{cases} N\left(\mu_0, \sigma_0^2\right), & H_0, \\ N\left(\hat{\mu}_1, \hat{\sigma}_1^2\right), & \hat{H}_1, \end{cases} \tag{7}$$

and in SS-PUEA strategy

$$\Lambda_N \sim \begin{cases} N\left(\mu_0, \sigma_0^2\right), & H_0, \\ N\left(\tilde{\mu}_1, \tilde{\sigma}_1^2\right), & \bar{H}_1, \end{cases} \tag{8}$$

where,

$$\mu_0 = M(\gamma_e + 1) = M(\rho\gamma_p + 1) \ ,$$
$$\sigma_0^2 = 2M(\gamma_e + 1)^2 = 2M(\rho\gamma_p + 1)^2 ,$$
$$\hat{\mu}_1 = M(\gamma_p + \rho\gamma_p + 1) \ ,$$
$$\hat{\sigma}_1^2 = 2M(\gamma_p + \rho\gamma_p + 1)^2 ,$$
$$\tilde{\mu}_1 = M(\gamma_p + 1) \ ,$$
$$\tilde{\sigma}_1^2 = 2M(\gamma_p + 1)^2$$

3- the proposed method

Our objective is to resolve two different issues. At first, assuming the attack strategy (AP or SS), the parameter NAPF (attack strength) is estimated to obtain mean and variance of the Gaussian random variable Λ_N. Then, the optimal value of threshold T_{opt} is calculated to minimize the global error probability. In the primary stages of the cooperative sensing, the calculated energies of all CR sensors are sent to the FC and the FC calculates the mean value of received energies to achieve the NAPF (ρ).

The mathematical expectation of Λ_N is calculated as follows:

$$\begin{aligned} \mathrm{E}(\Lambda_N) &= \mathrm{E}(\Lambda_N \,|H_0)p(H_o) + \mathrm{E}(\Lambda_N \,|H_1)p(H_1) \\ &= \mu_0 p(H_o) + \mu_1 p(H_1). \end{aligned} \tag{10}$$

for AP -PUEA,

$$\begin{aligned} \mathrm{E}(\Lambda_N) &= M(\gamma_e + 1)p(H_o) + M(\gamma_p + \gamma_e + 1)p(\widehat{H}_1) \\ &= M(\rho\gamma_p + 1)p(H_o) + M(\gamma_p + \rho\gamma_p + 1)p(\widehat{H}_1) \\ &= M\rho\gamma_p + M + M\gamma_p p(\widehat{H}_1). \end{aligned} \tag{11}$$

Considering the above equations, the values of unknown NAPF ρ is estimated as

$$\hat{\rho} = \frac{\mathrm{E}(\Lambda_N) - \widehat{\psi}}{M\gamma_p}. \tag{12}$$

where,

$$\widehat{\psi} = M\left(1 + \gamma_p p(\widehat{H}_1)\right).$$

Similarly, for SS -PUEA,

$$\begin{aligned} \mathrm{E}(\Lambda_N) &= M(\gamma_e + 1)p(H_o) + M(\gamma_p + 1)p(\widetilde{H}_1), \\ &= M(\rho\gamma_p + 1)p(H_o) + M(\gamma_p + 1)p(\widetilde{H}_1), \\ &= M\rho\gamma_p p(H_o) + M + M\gamma_p p(\widetilde{H}_1). \end{aligned} \tag{13}$$

thus,

$$\tilde{\rho} = \frac{\mathrm{E}(\Lambda_N) - \widetilde{\psi}}{M\gamma_p p(H_0)}, \tag{14}$$

where,

$$\widetilde{\psi} = M\left(1 + \gamma_p p(\widetilde{H}_1)\right).$$

Regarding the proposed system model and considering the attack scenario, two attack strategies AP-PUEA and SS-PUEA do not occur simultaneously in the CR network. Thus,

$$p(H_0) + p(\widehat{H}_1) = 1,$$
$$p(H_0) + p(\widetilde{H}_1) = 1.$$

After the estimation of the parameter ρ, the FC obtains optimal threshold value T_{opt} for minimizing the total error probability. The optimal threshold T_{opt}, to attain the minimal global error probability Q_e, is calculated as follows [17]:

$$\begin{aligned} &\frac{\partial Q_e}{\partial \lambda} = 0 \ \Rightarrow \\ &\lambda_{opt} = \frac{\mu_0\sigma_1^2 - \mu_1\sigma_0^2 + \sqrt{\varphi}}{\sigma_1^2 - \sigma_0^2} \qquad (\sigma_1^2 \neq \sigma_0^2). \end{aligned} \tag{15}$$

where

$$\begin{aligned} \varphi = &\left[\mu_0\sigma_1^2 - \mu_1\sigma_0^2\right]^2 + \\ &(\sigma_1^2 - \sigma_0^2)\left[\mu_1\sigma_0^2 - \mu_0\sigma_1^2 + 2\sigma_0^2\sigma_1^2 \ln\left(\frac{\sigma_1 p(H_0)}{\sigma_0 p(H_1)}\right)\right]. \end{aligned} \tag{16}$$

