İSTANBUL UNIVERSITY PRESS

RESEARCH ARTICLE

Electrica 2018; 18(2): 227-233

Dynamic Threshold Selection Approach in Voting Rule for Detection of Primary User Emulation Attack

Abbas Ali Sharifi, Mohammad Mofarreh-Bonab

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

Cite this article as: AA. Sharifi, M. Mofarreh-Bonab. "Dynamic Threshold Selection Approach in Voting Rule for Detection of Primary User Emulation Attack". *Electrica*, vol. 18, no. 2, pp. 227-233, 2018.

ABSTRACT

Cognitive radio (CR) technology presents a mechanism for efficient spectrum usage. Spectrum sensing is an essential CR function which includes an intelligent signal processing algorithm to identify the vacant frequency bands. Cooperative spectrum sensing (CSS) has been widely adopted to improve the performance of CR networks. Unfortunately, CR networks are vulnerable to security threats. In this study, we propose an optimal threshold selection approach to address one of the most important attacks called primary user emulation attack (PUEA). In PUEA, a malicious attacker mimics some important primary signal features and deceives CR sensors to prevent them from accessing the available channels. In this study, we assume a malicious PUEA which is relatively located near the potential user (PU) transmitter and senses the spectrum and accurately detects the vacant frequency bands to transmit its fake signal. We estimate attack strength and then apply the K-out-of-N rule to obtain an optimum and dynamic threshold K, minimizing the global error probability. Here, the attack strength is defined as the ratio of the average transmission power of the PUEA to the average power of the PU. The achieved simulation results indicate that the performance of the suggested method is satisfactory in detecting the malicious PUEA compared with conventional methods.

Keywords: Cognitive Radio (CR); Cooperative Spectrum Sensing (CSS); Primary User Emulation Attack (PUEA); K-out-N rule.

Introduction

Cognitive Radio (CR) networks are promising wireless networks and new technology in communication systems in order to resolve the spectrum scarcity issue [1]. Spectrum sensing is one of the main enabling functions of a CR device to make an intelligent decision about spectrum usage [2]. Cooperative Spectrum Sensing (CSS) has been confirmed to be an efficient approach to promote the sensing performance by providing a spatial form of diversity [3]. In the CSS process, each CR sensor separately senses the desired spectrum and then sends its measurement to a Fusion Center (FC). Due to the special structure of a CR network, it is vulnerable to security attacks. Two important security attacks include the Spectrum Sensing Data Falsification (SSDF) attack and the Primary User Emulation Attack (PUEA) [4]. During SSDF attacks, CR attackers send falsified spectrum sensing results to the FC and disrupt the global sensing decision. To overcome the impact of SSDF attacks, several different solutions have been proposed in previously [5-7]. In PUEA, a malicious attacker mimics some characteristics of the legitimate PU's signal. Whenever the PU transmitter does not send in the desired channel, the PUEA transmits its fake signal to the CR sensors, deceiving them to believe that the channel is occupied by the PU. This type of attack has been studied extensively [8-14].

The CSS procedure in the presence of a PUEA was considered in [8]. A proper dynamic collaborative weight was assigned to each CR sensor and then the received reports were aggregated in the FC with a weighted combined algorithm in order to maximize the performance of PU's signal detection in Neyman-Pearson (N-P) algorithm. The omnipresent attacker was assumed which is not practical due to the added power consumption [8]. A smart PUEA was considered in the case that it is located near the PU tower and adjusts its transmitted power to be the

