I.J. Wireless and Microwave Technologies, **2023, 3, 14-25**
Published Online on June 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2023.03.02

A Technique for PUE Detection and Isolation in Cognitive Radio Network

Samuel A. Adebo
Department of Telecommunication Engineering, Federal University of Technology Minna, Nigeria
E-mail: adebosamuel@yahoo.com
ORCID iD: https://orcid.org/0000-0002-7695-4893

Elizabeth N. Onwuka
Department of Telecommunication Engineering, Federal University of Technology Minna, Nigeria
E-mail: onwukaliz@futminna.edu.ng
ORCID iD: https://orcid.org/0000-0002-5981-272X

Abraham U. Usman
Department of Telecommunication Engineering, Federal University of Technology Minna, Nigeria
E-mail: usman.abraham@futminna.edu.ng
ORCID iD: https://orcid.org/0000-0002-3154-5156

Supreme Ayewoh Okoh*
Department of Software Engineering, Veritas University Abuja, Nigeria
E-mail: okohsa@veritas.edu.ng
ORCID iD: https://orcid.org/0000-0001-6354-0424
*Corresponding Author

Okwudili Onyishi
Department of Electrical and Electronics Engineering, Federal University of Technology Minna, Nigeria
E-mail: okwudilionyishi653@gmail.com
ORCID iD: https://orcid.org/0000-0002-7830-4771

Received: 14 November, 2022; Revised: 12 December, 2022; Accepted: 07 March, 2023; Published: 08 June, 2023

Abstract: The primary aim of a cognitive radio (CR) system is to optimize spectrum usage by exploiting the existing spectrum holes. Nevertheless, the success of cognitive radio technology is significantly threatened by the primary user emulation attack (PUEA). A rogue secondary user (SU) known as the primary user emulator (PUE) impersonates a legitimate primary user (PU) in a PUEA, thereby preventing other SUs from accessing the spectrum holes. Which leads to the decrease in quality of service (QoS), connection undependability, degraded throughput, energy depletion, and the network experiences a deterioration in its overall performance. In order to alleviate the impact of PUEA on Cognitive Radio Networks (CRNs), it is necessary to detect and isolate the threat agent (PUE) from the network. In this paper, a method for finding and isolating the PUE is proposed. MATLAB simulation results showed that the presence of PUE caused a significant decrease in the throughput of SUs, from 7×10^{-1} to 56×10^{-2}. The throughput was highest at a false alarm (FA) probability of 0.0, indicating no PUE, and decreased as the FA probability increased. At a FA probability of 1, the throughput reached zero, indicating complete takeover of the spectrum by PUE. By isolating the PUE from the network, the other SUs can access the spectrum holes, leading to increased QoS, connection reliability, improved throughput, and efficient energy usage. The presented technique is an important step towards enhancing the security and reliability of CRNs.

Index Terms: Spectrum, user, isolation, emulator, attack.

1. Introduction

The concept behind a cognitive radio network (CRN) involves allowing secondary users (SUs) to utilize the

authorized spectrum of primary users (PUs) when it is not in use. This is achieved by designing the network to detect when the primary users are idle, thereby enabling the SU to have access to the white space [1–3]. But, as a result of multipath fading, shadowing, and receiver uncertainty problems, the performance of signal detection is occasionally truncated. Thus, cooperative sensing is used to address these challenges [4–7]. There are two categories of cooperative spectrum sensing (CSS) viz; centralized and decentralized spectrum sensing. In centralized spectrum sensing, a fusion centre (FC) uses the results from the sensing of the SU to finally decide on the spectrum's state. However, in decentralized cooperative spectrum sensing, SUs exchange their sensed data among themselves, and each SU makes its judgment based on the sensed data [8–13].To prevent SUs from interfering with PUs, CRNs implement spectrum sensing techniques that detect the presence of PUs. Despite this, a significant challenge in CRNs is the emergence of primary user emulation (PUE) attacks, which involve malicious users mimicking the transmission patterns of PUs to disrupt network operations. PUE refers to the malicious act of an SU pretending to be a PU by mimicking its transmission patterns [14–16]. PUE attacks can be launched by an adversary with the intention of denying legitimate SUs access to the spectrum or causing interference to PUs. PUE attacks can be challenging to detect as the attacker can mimic the PU's transmission patterns accurately. Moreover, the attacker can adjust its transmission power and timing to avoid detection by the SUs. As a result, PUE attacks can lead to significant performance degradation in CRNs.

The detection and isolation of PUE attacks in a CRN are crucial for the reliable and secure operation of the network. The detection and isolation of PUE attacks can help ensure that the spectrum is available for legitimate users. Similarly, PUE attacks can deny legitimate secondary users (SUs) access to the spectrum, leading to a waste of valuable spectrum resources. PUE attacks can cause interference to primary users (PUs), leading to degraded performance or even failure of the primary communication system [17, 18]. Detecting and isolating PUE attacks can protect PUs from such interference. More so, PUE attacks can cause incorrect spectrum sensing results, leading to erroneous decisions by SUs. Detecting and isolating PUE attacks can improve the reliability of spectrum sensing. PUE attacks can be launched by malicious users to disrupt the operation of the CRN or steal sensitive information. Detecting and isolating PUE attacks can help maintain network security and prevent such attacks.

The detection and isolation of PUE involve identifying and distinguishing them from legitimate users, as well as preventing their unauthorized access to the spectrum. By doing so, the cognitive radio network can present a level ground for all secondary users, this will in turn improve the network's overall performance and reduce interference, leading to better user experience and greater spectral efficiency. To mitigate the problem of PUE, researchers have proposed several techniques such as cooperative spectrum sensing, intelligent jamming, and authentication-based approaches. These techniques aim to increase the reliability and accuracy of spectrum sensing and detect PUE attacks in real-time.