It should be noted that μ_1 corresponds to $\hat{\mu}_1$ or $\tilde{\mu}_1$ and σ_1 corresponds to $\hat{\sigma}_1$ or $\tilde{\sigma}_1$.

4- numerical results

We consider a CR network with N=12 cooperative sensors. Each CR sensor executes spectrum sensing with an energy detection method by M=30 samples. The prior probabilities $p(H_0)$ and $p(H_1)$ are respectively assumed to be equal to 0.8 and 0.2.

Figures 3 and 4 show the convergence of NAPF for two values 0.3 and 0.7 in AP-PUEA and SS-PUEA scenarios, respectively. The estimated values for attack factor ρ are converged to the constant values after approximately performing 200 stages of spectrum sensing. Hence, the initial sensing can be used as the first 200 sensing rounds to estimate the NAPF ρ.

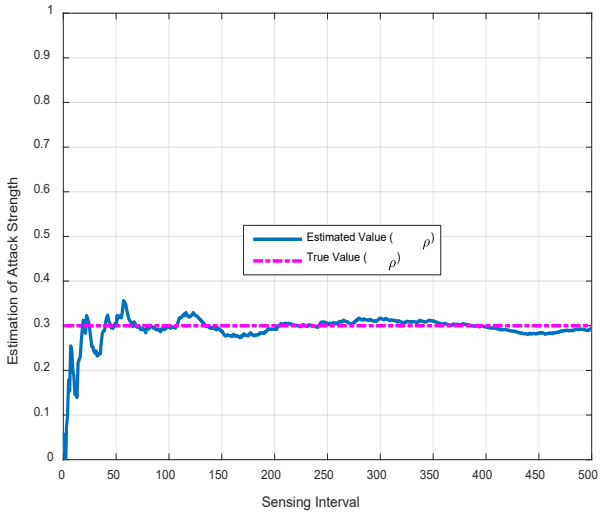

Fig. 3. The convergence of normalized attack power factor (NAPF) in AP-PUEA (ρ=0.3)

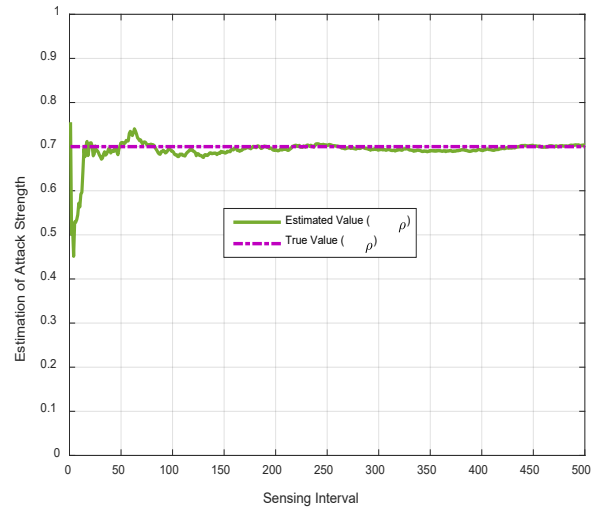

Fig. 4. The convergence of NAPF in SS-PUEA (ρ=0.7)

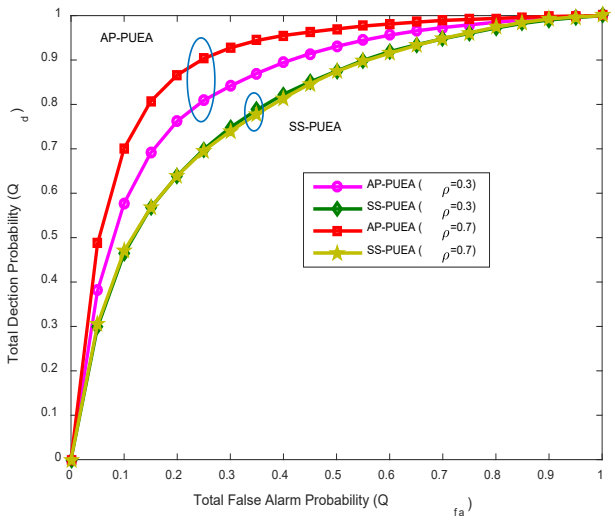

Fig. 5. The global detection probability versus the false alarm probability in SNR=-10dB