Corresponding Author:
Abbas Ali Sharifi

E-mail:
sharifi@bonabu.ac.ir

Received: 19.01.2018

Accepted: 23.03.2018

DOI: 10.5152/iujeee.2018.1819

same as the PU's power [9]. The malicious incumbent emulator only occupies a portion of the vacant frequency band and the channel occupancy rate of the attacker was estimated and applied in N-P criteria to improve the performance of cooperative sensing. In order to enhance the CSS performance, in the coexistence of a PUEA, a tow-level database-assisted spectrum sensing was proposed in [10]. Energy detection and location verification are combined for fast and consistent detection of PU signals. Game theory approach was proposed to mitigate the impact of PUEA [11]. The Nash Equilibrium (NE) was calculated and it was achieved that the NE depends on the available spectrum and the attacker's behavior. The Attack-Aware Threshold Finding method was introduced to defense against the PUEA [12]. Two important PUEA parameters, probabilities of PUEA activity in both occupied and unoccupied frequency bands, were estimated and used to derive the optimal threshold values. The authors proposed Multi-Level Hypotheses Test (MLHT) [13]. They partitioned the decision space into four different areas and then applied the Bays cost criteria to specify the PU channel status. Statistical characteristics of the received power from CR sensors were used to address the PUEA [14].

In this paper, we assume a centralized CR network with a malicious PUEA and propose an attack-aware CSS method based on a new hard-decision combining scheme. In the proposed method, the cooperative sensing process is performed in two stages: in the first stage, the CR users individually sense the frequency spectrum and then send their measured energies to the FC. In this stage, the FC estimates the attack strength. In the second round, each CR sensor sends its one bit hard decision about PU signal presence. In this round of cooperative sensing, the obtained attack strength is innovatively applied the K-out-of-N data fusion rule to obtain an optimal value of threshold K that minimizes the global error probability. In the proposed system model, the attacker only sends its fake signal in vacant frequency bands which is an important task of power saving strategy, unlike previous research [8, 12].

The rest of the paper is prepared as follows: Sec. II describes the considered system model and energy detection method. In Sec. III, we review the CSS process. Sec. IV explains the proposed optimal K-out-of-N rule. Sec. V provides simulation results. Finally, Sec. VI concludes the paper.

System Model and Energy Detection Scheme

The planned system model for a centralized CR network is shown in Figure 1. The proposed system model considers a wireless CR network with N number of collaborative CR sensors. In order to get a higher priority than other CR users in accessing unoccupied frequency bands, a malicious PUEA emulates some important characteristics of the legitimate PU's signal to defraud other CR users into believing that the PU's transmission is in process. It is further assumed that the whole CR network is in the communication range of PU and PUEA transmitters.

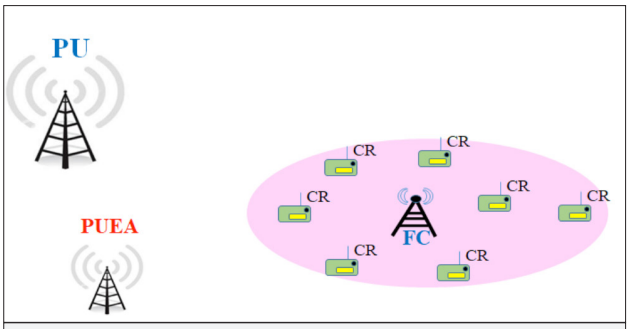

Figure 1. Network Layout

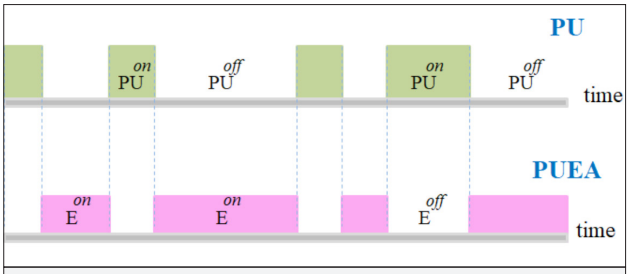

Figure 2. The transmission process of the PU and PUEA

We assume that the PUEA is located near the PU transmitter. Consequently, the spectrum sensing error caused by multipath fading and shadowing is ignored for the attacker. We further assume that the attacker is smart and only transmits its fake signal in unoccupied frequency bands. The transmission process of the PU and PUEA in several different time slots are shown in Figure 2.

The presence and absence of PU signal are denoted by PU^{on} and PU^{off}, respectively. Similarly, E^{on} and E^{off} indicate that the PUEA fake signal is present and absent, respectively.