This paper presents two algorithms designed to detect and isolate primary user emulators in a CRN. The algorithms were simulated on MATLAB and validated using throughput and FA probabilities. The structure of this manuscript is as follows. The second section encompasses an assessment of prior research and their methods of dealing with PUE attacks in a CRN. In section 3, the paper presents the proposed methodology, and section 4 scrutinizes the results obtained from the simulation. Lastly, the fifth section brings the paper to a close.

2. Related Works

Undoubtedly, cognitive radio (CR) technology presents a novel method to enhance the utilization of available spectrum. However, several impediments have surfaced that impede the effective implementation of this technology, ultimately compromising the system's overall efficiency. These issues include PUEA and falsification of spectrum sensing data, among others, as identified in literature [19]. Among these, primary user emulation attack (PUEA) is deemed highly hazardous [20]. PUEA represents a more active technique for spectrum sensing where assailants imitate and transmit an indistinguishable primary signal during sensing. With the presence of an imitated primary signal, secondary access to the sensed channel may be instantly denied. PUEAs are attacks where a secondary user tries to emulate the signal of a primary user to gain access to a spectrum band for their own benefit, which can be either selfish or malicious in nature. Selfish PUEAs may attempt to take over a spectrum band to monopolize it for their own use, which undermines the impartiality of the secondary access of the CR system. This is because other secondary users are prevented from accessing the spectrum band, which can limit the overall efficiency and effectiveness of the CR system. On the other hand, malicious PUEAs may attempt to disrupt the functionality of the CR network by causing harmful interference or denial of service attacks.

Several studies have scrutinized the difficulties of PUE problem and posited an array of solutions for managing the problem. Authors have presented a surveillance technique in [19] and [21] for determining the identity of the PU and the mischievous PUE attacker. Additionally, an auxiliary perception process was instigated to detect supplementary prospects for accessing the channel and subsequently decreasing the impact of the malevolent PUE attacker [22]. By employing game theory-based scrutiny and demonstrating the Nash equilibrium, they have uncovered the fitting techniques for deploying their technology. In addition, in [1] and [4], the authors have advocated for a technique called "inactive, nonparametric classification," which can pinpoint the concentration of devices communicating within the PU spectrum. The authors in [20] introduce a passive technique where the perception mechanism observes and accumulates signals without introducing any signals into the wireless channel. As the count of active devices does not need to be

pre-established, it is thus nonparametric. Characteristics that are not channel-reliant were employed to establish fingerprints for the devices, which can't be changed subsequently. To recognize the gathered fingerprints, a modified collapsed Gibbs sampling technique and the infinite Gaussian mixture model (IGMM) were employed.

In [23], the frequency domain-based action recognition approach was applied to evaluate the FFT sequences of signals transmitted in a CRN setting. The researchers leveraged an artificial neural network and a relational database to classify the signals' behavior. Energy detection was utilized to identify potential primary user emulators in a specific frequency range. The motion-related feature vectors of the PUs within this frequency spectrum were captured using a relational database system. It is considered that a transmission comes from the PUE when it is intercepted and there is no database match. Similar to this, the authors in [24] presented three (3) different methods: Constellation-Based Distinct Native Attribute (CB-DNA), Signal Watermarking, and RF-DNA for identifying and countering PUE attacks. RF-DNA fingerprinting uses a constant Area of Interest (ROI) for all transmissions, including preambles, pilot tones, etc., to extract differentiating information from RF signals. Using Time-Domain (TD) RF-DNA fingerprints, the genuine source of transmission was correctly identified with 78% accuracy in a test scenario involving 15 devices. CB-DNA fingerprinting identifies radio emissions by computing the statistical characteristics of the received signal projected into a constellation space. The manufacturer, model, serial number, and other device-specific data may be obtained using these properties. In a test case using 15 devices, the average accurate categorization rate using CB-DNA fingerprints was 95%. In order to exchange a Hash-Based Message Authentication Code (HMAC) that verifies the signal's source, the watermarking method establishes a side channel. The constructed side-channel ensures a dependable communication link even in conditions of low Signal to Noise-Ratio (SNR).

The author in [25] suggested a higher-order statics-based PUEA detection method that can replicate the PU and PUE attackers' network information. Between the PU and the PUE, different fading channel situations such as Rayleigh, Rician, and Nagagammi were examined. The PUE detection performance was evaluated on this basis. Second and fourth-order moments, as well as their cumulants, were also used in the method. It is a less sophisticated and accurate approach that may be utilized in fading conditions when the received signal intensity fluctuates rapidly and the old RSSI-based method cannot provide better PUEA identification. The authors in [26] also developed a spectrum sensing system for low-noise environments as well as a tri-layered strategy to reduce the PUEA in the CR's physical layer. Three different methods were used to create the tag. DNA and the chaotic algorithm were used to produce sequences. The first seed value for the production of gold codes was then derived from these sequences. The authentication tag was the final result of the generator's output. The identification of the malicious user through the use of this technique mitigated the impact of PUEA on the CRN.

From literature, it is revealed that though a number of works have been done on the sensing of PUE using various approaches, no effort has been made in its isolation from the CRN. This work presents a simplified detection and isolation approach of PUE in a CRN.