Fig. 5 displays the global detection probability versus the global false alarm probability in two attack scenarios AP and SS for ρ=0.3, 0.7. The average SNR between PU and CR users is set as -10dB. As shown in the figure, for a constant value of Q_{fa}, the AP-PUEA has a higher detection probability than that of the SS-PUEA. The reason is that in AP strategy the fake signal occurs in both idle and busy frequency bands. Thus, it would be an assistance signal for CR user energy detection to detect PU signals. More clearly, the simultaneous presence of the fake signals with the PU signals causes a more powerful signal to be received by the CR users, and hence the detection probability Q_d is increased.

Fig. 6 indicates the global detection and false alarm probabilities versus NAPF. Obviously, for a larger value of ρ ($\rho \sim 1$), two hypotheses H_0 and $\widetilde{H}_1$ cannot be easily distinguished. In other words, two conditional probabilities $p(\Lambda_N | H_0)$ and $p(\Lambda | \widetilde{H}_1)$ are almost identical and the global false alarm probability is remarkably increased. As explained before, the AP-PUEA causes a high detection probability compared with SS-PUEA.

In Fig. 7, the effect of received SNR from PU is studied in three different states; No-attack, AP-PUEA, and SS-PUEA. Two normalized attack factors ρ=0.3 and ρ=0.7 are considered. It can be observed that the global error probability is increased by increasing the SNR, especially for larger values of ρ. The reason is that without any defense strategy the presence of PUEA signals is not considered and the optimal value of the threshold is obtained based on noise variance. When SNR increases (noise power reduces in simulation) the global false alarm increases and consequently, total error probability under PUEA is increased in higher SNRs.

Fig. 8 demonstrates the global error probability versus NAPF for AP and SS scenarios with SNR=-5dB. As shown in the figure, in the AP and SS attacks, the global error probability is increased by increasing the NAPF and the error probability of SS-PUEA is almost higher than that of AP-PUEA. As mentioned before, for a constant value of normalized attack parameter, the AP and SS attacks have identical false alarm rate, whereas; SS-PUEA has a lower detection probability than that of AP-PUEA. By contrast, by the proposed method, increasing NAPF leads to a small change in the rate of total error probability.

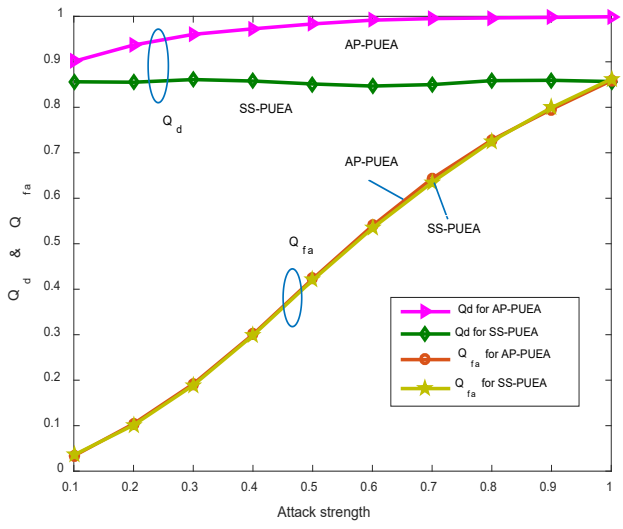

Fig. 6. The total detection and false alarm probabilities versus NAPF (attack strength) in SNR=-5dB

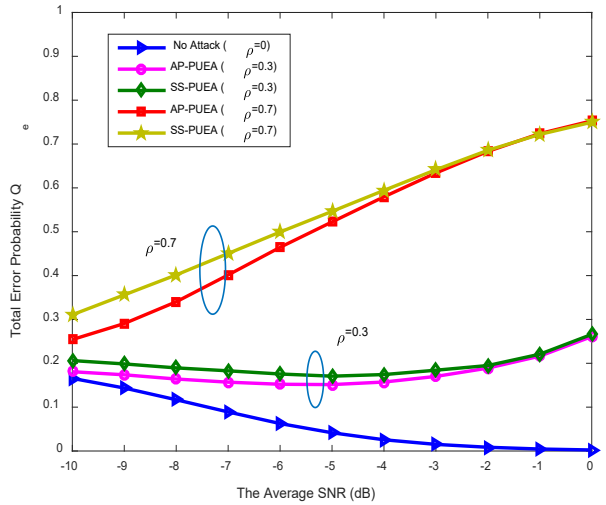

Fig. 7. The total error probability in the absence and presence of an attacker for ρ=0.3, 0.7

