CIT. Journal of Computing and Information Technology, Vol. 29, No. 2, June 2021, 77–88
doi: 10.20532/cit.2021.1005297

Signal Processing-based Model for Primary User Emulation Attacks Detection in Cognitive Radio Networks

Diafale Lafia, Mistura Laide Sanni, Rasheed Ayodeji Adetona, Bodunde Odunola Akinyemi and Ganiyu Adesola Aderounmu

Obafemi Awolowo University, Ile-Ife, Nigeria

Cognitive Radio Networks (CRNs) have been conceived to improve the efficiency of accessing the spectrum. However, these networks are prone to various kinds of attacks and failures that can compromise the security and performance of their users. One of the notable malicious attacks in cognitive radio networks is the Primary User Emulation (PUE) attack, which results in underutilization and unavailability of the spectrum and low operational efficiency of the network. This study developed an improved technique for detecting PUE attacks in cognitive radio networks and further addressed the characteristics of sparsely populated cognitive radio networks and the mobility of the primary users. A hybrid signal processing-based model was developed using the free space path loss and additive Gaussian noise models. The free space path loss model was used to detect the position of the transmitter, while the additive Gaussian noise model was used to analyze the signal transmitted, *i.e.*, energy detection in the spectrum at the detected location. The proposed model was benchmarked with an existing model using the number of secondary users and the velocity of the transmitter as performance parameters. The simulation results show that the proposed model has improved accuracy in detecting primary user emulation attacks. It was concluded that the proposed hybrid model with respect to the number of secondary users and the velocity of the transmitter can be used for primary user emulation attack detection in cognitive radio networks.

ACM CCS (2012) Classification: Security and privacy → Network security → Mobile and wireless security

Keywords: cognitive radio, user emulation attacks, position detection, energy detection, mobile primary users

1. Introduction

In recent years, wireless-based transmission has been one of the sectors that has seen rapid growth in the domain of communication. This is due to the various applications and development of wireless-based technologies. The consequence is that many wireless-based communication systems (up to 85%) crowd the available limited spectrum [1], [2]. There are numerous bodies commissioned for the regulation of radio spectrum usage [3]. In this spectrum allocation, the regulatory bodies attribute the spectrum to license holders for the long term, covering a huge geographic range. This static regulation policy renders the spectrum a constrained resource [4].

Various research has proved that a huge part of the assigned spectrum is still used sparsely, sporadically, or is sometimes completely unused. The usage trend considers a specific range of frequencies (1 GHz to 10 GHz) as mostly unoccupied [5]. Hence, both spectrum scarcity and inefficient utilization can be considered issues emanating from legacy regulatory and licensing processes [1].

Therefore, in order to address the problem of spectrum underutilization and unavailability, a new spectrum management technique is required. Such a technique allows unlicensed users (secondary users) to occupy the spectrum opportunistically while interference with licensed users (primary users) is addressed. Pri-

mary Users (PUs) have priority in accessing the spectrum over Secondary Users (SUs) using Dynamic Spectrum Access (DSA) [6]. This implies that whenever the spectrum is occupied by a licensed user, the unlicensed users must vacate the spectrum till the licensed user releases it.

Cognitive Radio (CR) technology is being developed to be an implementation of the dynamic spectrum access paradigm [7], [8]. CR is derived from the software-defined radio applied to wireless-based transmission [7]. CR can sense its surrounding environment and, based on the result, decide and adjust its parameters without external intervention. It can also sense the presence of the PU automatically and autonomously. When a CR user identifies a PU transmitting in the spectrum, it has to leave the spectrum and search for another that is idle or a hole in the spectrum that is unoccupied by the primary user. All the secondary users can access the spectrum without any priority [9]. The physical location of radio frequency transmission sources has been a hot topic for many years in wireless applications [10], [11]. These specific features of CR predispose the network to new kinds of threats, one of which is called a primary user emulation attack [12]. The Primary User Emulation (PUE) attack is illustrated in Figure 1. This paper focused on signal analysis with the aim of addressing PUE attacks on cognitive radio networks. The remaining sections of the paper are organized as follows: The second section discussed previous related research work; the third section discussed the design of the proposed model; the fourth section examined the simulation results and the fifth section contains the conclusion of the paper.

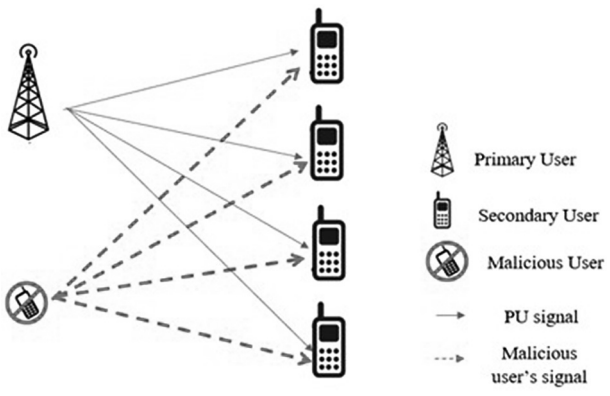

Figure 1. Illustration of the problem of PUE attack scenario.