3. Methodology

This section explains the methodology for the proposed PUE isolation. To achieve this, the methodology uses a system model that represents the CRN, including the devices that are authorized to use the radio spectrum and those that are not. The model includes inputs such as the radio frequency (RF) environment, the authorized PU transmissions, and the unauthorized PUE transmissions. The model is used to simulate the expected RF environment for the cognitive radio network under normal operating conditions. This section also discusses the detection and isolation algorithms design.

3.1 System Model

Fig.1 depicts the proposed PUE isolation method which involves the primary user (PU), secondary base station (SBS), secondary users (SUs), and the potentially interfering user equipment (PUE). The SUs are equipped with location awareness and are cognizant of the locations of both the PU and PUE. The system is comprised of two components - PUE detection and PUE isolation. PUE detection is accomplished by using the results of each SU's sensing experiment. Each SU locates the transmitter, calculates the distance to it, and determines the signal's angle of arrival (AoA). The method used to differentiate between a legitimate PU and a PUE involves comparing the known distance and AoA of the PU with that of the SUs. If the expected distance and AoA match those of the PU, then the transmitter is identified as the PU. Else, it is identified as the PUE. The SUs transmits the SUs information regarding the location. Using data from SUs, the SBS calculates the transmitter's accurate position before comparing it to the PU's known location [27]. Any deviation from the PU's well-known position indicates that the emitter is a PUE.

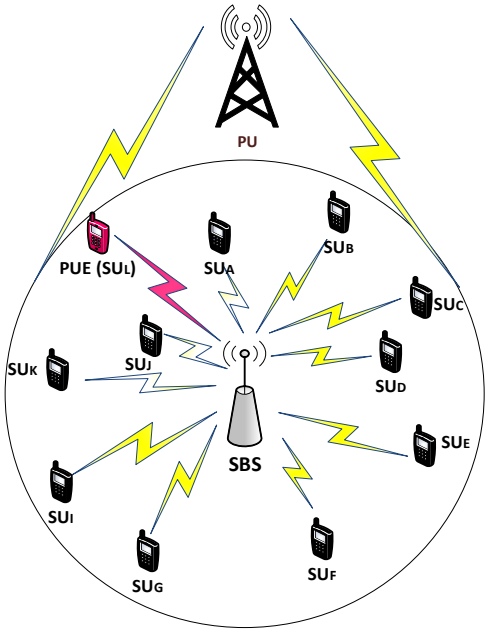

Fig. 1. System model

Fig. 2 shows the configuration of a typical PUEA, in which the PUE sends out a signal that is received by all SUs within that network.

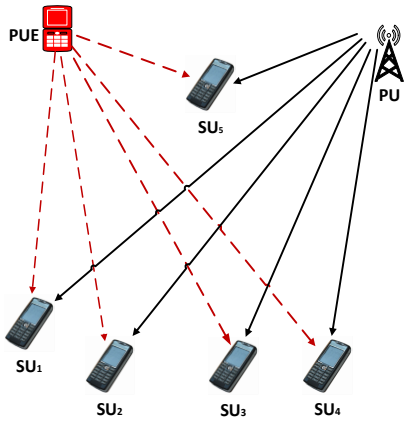

Fig. 2. PUE Attack Scenario [3]

3.2 Energy Detection

As there is often a lack of information regarding the PUE signal, energy detection is commonly employed as a detection technique. This method involves utilizing various parameters such as test statistic $T_i(x)$, binary hypothesis testing $x_i(m)$, detection probability P_{di}, FA probability p_{fi}, and missed detection probability P_{mi} to identify the presence of PUE attacks in the CRN presented in (1), (2), (4), (6), and (7) respectively [8].

$$T_i(x) = \frac{1}{N}\sum_{m=1}^{N} |\, x_i(m)\,|^2 \tag{1}$$

$$x_i(m) = \begin{cases} u_i(m) & ; H_0 \\ s_i(m)+u_i(m) & ; H_1 \end{cases} \tag{2}$$

In the process of energy detection, the samples collected by SU are denoted by m = 1, 2, 3, ...N. Where N indicates total number of samples. The received signal at the i^{th} SU is denoted as $x_i(m)$, where i = 1, 2, 3, ..., up to K. The signal of the PUE is represented by $S_i(m)$ and has zero mean with a variance of σ_s^2. The white Gaussian noise is denoted by

$u_i(m)$ and has a mean of 0 and a variance of σ_n^2. The two hypotheses of H_0 and H_1 are utilized to describe. Where H_0 represents the absence of PUE and H_1, the presence of the PUE signal.

$$P_{di} = P\{T_i(X) > \lambda_i / H_1\} \tag{3}$$

$$p_{di} = Q\left(\frac{\lambda_i - (\sigma_s^2 + \sigma_n^2)}{(\sigma_s^2 + \sigma_n^2)/\sqrt{N/2}}\right) \tag{4}$$

$$p_{fi} = P\{T_i(X) > \lambda_i / H_0\} \tag{5}$$

$$P_{fi} = Q\left(\frac{\lambda_i - \sigma_n^2}{\sigma_n^2/\sqrt{N/2}}\right) \tag{6}$$

$$P_{mi} = 1 - P_{di} \tag{7}$$

$$Q(x) = \frac{1}{\sqrt{2\lambda}}\int_x^{\infty} e^{-\frac{t^2}{2}} dt \tag{8}$$

$$\lambda_i = \sigma_n^2 Q^{-1}(p_{fi})/\sqrt{N/2} + \sigma_n^2 \tag{9}$$

3.3 Sensing and Transmission Times of SU

The secondary base station (SBS) in a cognitive radio network only allocates a detected spectrum hole to a single secondary user (SU) during a specific time period referred to as a time span. As illustrated in Fig.3, this approach is limited to a single SU within a single time span, denoted as T+T1, where T represents the detection time and T1 represents the transmission time. Once the SBS confirms the absence of the primary user, whether accurately or mistakenly, the assigned SU is permitted to transmit within the assigned spectrum hole. [28, 29].