It is assumed that each CR sensor has a local energy detector to sense its surrounding area. Spectrum sensing is a binary hypothesis between H_0 and H_1, which are the hypotheses of absence and presence of the PU signal, respectively. In the absence of PUEA (No attack scenario), two well-known hypotheses can be written in general as:

$$\begin{cases} H_0: & \text{Only Noise} \\ H_1: & \text{PU} + \text{Noise} \end{cases}$$

The first state H_0 indicates that the channel is free of any PU signals and the second hypothesis H_1 declares that the PU sends its legitimate signal through the channel. Considering the above mentioned hypotheses, the received signal at the *i*th sample of the *j*th sensor, x_j^i, can be written as [15, 16]

$$x_j^i = \begin{cases} n_j^i & H_0 \\ \sqrt{\gamma_j}\, P_j^i + n_j^i & H_1 \end{cases} \quad (1)$$

where n_j^i is the received noise sample at the *j*th sensor. The parameter $\sqrt{\gamma_j}\ p_j^i$ belongs to the PU signal with a power value g_j. The noise and PU signal samples (n_j^i, p_j^i) are assumed to γ_j be identically independent distributed Gaussian random variables with zero mean and unit variance. Therefore, γ_j can be defined as the average SNR of PU signal at the *j*th spectrum sensor. We further assume that the CR sensors are randomly deployed in a small area and both PU and PUEA transmitters are relatively far away from the CR network. Hence, the average SNR is almost the same for each CR receiver. Thus, the index j is omitted from γ_j. With regard to the equation (1) and considering the above assumptions, the received signal x_j^i is a Gaussian distributed variable as [15],

$$x_j^i \sim \begin{cases} \mathcal{N}(0,1) & H_0 \\ \mathcal{N}(\gamma+1,1) & H_1 \end{cases} \quad (2)$$

Furthermore, each CR sensor uses M samples for its local energy detection. The decision statistics associated with the output of an energy detector for *j*th CR E_j is obtained as follows:

$$E_j = \sum_{i=1}^{M} \left| x_j^i \right|^2 \sim \begin{cases} a_j & H_0 \\ (\gamma+1) b_j & H_1 \end{cases} \quad (3)$$

where two parameters a_j and b_j are two central Chi-square distributed random variables with M degrees of freedom. But, according to the Central Limit Theorem, when M is large enough (i.e., $M > 10$), E_j can be approximated as a Gaussian random variable as follows [17]:

$$E_j \sim \begin{cases} \mathcal{N}(\mu_0, \sigma_0^2) & H_0 \\ \mathcal{N}(\mu_1, \sigma_1^2) & H_1 \end{cases} \quad (4)$$

where

$$\mu_0 = M, \quad \sigma_0^2 = 2M$$
$$\mu_1 = M(\gamma+1), \quad \sigma_1^2 = 2M(\gamma+1)^2$$

The measured energy of each sensor is compared with a predefined threshold T and then the CR sensor makes a binary decision u_j about the PU channel status: $u_j = 1$ (the channel is occupied) if $E_j > T$ and $u_j = 0$ (the PU channel is vacant) otherwise. The obtained binary decision of the *j*th sensor u_j is sent to the FC. The communication channel between the CR users and FC is assumed to be an error-free reporting channel. The probabilities of PU signal detection and false alarm are computed by

$$p_d = p\left(u_j = 1 \middle| H_1\right) = p\left(E_j > T \middle| H_1\right) = Q\left(\frac{T-\mu_1}{\sigma_1}\right)$$
$$p_{fa} = p\left(u_j = 1 \middle| H_0\right) = p\left(E_j > T \middle| H_0\right) = Q\left(\frac{T-\mu_0}{\sigma_0}\right) \quad (5)$$

where $Q(.)$ is the tail probability of standard normal distribution.

Cooperative Spectrum Sensing

After comparing the local received energy E_j with a threshold T, a binary decision of each sensor is sent to the FC. The FC fuses the received decisions by using the K-out-of-N rule (voting rule) to make a global decision about the PU activity. In the K-out-of-N rule, all of the binary sensing reports are collected and compared with the threshold value K. A threshold value N is an AND fusion rule, a threshold 1 is an OR rule and N/2 is a majority fusion rule.