2. Related Work

In CRNs, security threats have grown significantly over the previous two decades. These attacks have a negative influence on the networks' normal operation, and thus several approaches have been proposed.

One method for detecting PUE attacks in CRNs is to use localization-based approaches [13–15]. The Distance Ratio Test (DRT) technique [13], a localization-based approach, is a Received Signal Strength (RSS)-based method to determine transmitter-receiver distance. The ratio between the RSS at two different points is a function of the distance ratio between these points and the transmitter. In this case, the transmitter's location detection accuracy increases with the number of CR users. If the RSS ratio of the receiver is close to that of the transmitter, then it is assumed to be the legitimate transmitter; otherwise, a PUE attack is detected. This technique works for fixed or static users and a dense population of CR users.

Also, the Distance Difference Test (DDT) technique measures the received signal at two distinct points and the resulting time difference. Using the time difference, the distance difference is determined. The greater the distance, the more the detection is accurate. Accuracy is also a function of the synchronization between the two location points (the distance between the points must be small [13]. The position of the transmitter must be well known, and the mobile transmitter is not considered in this work.

Also, Received Signal Strength (RSS), Direction of Arrival (DoA) [16], and Cooperative Spectrum Sensing (CSS) [17] techniques are also used to achieve localization between the primary and secondary users. Localization-Based Defence (LocDef) is a non-interactive technique that analyzes the characteristics of the signal present in the spectrum to determine if it is a PU's signal by estimating its location based on the measurement of RSS collected at the receiver side. The location of the transmitter is detected when the RSS is at its maximum. The assumption governing the study is that the smaller the RSS, the bigger the distance between transmitter and receiver [16]. Time Difference of Arrival (TDoA) is also a non-interactive technique for fixed transmitters

using the difference in arrival time of a signal. The arrival time is measured at two or more different receivers' sides using correlation techniques. TDoA is used to localize the transmitter and consequently detect an eventual attacker. The Weighted Least Square (WLS) is then used to reduce the second-degree error. The position of the receiver must be known and tightly synchronized [15]. The main objective of these localization-based schemes is to minimize the loss ratio during the communication process.

Another approach used to detect PUE attacks is the Advanced Encryption Standard (AES) approach [18]. When a PU wants to start the transmission, it sends an encrypted signal to the spectrum, and the secondary users verify its authenticity. Using the pre-shared secret key, the AES approach generates a reference signal used for authenticating the PU. If the SUs confirm the authenticity, they vacate the spectrum to avoid interference. Furthermore, autocorrelation analysis of the received signal added to AES can detect PUE attacks with no information about the PU.

One other approach used to detect PUE attacks in CRNs is belief propagation-based [19],[20]. In this approach, SUs determine the location and compatibility functions. The results are shared among the CR users to execute the belief function; this is done repetitively. When the results converge for all CR users, the attacker is detected and its signal's features and parameters are broadcast over the network. When a similar signal is detected in the spectrum, the transmission is discarded and the spectrum is set free for all CR users. Since transmission time and the transmitted signal strength are unknown, the location verification approach is deployed using the difference in the RSS at the CR users' level. At least four CR users are needed to localize the attacker.

Another approach used to detect PUE attacks in CRNs is watermarking-based [21] and hash message techniques [22], [23]. In the watermarking-based technique, the PU's signal is watermarked before transmission. The watermarks served as a signature for authenticating the PU's signal in order to differentiate it from an eventual attacker's signal. The proposed method does not affect the bit error rate of the PU's signal, and there is no need for signal conversion nor to modify the receivers' protocol. In the hash message technique, an authentication code was used to detect the attacker. Before the PU starts transmitting, a tag is generated using the hash function. This tag, which is initially part of the transmission key, is embedded in a message sent together with the PU's signal. At the CR users' level, the same hash function is used in addition to the transmission key to regenerate the tag, which is compared to the one embedded in the message. If the two tags are the same, the message is from a genuine primary user; otherwise, the attacker is detected.

The cooperative sensing-based detection technique [24–27] is another approach used to detect PUE attacks in CRNs. There are two different cooperative spectrum sensing techniques, *i.e.*, partially and fully cooperative spectrum sensing. In partially cooperative spectrum sensing, each SU executes the process independently, and the one who detects the primary user's signal first broadcasts the result to the remaining SUs. While in fully cooperative spectrum sensing, all SUs execute the detection process and forward the result to the base station. The global decision is then made by the base station for PUE attack detection. Fully cooperative spectrum sensing is efficient and saves time compared to partially cooperative spectrum sensing. Collaborative Spectrum Sensing (CSS), *e.g.*, a one-class classification technique [28], is also exploited to characterize a PU signal. The PU signal features will learn to aid in distinguishing a PU signal from a PU signal emulation.