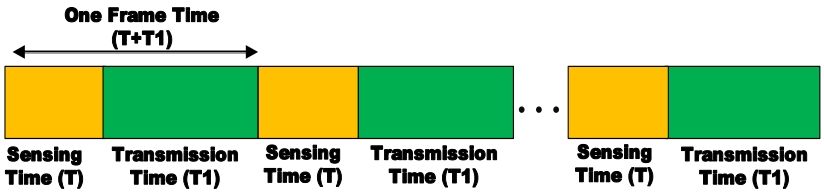

Fig. 3. SU Sensing and transmission time

Equation (10) shows the effective throughput G_i of i^{th} SU transmitting over the unoccupied licensed spectrum.

$$G_i = \frac{T_1}{T + T_1}\left[C_{0i}(1 - p_f)p(H_0) + C_{1i}(1 - p_d)p(H_1)\right] \tag{10}$$

The detecting time is T, while the transmission time is T_1. Under the H_0 and H_1 hypotheses, C_{0i} and C_{1i} are the normalized channel capacities of the white space utilized by ith

Since we know that $P(H_0) > P(H_1)$, $C_{0i} \gg C_{1i}$ and $1-P_f > 1-P_d$ [34], (11) presents the throughput of the ith SU.

$$G_i = \frac{T_i}{T + T_i} C_{0i}(1 - p_f)p(H_0) \tag{11}$$

Fig. 4 [27] illustrates a typical PUE detection situation. (x_1,y_1) and (x_2,y_2) represent the positions of SU_1 and SU_2 respectively. Likewise, $r_1$and r_2 denote the radii of the areas of coverage of SU_1 and SU_2respectively, whereas (x_a,y_a) and (x_b,y_b) denote the points of intersection of the areas of coverage of SU_1 and SU_2. Line PQ links the center of SU_1 to the center of SU_2, while angles ϕ and θ are the angles at which signals get to SU_1 and SU_2 from the PU, respectively. Angles α_1 and α_2 indicate the angles at which the signal from PUE gets to SU_1 and SU_2, respectively.

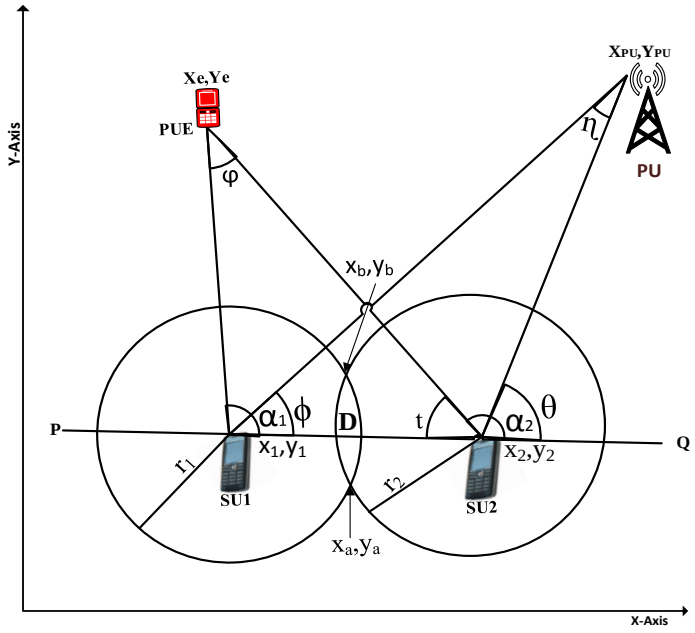

Fig. 4. SU_1 and SU_2 in the detection process

An initial detection result of (0) is assigned to each SU. The reported detection status is 1 when the location of the genuine PU and the $SU's$ detection of the transmitter are in tandem; otherwise, it is 0. As a result, the i[th] SU results of detection can be determined using the formula below:

Transmitter detection is given by (12)

$$tx \in \mathbb{Z} : \mathbb{Z} \to [1,0] \tag{12}$$

Equation (13) shows PU-SU distance for any i[th] SU.

$$d_{i(PU)} = \sqrt{(X_{PU} - x_i)^2 + (Y_{PU} - y_i)^2} \tag{13}$$

$$d_i = \exp\left(\frac{p_t - p_{r(imean)} - p_{loss(d0)}}{10n}\right) \tag{14}$$

Using (16) to calculate the distance for detection, the detection status of the transmitter making use of the distance between i[th] SUs and the transmitter as given in (15).

$$d_{i(tx)} = \begin{cases} 1, \to tx \in \mathbb{Z} \backslash 0 \\ 0, \to tx \in \mathbb{Z} \backslash 1 \end{cases} \tag{15}$$

Similarly, (16) and (17) give AoA of the signal at SU_1 and SU_2 respectively while the detection status is given in (20)

$$\alpha_1 = arc\cos\left(\frac{D^2 + d_1^2 - d_2^2}{2Dd_1}\right) \tag{16}$$

$$\alpha_2 = 180 - \left(\arccos\left(\frac{D^2 + d_2^2 - d_1^2}{2Dd_2}\right)\right) \tag{17}$$

$$AoA_{i(tx)} = \begin{cases} 1, \to tx \in \mathbb{Z} \backslash 0 \\ 0, \to tx \in \mathbb{Z} \backslash 1 \end{cases} \tag{18}$$