The AND fusion rule announces the occupancy of the PU channel only when all of the CR sensors report PU signal presence. For the AND rule the global detection and false alarm probabilities are calculated as [18]:

$$Q_d = (p_d)^N \ ; \quad Q_{fa} = (p_{fa})^N \quad (6)$$

The global error probability is defined as the average of detection and false alarm probabilities by each hypothesis:

$$Q_e = Q_{fa} p(H_0) + (1 - Q_d) p(H_1) \quad (7)$$

The AND rule has a very low false alarm rate which makes an efficient spectrum utilization, however it may not protect the PU from strong interferences from the CR users.

$$Q_{fa} \to 0 \ , \quad Q_d \to 0$$
$$Q_e \approx p(H_1) \quad (8)$$

For the OR fusion rule, the global detection and false alarm probabilities at the FC are respectively given by:

$$Q_d = 1 - (1 - p_d)^N \ ; \quad Q_{fa} = 1 - (1 - p_{fa})^N \quad (9)$$

The OR rule has a very high detection probability which is helpful to protect the PU. In contrary, it has a relatively high false alarm probability which makes an inefficient spectrum consumption.

$$Q_{fa} \to 1 \ , \quad Q_d \to 1$$
$$Q_e \approx p(H_0) \quad (10)$$

In the majority fusion rule, the FC confirms the presence of the PU signal when at least half the of sensors report the occupancy of the PU channel. The majority rule has a compromised characteristic of OR and AND rules and its detection and false alarm probabilities are

$$Q_d = \sum_{l=N/2}^{N} \binom{N}{l} p_d^{\,l} (1-p_d)^{N-l}$$
$$Q_{fa} = \sum_{l=N/2}^{N} \binom{N}{l} p_{fa}^{\,l} (1-p_{fa})^{N-l} \quad (11)$$

In the current study, we present the K-out-of-N rule which leads the presence of a PU signal when more than K sensors out of N sensors confirm the presence of PU signal. The global detection and false alarm probabilities the of the K-out-of-N rule are respectively given by:

$$Q_d(K) = \sum_{l=K}^{N} \binom{N}{l} p_d^{\,l} (1-p_d)^{N-l}$$
$$Q_{fa}(K) = \sum_{l=K}^{N} \binom{N}{l} p_{fa}^{\,l} (1-p_{fa})^{N-l} \quad (12)$$

The Proposed Optimal K-out-of-N Rule Under PUEA

Based on the presence of the PUEA and with regard the proposed system model, two different possible hypotheses can be expressed as:

$$\begin{cases} H_0: & \text{PUEA} + \text{Noise} \\ H_1: & \text{PU} + \text{Noise} \end{cases}$$

The first state H_0 occurs when the PUEA transmits the fake signals in vacant frequency bands. In this case, the parameter x_j^i can be formulated as:

$$x_j^i = \begin{cases} \sqrt{\lambda_j}\, e_j^i + n_j^i & H_0 \\ \sqrt{\gamma_j}\, P_j^i + n_j^i & H_1 \end{cases} \quad (13)$$

where the parameter $\sqrt{\lambda_j}\, e_j^i$ is the received PUEA signal with the power λj. The parameter $\rho = \lambda/\gamma$ is considered as PUEA strength. For a more powerful PUEA, we obtain a larger value of ρ. Obviously, in the absence of PUEA ($\rho = 0$), the hypothesis H_0 corresponds to the state H_0. As mentioned before, in the presence of the PUEA, we have

$$x_j^i \sim \begin{cases} \mathcal{N}(\lambda + 1, 1) & \overline{H_0} \\ \mathcal{N}(\gamma + 1, 1) & H_1 \end{cases} \quad (14)$$

and

$$E_j = \sum_{i=1}^{M} \left| x_j^i \right|^2 \sim \begin{cases} (\lambda+1)a_j & \overline{H_0} \\ (\gamma+1)b_j & H_1 \end{cases} \quad (15)$$