5- conclusion

Primary user emulation attack (PUEA) was studied in cognitive radio (CR) networks. Assuming the attack strategy, the received reports of the CR users were used to estimate normalized attack power factor (NAPF) to obtain an optimum value of threshold that minimizes the global error probability. The parameter NAPF was defined as the ratio of average emitted power of the malicious PUEA to the average power of the legitimate PU. Two different attack strategies were investigated for the PUEA; Always present (AP) and spectrum sensing (SS) based attacks. It was concluded that without any defense strategy, the SS based emulator is a little more harmful than AP-PUEA. In addition, from the attacker's point of view, the AP strategy cannot be a practical choice due to more power consumption. Numerical results validated the efficiency of the proposed approach compared with the conventional method.

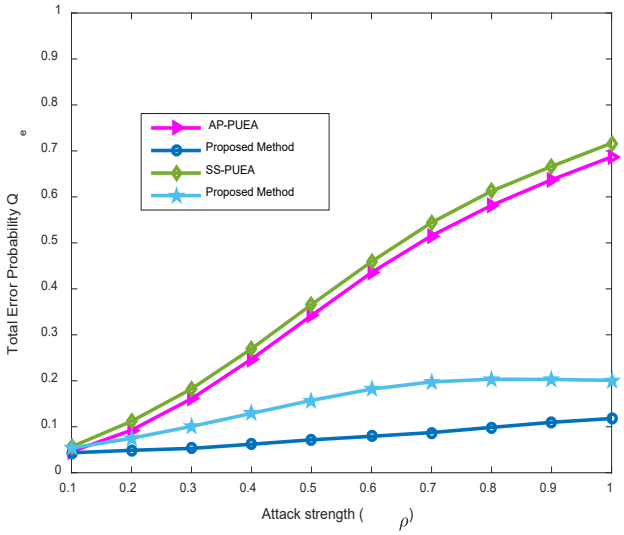

Fig. 8. The total error probability versus NAPF (ρ) in SNR=-5dB

References

[1] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, 23(2) (2005) 201-220.

[2] Akyildiz IF, Lee WY, Vuran MC, Mohanty S, "NeXt generation/dynamic spectrum access cognitive radio wireless networks: A survey," *Computer Networks,* 50(13) (2006) 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] I. F. Akyildiz, B. F. Lo, R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, 4(1) (2011) 40-62.

[5] R. Chen, J. m. Park, Y. T. Hou and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Communications Magazine*, 46(4) (2008) 50-55.

[6] Chen R, Park JM, Reed JH, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal of Selected Area in Communications,* 26(1) (2008) 25-37.

[7] 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.

[8] A. A. Sharifi, M. Sharifi, M. J. Musevi Niya. "Collaborative spectrum sensing under primary user emulation attack in cognitive radio networks," *IETE Journal of Research*, 62(2) (2016) 205-211.

[9] A. A. Sharifi, M. J. Musevi Niya. "Robust cooperative spectrum sensing under primary user emulation attack in cognitive radio networks," *Journal of Computing and Security*, 2(2) (2015) 109-117.

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

[11] A. A. Sharifi, M. Sharifi, M. J. M. Niya, "Secure cooperative spectrum sensing under primary user emulation attack in cognitive radio networks: Attack-aware threshold selection approach," *International Journal of Electronics and Communications (AEU)*, 70(1) (2016) 95-104.

[12] 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*, 10(7) (2011) 2135-2141.

[13] A. Ahmadfard, A. Jamshidi, A. Keshavarz-Haddad, "Game theoretic approach to optimize the throughput of cognitive radio networks in physical layer attacks," *Journal of Intelligent & Fuzzy Systems*, 28(3) (2015) 1281-1290.

[14] Ghaznavi. M, Jamshidi. A, "Defence against primary user emulation attack using statistical properties of the cognitive radio received power," *IET Communications*, 11 (2017) 1535-1542.

[15] S. Shrivastava, A. Rajesh, P. K. Bora, "Defense against primary user emulation attacks from the secondary user throughput perspective," *International Journal of Electronics and Communications (AEU)*, (2018) 131-143.

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

[17] M. Sharifi, A. A. Sharifi, M. J. M. Niya, "A new weighted energy detection scheme for centralized cognitive radio networks," *7th international symposium on telecommunications*, 2014.

Please cite this article using:

A. A. Sharifi, Investigation of Always Present and Spectrum Sensing Based Incumbent Emulators , *AUT J. Elec. Eng.*, 51(1) (2019) 39-44.

DOI: 10.22060/eej.2019.14147.5209