Also, using (19) and (20), the PUE's position is calculated, and the detection status is provided by (21)

$$X_e = \frac{x_1 \tan\alpha_1 - x_2 \tan\alpha_2 + y_2 - y_1}{\tan\alpha_1 - \tan\alpha_2} \tag{19}$$

$$Y_e = \tan\alpha_1 \left(\frac{x_1 \tan\alpha_1 - x_2 \tan\alpha_2 + y_2 - y_1}{\tan\alpha_1 - \tan\alpha_2} \right) x_1 \tan\alpha_1 + y_1 \tag{20}$$

$$loc_{i(tx)} = \begin{cases} 1, \rightarrow tx \in \mathbb{Z} \setminus 0 \\ 0, \rightarrow tx \in \mathbb{Z} \setminus 1 \end{cases} \tag{21}$$

A fusion rule utilizing the AND gate is used to infer whether the transmitter is the PU or the PUE based on the detection outcomes of distance, AoA, and location as described in [30]. It's a PU if all of the SBS's computed results are high threshold (1)s; otherwise, it's a PUE and should be isolated. The SBS is expected to provide eight different outcomes for the three inputs (distance, AoA, and location), as shown in the table below (22).

$$output = 2^n \tag{22}$$

where n is the number of inputs. Table 1 shows the final decision on the transmitter's status.

Table 1. Detection decision table

SU-Tx distance	AoA	Location of the Tx	Detection result
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

The SU detection result is set to low (0) if the Tx is PUE and high (1) if the Tx is PU based on the calculation of SU detection parameters. When SBS concludes that all of the findings are high, the transmitter is deemed to be a genuine PU. However, if any of the results is low (0), the Tx is labeled as PUE and hence disconnected from the CRN. The PUE detection algorithm is presented as follows:

1. Each SU computes its distance SU_{dTx} and angle of arrival SU_{aTx} from the transmitter and compares it with the known distance SU_{dPU} and angle of arrival SU_{aPU} from the PU
2. Each SU also calculates the location (x_{tx}, y_{tx}) of the transmitter and compares it with that of the PU (x_{pu}, y_{pu})
3. $if\,(SU_{dTx} = SU_{dPU})$
4. $SU \equiv PU$, $SU_{dTx} = 1$
5. $else\ \ SU \equiv PUE$, $SU_{dTx} = 0$
6. $if\,(SU_{aTx} = SU_{aPU})$
7. $SU \equiv PU$, $SU_{aTx} = 1$
8. $else\ \ SU \equiv PUE$, $SU_{aTx} = 0$
9. $if\,((x_{tx}, y_{tx}) = (x_{pu}, y_{pu}))$
10. $SU \equiv PU$, $(x, y)_{tx} = 1$
11. $else\ \ SU \equiv PUE$, $(x, y)_{tx} = 0$
12. $if\,(SU_{dTx}, SU_{aTx}\ \&(x_{tx}, y_{tx}) = 1)$
13. $SU = PU$
14. $else\ \ SU = PUE$

3.4 Isolation Process

The secondary Base Station (SBS) will cease to select a specific SU to participate in the detection process after it has been verified that it is a PUE. Furthermore, its sensing data will not be used in the detection process, and PUE will not be provided any further information on the network's state or spectrum holes. The detected PUE is thereby removed from the CRNs. Equation (23) is used to select the two SUs that will partake in the detection processes, while the network's participating SUs are identified for communication as (24).

$$2SU_{(signals)} \in \Re : \Re \rightarrow \left[SU_1, SU_2, SU_3, SU_4, ..., SU_N\right] \setminus PUE \tag{23}$$

$$SBS \rightarrow \Re : \Re \in \left[SU_1, SU_2, SU_3, SU_4, ..., SU_N\right] \setminus PUE \tag{24}$$

The isolation algorithm is presented as follows

1. SUs initialize sensing
2. SUs detect signal from Utx, an unknown Tx.
3. SUs estimate the spectral characteristics (S_{utx}) of Utx and compare with that of the PU (S_{pu})
4. $if\,(S_{Utx} = S_{pu})$
5. Run detection algorithm
6. If detection result=1
7. $Utx = PU$
8. Else $Utx = PUE$
9. Isolate Utx
10. Else $Utx \neq PU$
11. SUs continue sensing

The flow process for the isolation algorithm is shown in Figure 5.