Thus,

$$E_j \sim \begin{cases} \mathcal{N}(m_0, v_0^2) & \overline{H_0} \\ \mathcal{N}(\mu_1, \sigma_1^2) & H_1 \end{cases} \quad (16)$$

where

$$m_0 = M(\lambda+1) = M(\rho\gamma+1), \quad v_0^2 = 2M(\lambda+1)^2 = 2M(\rho\gamma+1)^2$$
$$\mu_1 = M(\gamma+1), \quad \sigma_1^2 = 2M(\gamma+1)^2$$

In this case, the false alarm probability will be changed and can be written as:

$$\begin{aligned} p_{fa}(\rho) &= p\left(E_j > T \middle| H_0\right) \\ &= p\left(E_j > T \middle| H_0, E^{on}\right) p\left(E^{on} \middle| H_0\right) \\ &+ p\left(E_j > T \middle| H_0, E^{off}\right) p\left(E^{off} \middle| H_0\right) \\ &= p\left(E_j > T \middle| H_0\right) = Q\left(\frac{T - m_0}{v_0}\right) \end{aligned} \quad (17)$$

With regard the proposed system model, we have

$$p\left(E^{on} \middle| H_0\right) = 1$$
$$p\left(E^{off} \middle| H_0\right) = p\left(E^{on} \middle| H_1\right) = 0$$

Assuming the presence of PUEA in vacant frequency bands, the parameter P_{fa} is parameterized by attack strength ρ. Thus, the FC needs to be estimate of attack parameter ρ to obtain an optimal threshold K_{opt} in the K-out-of-N rule. In the initial stages of the cooperative sensing, the measured energies of all CR users are sent to the FC and the FC calculates the average of the received sensing reports to derive the attack strength ρ.

The average value of received energy reports $\mathfrak{M}$ is defined as

$$\mathfrak{M} = \frac{1}{N} \sum_{j=1}^{N} E_j \quad (18)$$

The mathematical expectation of $\mathfrak{M}$ is

$$\mathrm{E}(\mathfrak{M}) = \frac{1}{N} \sum_{j=1}^{N} \mathrm{E}(E_j) \quad (19)$$

where

$$\begin{aligned} \mathrm{E}(E_j) &= \mathrm{E}(E_j | H_0) p(H_0) + \mathrm{E}(E_j | H_1) p(H_1) \\ &= m_0 p(H_0) + \mu_1 p(H_1) \end{aligned} \quad (20)$$

It should be noted that $p(H_0) = p(H_0)$,thus,

$$\begin{aligned} \mathrm{E}(\mathfrak{M}) &= M(\lambda+1)p(H_o) + M(\gamma+1)p(H_1) \\ &= M(\rho\gamma+1)p(H_o) + M(\gamma+1)p(H_1) \\ &= M\rho\gamma\, p(H_o) + M(1+\gamma p(H_1)) \end{aligned} \tag{21}$$

From the above equations, the values of unknown attack strength ρ is estimated as

$$\hat{\rho} = \frac{\mathrm{E}(\mathfrak{M}) - A}{B} \tag{22}$$

where two parameters A and B are defined as

$$A = M(1+\gamma p(H_1))$$
$$B = M\gamma p(H_o)$$

After the estimation of the parameters ρ, the FC obtain an optimal threshold K_{opt} in the K-out-of-N rule to minimize the total error probability. Assuming that $Q_e(K)$ represents a single minimum, the optimum value of K will be obtained based on the following optimization problem

$$K_{opt}(\rho) = \arg\min_K (Q_e(K)) \tag{23}$$

By substituting (12) into (7), the global error probability $Q_e(k)$ is rewritten as:

$$\begin{aligned} Q_e(k) = {} & p(H_0)\left[\sum_{l=K}^{N}\binom{N}{l} p_{fa}{}^{l}(1-p_{fa})^{N-l}\right] \\ & + p(H_1)\left[1-\sum_{l=K}^{N}\binom{N}{l} p_d{}^{l}(1-p_d)^{N-l}\right] \end{aligned} \tag{24}$$