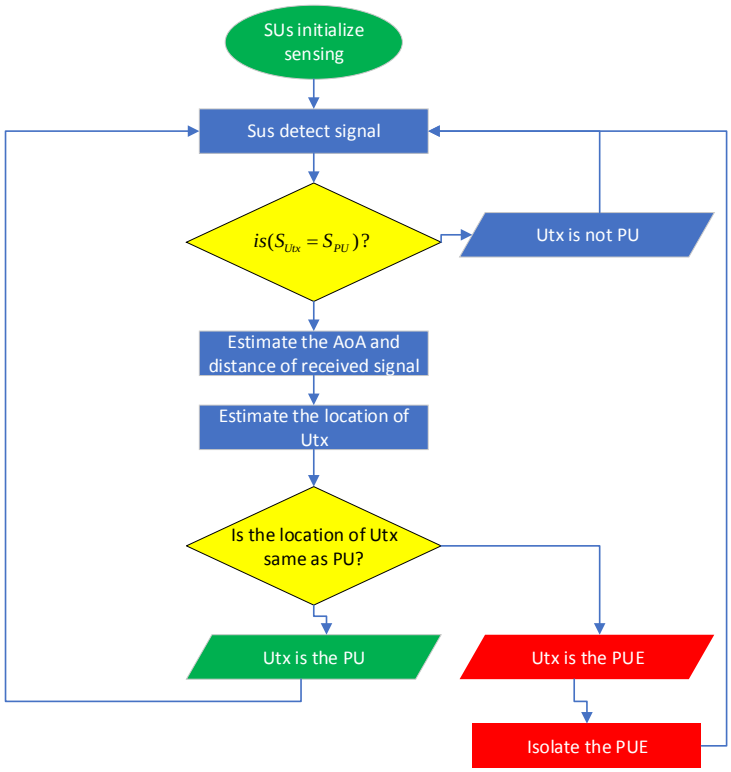

Fig. 5. Isolation Algorithm

4. Result and Discussion

MATLAB simulation of proposed algorithm showed that when PUE is absent, SU transmits for extended periods, resulting in high throughput. However, when PUE arrives with a PU-like signal and the SU interrupts its transmission, the throughput of an SU will be reduced. SU was projected to have a throughput of 104×10^{-2} when transmitting for 25 milliseconds, as shown in Fig.6. However, if SU at any time left the spectrum for PUE, assuming that PUE was the PU, its throughput would drop. With the presence of PUE, for example, during a delay of 25 milliseconds, SU's throughput fell to 84×10^{-2}. Likewise, during SU's 15 millisecond transmission but PUE seized the spectral space and transmitted for the remainder of the time, SU's throughput would be 56×10^{-2} compared to 7×10^{-1} when PUE was absent. Likewise, after 20 milliseconds of SU's transmission when PUE took over the spectrum, throughput fell to 7×10^{-1}, compared to 9×10^{-1} when PUE was not there.

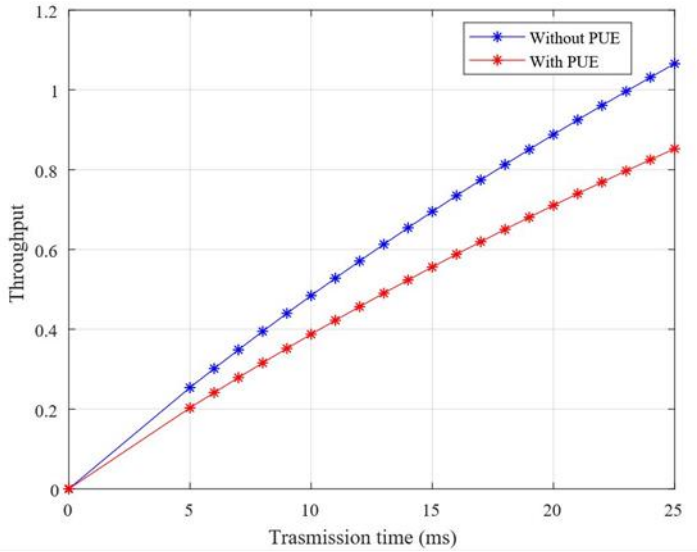

Fig. 6. Effect of PUE on Throughput.

The effect of false alarms (FA) on throughput is depicted in Fig.7. The throughput is 25×10^{-2} when the likelihood of FA is 0.0, which denotes that PUE is absent. Yet when the likelihood of a false alarm rose to 0.2, throughput fell to 20×10^{-2}. The throughput also increased to 15×10^{-2} when the FA probability was raised to 0.4. Yet, throughput was 0 when the FA probability was 1. According to this, the spectrum has been hijacked by the PUE when the likelihood of FA is 1, making the SU's throughput 0 at that time. As a result, decreased throughput results from a higher risk of FA, and vice versa.

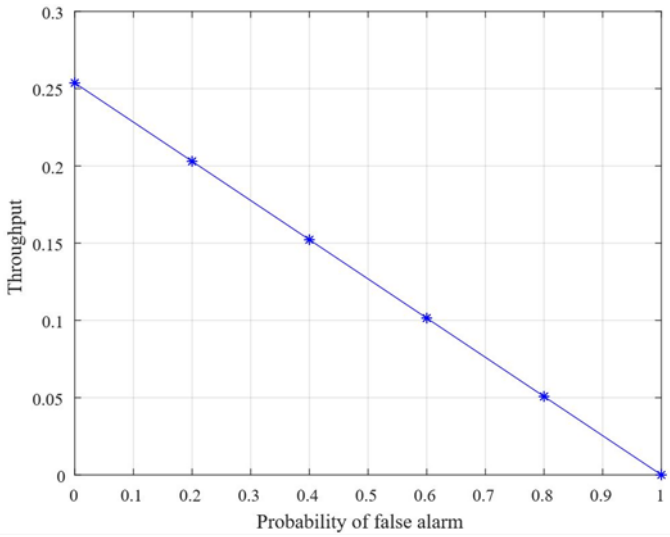

Fig. 7. Relationship between throughput and false alarm.

5. Conclusion

Primary User Emulation (PUE) attack involves a deceitful secondary user masquerading as the authorized primary user, resulting in the evacuation of the spectrum by SUs in favor of the rogue user. This type of attack leads to various negative outcomes such as denial of service, unreliable connections, reduced throughput, wasted bandwidth, and a decline in the quality of service. If left in the network, PUE leads to an eventual collapse of the CRNs. To forestall this and improve the general performance of CRNs, PUE should be isolated from the network when detected. Hence, in this research article, we designed a method to remove PUEs from a cognitive radio network after their detection. MATLAB simulation results indicate that in the presence of PUE, the throughput of SUs dropped to 56×10^{-2}, as compared to 7×10^{-1} when PUE was absent. Additionally, when the false alarm (FA) probability was 0.0, indicating the absence of PUE, the throughput was 25×10^{-2}. However, when the FA probability was increased to 0.2, the throughput dropped to 20×10^{-2}. Similarly, with an increase in the FA probability to 0.4, the throughput decreased to 15×10^{-2}. Finally, when the FA probability was 1, the throughput was 0, indicating that PUE had taken over the spectrum completely. Therefore, it can be concluded that the throughput of SU is reduced by the presence of PUE.