As $Q_e(K)$ is a convex function of K, we use a simple linear equation

$$\nabla Q_e(K_{opt}) = Q_e(K_{opt}) - Q_e(K_{opt}-1) \approx 0 \tag{25}$$

Substitution of (24) to (25) gives the following result

$$\left(\frac{p_d}{p_{fa}}\right)^{K_{opt}} \left(\frac{1-p_d}{1-p_{fa}}\right)^{N-K_{opt}} = \frac{p(H_0)}{p(H_1)} \tag{26}$$

Taking the logarithm on (26), K_{opt} is obtained as

$$K_{opt}(\rho) = \frac{\log(\psi^N \frac{p(H_0)}{p(H_1)})}{\log(\psi\varphi)} \tag{27}$$

where

$$\psi = \frac{1-p_{fa}}{1-p_d} \quad ; \quad \varphi = \frac{p_d}{p_{fa}}$$

It should be noted that the two parameters ψ and φ depend on the probabilities p_d and p_{fa}. Hence, the false alarm probability p_{fa} is parameterized by attack strength ρ. Therefore, for different values of and ρ, we will have different values for K_{opt}.

Simulation Results

In the considered CR network model, there are $N = 20$ cooperative CR sensors. Each sensor uses $M = 30$ samples for its local spectrum sensing. The local false alarm probability of each sensor is considered to be 0.1 to obtain the local detection threshold *T*. The average SNR of each sensor received from PU signal (γ) is assumed to be -5 dB. The two probabilities $p(H_0)$ and $p(H_1)$ are considered as 0.8 and 0.2, respectively.

Figures 3 and Figure 4 show the estimation of attack strength for $\rho = 0.3$ and $\rho = 0.7$, respectively. The obtained values for ρ are reached to the constant values after using almost 200 iterations of spectrum sensing. Therefore, in computer simulation, we use about 200 sensing intervals in the initial stage to estimate the attack strength and then apply the K-out-of-N fusion rule to achieve an optimal threshold K that minimizes the global error probability.

Figure 5 displays the total error probability versus threshold K for No-Attack scenario and several different values of attack strength. It is clearly shown that for a given values of ρ there is an optimum value of K that indicates the minimum global error probability and confirms the convexity of equation (23).

Figure 6 depicts the total error probability versus the attack strength ρ. In the conventional hard decision combining schemes (AND rule, OR rule and the Majority Fusion Rule), in-

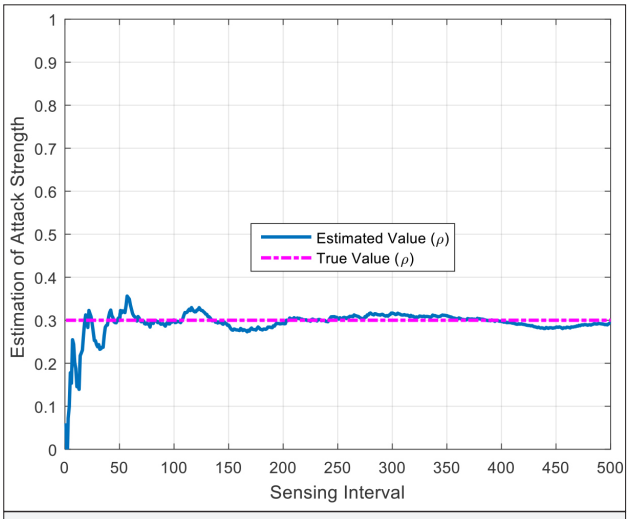

Figure 3. The convergences of attack parameters ($\rho = 0.3$)