References

[1] M. Ozger and O. B. Akan, "On the utilization of spectrum opportunity in cognitive radio networks," *IEEE Communications Letters*, vol. 20, no. 1. pp. 157–160, 2016.

[2] P. Goyal, A. S. Buttar, and M. Goyal, "An efficient spectrum hole utilization for transmission in Cognitive Radio Networks," in *3rd International Conference on Signal Processing and Integrated Networks, SPIN 2016*, 2016, pp. 322–327.

[3] K. Yadav, S. D. Roy, and S. Kundu, "Total error reduction in presence of malicious user in a cognitive radio network," in *2018 2nd International Conference on Electronics, Materials Engineering and Nano-Technology, IEMENTech 2018*, 2018, pp. 4–7.

[4] X. Li, G. Xie, and J. Gao, "Detection efficiency analysis of cooperative spectrum sensing in cognitive radio networks," *2018 IEEE 4th Int. Conf. Comput. Commun. ICCC 2018*, vol. 15, no. 3, pp. 462–467, 2018.

[5] S. Althunibat, M. Di Renzo, and F. Granelli, "Cooperative spectrum sensing for cognitive radio networks under limited time constraints," *Comput. Commun.*, vol. 43, pp. 55–63, 2014.

[6] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, 2011.

[7] H. Du, S. Fu, and H. Chu, "A Credibility-Based Defense SSDF Attacks Scheme for the Expulsion of Malicious Users in Cognitive Radio," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 9, pp. 269–280, 2015.

[8] C. K. Yu, M. Van Der Schaar, and A. H. Sayed, "Distributed spectrum sensing in the presence of selfish users," *2013 5th IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing, CAMSAP 2013*. pp. 392–395, 2013.

[9] G. Sharma and R. Sharma, "Distributed cooperative spectrum sensing over different fading channels in cognitive radio," in *2017 International Conference on Computer, Communications and Electronics, COMPTELIX 2017*, 2017, pp. 107–111.

[10] W. Khalid and H. Yu, "Optimal sensing performance for cooperative and non-cooperative cognitive radio networks," *International Journal of Distributed Sensor Networks*, vol. 13, no. 11. 2017.

[11] M. G. Khoshkholgh, K. Navaie, and H. Yanikomeroglu, "Outage performance of the primary service in spectrum sharing networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 10. pp. 1955–1971, 2013.

[12] S. Shrivastava and D. P. Kothari, "SU throughput enhancement in a decision fusion based cooperative sensing system," *AEU - Int. J. Electron. Commun.*, vol. 87, no. January, pp. 95–100, 2018.

[13] A. Ashokan and L. Jacob, "Distributed cooperative spectrum sensing with multiple coalitions and non-ideal reporting channel," in *2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems, SPICES 2017*, 2017, pp. 1–6.

[14] R. Sultana and M. Hussain, "Mitigating primary user emulation attack in cognitive radio network using localization and variance detection," in *Smart Innovation, Systems and Technologies*, 2018, vol. 79, pp. 433–444.

[15] N. Saeed, H. Nam, T. Y. Al-Naffouri, and M. S. Alouini, "Primary user localization and its error analysis in 5G cognitive radio networks," *Sensors (Switzerland)*, vol. 19, no. 9. 2019.

[16] Z. El Mrabet, Y. Arjoune, H. El Ghazi, B. A. Al Majd, and N. Kaabouch, "Primary user emulation attacks: A detection technique based on kalman filter," *Journal of Sensor and Actuator Networks*, vol. 7, no. 3. 2018.

[17] R. Yu, Y. Zhang, Y. Liu, S. Gjessing, and M. Guizani, "Securing cognitive radio networks against primary user emulation attacks," *IEEE Network*, vol. 30, no. 6. pp. 62–69, 2016.

[18] K. Philemon Dawar, A. U. Usman, B. Alhaji Salihu, M. David, S. Ayewoh Okoh, and A. Ajiboye, "Comparative Analysis of Macro-Femto Networks Interference Mitigation Techniques," *Int. J. Wirel. Microw. Technol.*, vol. 12, no. 6, pp. 14–24, Dec. 2022.

[19] N. Nguyen Thanh, P. Ciblat, A. T. Pham, and V. T. Nguyen, "Surveillance Strategies Against Primary User Emulation Attack in Cognitive Radio Networks," *IEEE Trans. Wirel. Commun.*, vol. 14, no. 9, pp. 4981–4993, 2015.

[20] N. T. Nguyen, R. Zheng, and Z. Han, "On identifying primary user emulation attacks in cognitive radio systems using nonparametric Bayesian classification," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1432–1445, 2012.

[21] D. Ta *et al.*, "Mitigating Primary Emulation Attacks in Multi-Channel Cognitive Radio Networks : A Surveillance Game To cite this version : HAL Id : hal-01713280 Mitigating primary emulation attacks in multi-channel cognitive radio networks : A surveillance game," 2018.

[22] M. García-Otero and A. Población-Hernández, "Location Aided Cooperative Detection of Primary User Emulation Attacks in Cognitive Wireless Sensor Networks Using Nonparametric Techniques," *J. Sensors*, vol. 2016, 2016.