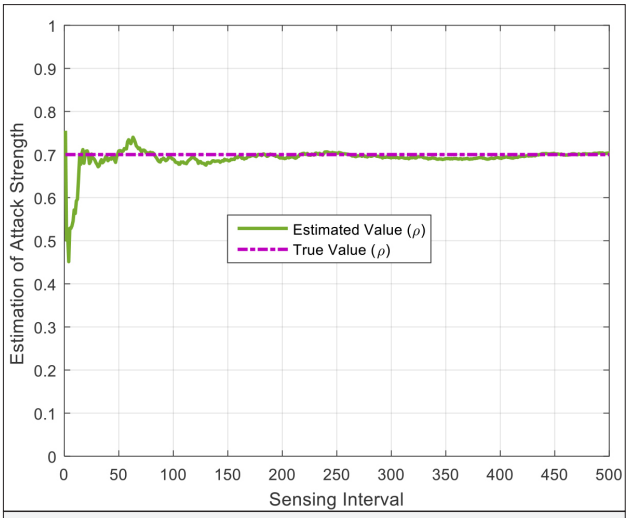

Figure 4. The convergences of attack parameters ($\rho = 0.7$)

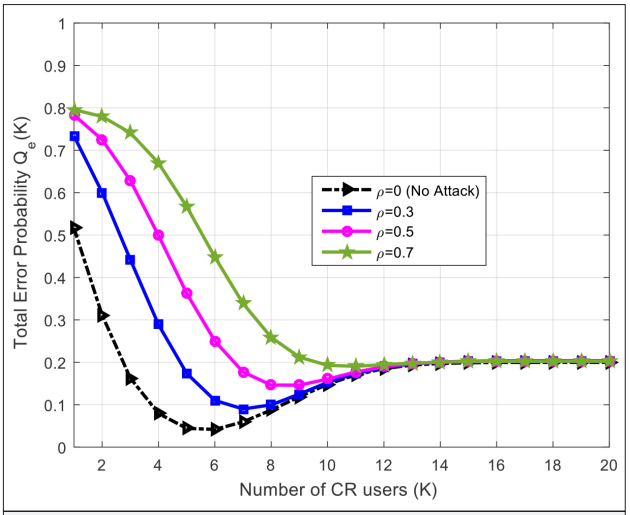

Figure 5. Probability of error versus **K** for several different values of ρ

creasing the attack strength causes high error probability. The obtained error probabilities for AND and OR fusion rules are independent of attack strength ρ and they are fixed in constant values $p(H_1)$ and$p(H_1)$, respectively. This confirms equations (8) and (10). In contrast, with the proposed method, increasing attack strength yields a slight change in total error probability.

Conclusion

This study has investigated the Primary User Emulation Attack (PUEA) in Cognitive Radio (CR) networks. In our scheme, a smart and malicious PUEA was assumed, in which, the attacker carefully senses the spectrum and sends its fake signal in the vacant frequency bands. In the initial stage of Cooperative Spectrum Sensing (CSS), the CR sensors sent their measured energies to the Fusion Center (FC) and the FC estimated the attack strength. The attack strength was defined as the ratio

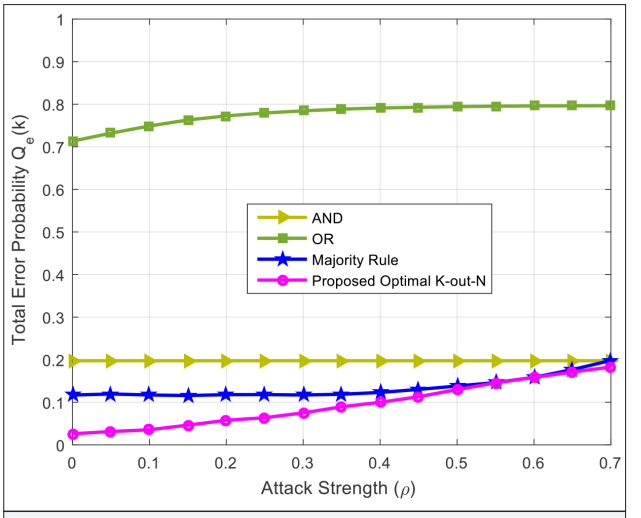

Figure 6. Probability of error versus attack strength (ρ)

of the average transmission power of the malicious attacker to the average emitted power of the legitimate PU. After estimation of the attack strength, the CR users sent their hard one bit decision about PU signal presence to the FC. The FC applied the estimated attack strength in the K-out-of-N fusion rule to obtain an optimal threshold K that minimizes the global error probability. Computer simulation results depicted that the proposed method provides less error detection probability compared with other hard decision combining schemes such as AND, OR, and majority fusion rules.

Peer-review: Externally peer-reviewed.

Conflict of Interest: The authors have no conflicts of interest to declare.

Financial Disclosure: The authors declared that this study has received no financial support.

References

1. J. Mitola, G. Q. Maguire, "Cognitive radio: making software radios more personal", *IEEE Personal Communication*, vol. 6, no. 4, pp. 13-18, 1999.
2. S. Haykin, "Cognitive radio: brain-empowered wireless communications", *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201-220, 2005.
3. I. F. Akyildiz, B. F. Lo, R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical Communication*, vol. 4, no. 1, pp. 40-62, 2011.
4. R. Chen, J. M. Park, Y. T. Hou, J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks,"*IEEE Communications Magazine*, vol. 46, no. 4, pp. 50-55, 2008.
5. A. A. Sharifi, M. J. Musevi Niya, "Defense against SSDF attack in cognitive radio networks: attack-aware collaborative spectrum sensing approach", *IEEE Communications Letters*, vol. 20, no. 1, pp. 93-96, 2016.
6. A. A. Sharifi, M. Sharifi, J. Musevi Niya, "Reputation-based Likelihood Ratio Test with Anchor Nodes Assistance", International Symposium on Telecommunications, 2016.

7. A. A. Sharifi, J. Musevi Niya, "Securing collaborative spectrum sensing against malicious attackers in cognitive radio networks", *Wireless Personal Communications*, vol. 90, no. 1, pp. 75-91, 2016.
8. C. Chen, H. Cheng. H, Y.D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, 2135-2141, 2011.
9. 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*, vol. 62, no. 2, pp. 205-211, 2016.
10. R. Yu, Y. Zhang, Y. Liu, S. Gjessing, M. Guizani, "Securing cognitive radio networks against primary user emulation attacks", *IEEE Network*, vol. 30, no. 6, pp. 62-69, 2016.
11. 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 and Fuzzy Systems*, vol. 28, no. 3, pp. 1281-1290, 2015.
12. 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)*, vol. 70, no. 1, 95-104, 2016.
13. M. Sharifi, A. A. Sharifi, M. J. M. Niya, "Cooperative spectrum sensing in the presence of primary user emulation attack in cognitive radio networks: multi-level hypotheses test approach," Wireless Networks, vol. 24, no. 1, pp. 61-68, 2018.
14. M. Ghaznavi, A. Jamshidi, "Defence against primary user emulation attack using statistical properties of the cognitive radio received power", *IET Communications*, vol. 11, no. 9, pp. 1535-1542, 2017.
15. J. Ma, G. Zhao, Y. Li, "Soft combination and detection for cooperative spectrum sensing in cognitive radio networks", *IEEE Transactions on Wireless Communications*, vol. 7, no. 11, pp. 4502-4507, 2008.
16. M. Sharifi, A. A. Sharifi, M. J. M. Niya, "A new weighted energy detection scheme for centralized cognitive radio networks", International symposium on telecommunications, 2014.
17. F.F. Digham, M.S. Alouini, M.K. Simon, "On the energy detection of unknown signals over fading channels", *IEEE International Conference on Communications*, vol. 5, pp. 3575–3579, 2003.
18. P. K. Varshney, "Distributed detection and data fusion," Springer-Verlag, 1997.

Abbas Ali Sharifi received the B.Sc. degree in electronic engineering from Amir Kabir University of Technology and the M.Sc. and Ph.D. degrees in telecommunication engineering from Malek Ashtar University of Technology and University of Tabriz, respectively. His current research interests include wireless communication and networking, cognitive radio, security, and signal processing.

Mohammad Mofarreh-Bonab received the B.Sc. and M.Sc. degrees both in telecommunication engineering from K.N.Toosi University of technology (KNTU) and Iran university of Science and technology (IUST), respectively. His research interests span the areas of wireless communications, image and video processing, signal processing, cognitive radio and Image compression.