[23] D. Pu and A. M. Wyglinski, "Primary-user emulation detection using database-assisted frequency-domain action recognition," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4372–4382, 2014.
[24] J. A. Betances, "Physical Layer Defenses Against Primary User Emulation Attacks," p. 109, 2016.
[25] S. Arulselvi, "Higher Order Statics based Primary User Emulation Attack Detection," *Indian J. Sci. Technol.*, vol. 8, no. 32, 2015.
[26] A. Jayapalan and T. Karuppasamy, "Spectrum Sensing and Mitigation of Primary User Emulation Attack in Cognitive Radio," in Cognitive Radio in 4G/5G Wireless Communication Systems, S. S. Moghaddam, Ed. Rijeka: IntechOpen, 2018.
[27] S. A. Adebo, E. N. Onwuka, A. U. Usman, and A. J. Onumanyi, "A hybrid localization scheme for detection of primary user emulator in cognitive radio networks," *International Journal of Computing and Digital Systems*, vol. 8, no. 3. pp. 217–227, 2019.
[28] Y. C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wirel. Commun.*, vol. 7, no. 4, pp. 1326–1337, 2008.
[29] S. Stotas and A. Nallanathan, "On the throughput maximization of spectrum sharing cognitive radio networks," in *GLOBECOM - IEEE Global Telecommunications Conference*, 2010, pp. 0–4.
[30] P. R. Lin, Y. Z. Chen, P. H. Chang, and S. S. Jeng, "Cooperative spectrum sensing and optimization on multi-Antenna energy detection in Rayleigh fading channel," in *2018 27th Wireless and Optical Communication Conference, WOCC 2018*, 2018, pp. 1–5.

Authors' Profiles

Samuel Attai Adebo received B.Eng. degree in electrical and Computer Engineering and M.Eng. degree in Communications Engineering from Federal University of Technology Minna, Nigeria in 2008 and 2013 respectively. He also completed his Ph.D degree in Communications Engineering at the Department of Telecommunications Engineering Department, Federal University of Technology, Minna, Nigeria. Presently he works with the National Examination Council, Nigeria. His research interests include cognitive radio network, spectrum management, and sensing techniques.

Elizabeth N. Onwuka is a Professor of Telecommunications Engineering. She holds a Ph.D. in Communications and Information Systems Engineering, from Tsinghua University, Beijing, People's Republic of China; a Master of Engineering degree, in Telecommunications; and a Bachelor of Engineering degree from Electrical and Computer Engineering Department, Federal University of Technology (FUT) Minna, Niger State, Nigeria. Her research interest includes Mobile communications network, Mobile IP networks, Handoff management, Paging, Network integration, Resource management in wireless networks, spectrum management, and Big Data Analytics.

Abraham U. Usman is a highly motivated and dedicated teacher with twenty-two (22) years teaching experience in Electrical and Electronics with specialization in Electronics and Communication Engineering. He was a Senior Lecturer with the Department of Electrical and Electronics Engineering, Federal University of Technology, Minna, Nigeria and transferred to Department of Telecommunication Engineering, of the same University. He is now an Associate Professor of Communication Engineering and Head of the same department. He obtained his B.Eng. in Electrical & Computer Engineering from the same University in 1998. He acquired M.Sc. in Electrical Engineering from University of Lagos, Nigeria and Ph.D. in Communication Engineering from Abubakar Tafawa Balewa University, Bauchi Nigeria in 2002 and 2014 respectively. He was the pioneer Deputy Dean of School of Electrical Engineering and Technology between 2017 - 2021. Abraham is a member of Nigerian Society of Engineers (MNSE), and a registered Engineer with the Council for the Regulation of Engineering in Nigeria (COREN). He has teaching experience in the area of antenna and mobile radio propagation, wireless communication systems and digital electronics. His research interest includes Radio propagation modelling, Mobile radio resource utilization, Antenna and RF design, Indoor and Outdoor wireless communication, teletraffics and application of Artificial Intelligent techniques in Wireless communication. He has published several papers in national/international journals and conferences.

Supreme A. Okoh is a faculty member in Software Engineering Department, Veritas University Abuja Nigeria. He holds a B.Eng. degree in Telecommunication Engineering from the Federal University of Technology (FUT) Minna, Nigeria with first class honours. He also completed his M.Eng. research in Communication Engineering in the same University and an M.Ed. degree in Advanced Teaching at University of the People, Pasadena, California, USA with distinctions. He is a recipient of various awards such as Total Petroleum scholarship award, best graduating student award, University of the People prestigious scholarship award, etc. He is a Certified Internet Webmaster (CIW), Cisco Certified Network Associate (CCNA) and a Huawei Certified ICT Associate (HCIA). He is a member of IEEE and the Nigerian Society of Engineers (NSE). He is a reviewer with IEEE Access and PLOS One Journal. His research interests include software systems engineering, algorithms, artificial intelligence, healthcare engineering, internet of things, information & network security, curriculum development and outcome-based learning.

Okwudili Onyishi is a first-class student of Electrical and Electronic Engineering department, and a research assistant at Green Wireless Networking (GreenWiN) research group, Federal University of Technology Minna, Nigeria. He is a recipient of various scholarship awards such as Agbami Petroleum and Petroleum Development Trust Fund (PTDF) Nigeria scholarships. His research interests include artificial intelligence, data mining, internet of things and cloud computing.

How to cite this paper: Samuel A. Adebo, Elizabeth N. Onwuka, Abraham U. Usman, Supreme Ayewoh Okoh, Okwudili Onyishi, "A Technique for PUE Detection and Isolation in Cognitive Radio Network", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.13, No.3, pp. 14-25, 2023. DOI:10.5815/ijwmt.2023.03.02