One other approach used to detect PUE attacks in CRNs is a channel-based technique. For example, using wireless channels as a fingerprint [29], [30] was employed to detect PUE attacks in CRNs. It was discovered that the probability of detection increases with an increase in the Signal-To-Noise Ratio (SNR).

Position detection is another key approach used to detect PUE attacks in CRNs. In [31], a position detection technique using transmission power was employed to detect PUE attacks in a CRN. Transmission power is a characteristic of the signal that is not easy to emulate. This is because the primary users usually transmit with a power scale of hundreds or thousands of watts, while the cognitive radio users cannot transmit with a power scale of more than ten to hundreds

of milliwatts. The transmission power was used to determine the transmitter-receiver distance, which allows for the detection if the source of the signal is from a real PU or from an attacker.

The energy detection technique [32], [33] is another key approach used to detect PUE attacks in CRNs. These energy-based detection techniques are meant for highly populated CR users in the network. In [33], a database-assisted detection approach using energy detection and localization is proposed to efficiently discover PUE attacks. The energy detector is being used to reduce the time for detecting PUE attacks. This method distinguishes the legitimate user's signal from the attacker's signal using energy thresholds. The energy of the signal (E) is considered as an input, which is compared to a set of three energy thresholds: θ_0, θ_1 and θ_2. $\theta_0 < \theta_1 < \theta_2$, and θ_0 is the conventional energy detection threshold. E is obtained after sampling, squaring, and aggregating the signal being observed in the spectrum. If $E < \theta_0$, then there are only secondary users occupying the spectrum; otherwise, θ_1 and θ_2 are used to identify the signal being observed. If $\theta_0 < E < \theta_1$ or $E > \theta_2$, it is an attacker; otherwise it is the genuine primary user. Furthermore, a localization technique is deployed. The localization scheme is a fingerprint-based approach using a Bayesian hypothesis for estimation. This approach is computationally complex (time complexity) due to the fingerprint-based technique.

In this study, the need to address the detection accuracy of PUE attacks in sparse CRNs and the mobility of primary users is considered. This study proposes the hybrid of position [31] and energy [33] detection to address the detection of PUE attacks in CRNs to increase the detection accuracy for a mobile and sparse population of CR users.

3. Methodology

The proposed model tagged "Hybrid Signal Processing-based Model for Primary User Emulation Attacks Detection" (HSPEAD) developed for detecting PUE attacks comprises two major phases: the position detection of the transmitter and energy detection. During the position detection process in the first phase, once a signal is detected in the spectrum, the distance (di) between the transmitter and the receivers is computed by using the Free-Space Path Loss (FSPL) model. In the FSPL model, the transmitter-receiver distance is proportional to the square of the frequency. The signal disperses in wireless communication with an increase in distance. As a result, the farther the receiver is from the transmitter, the less power it receives. This is because a transmitted signal attenuates over distance due to the fact that the signal is being spread over a larger area. In the FSPL model, there are no obstacles between transmitter and receiver while the signal passes through the Line Of Sight (LOS) channel in a classic transmission. This classic transmission model induces a logical quick insight into detecting primary user emulation attacks. This is because FSPL allows determining the position of the transmitter, which is an important parameter in detecting whether the signal observed in the spectrum is from the genuine primary user or the attacker following hypothesis tests.

In the second phase, the energy detection process implements the additive Gaussian noise model, and the signal detected in the spectrum is analyzed. The signal processing, in this case, comprises the signal sampling to obtain energy vectors; the energy vectors are then squared and aggregated. The output of the signal processing is the energy value of the signal, which is compared to thresholds with the view of detecting PUE attacks in CRNs.

3.1. Position Detection Model

When there is no reflection or diffraction, the loss of signal strength in a line of sight path with air as a medium of transmission is known as Free-Space Path Loss (FSPL). The gain of the antennas and hardware imperfections are not considered.

In the FSPL model, the distance between transmitter and receiver is proportional to the square of the frequency. The signal disperses in wireless communication with the increase of distance. Even in satellite-based transmission, FSPL is the primary model for analyzing signal loss. In the FSPL model, there is an assumption of no obstacles between transmitter and receiver while the signal passes through the Line of Sight (LOS) channel in a classic transmis-

sion. This classic transmission model induces a logical quick insight into detecting primary user emulation attacks. This is because FSPL allows determining the position of the transmitter, which is important in detecting whether the signal observed in the spectrum is from the genuine primary user or the attacker [31]. In Equation (1), the FSPL model is expressed as follows:

$$\frac{P_r}{P_t} = \frac{G\lambda^2}{(4\pi d)^2} \tag{1}$$

where P_r and P_t represent received and transmitted signal power respectively, λ is the signal's wavelength, d is the distance between the transmitter and the receiver in a LOS, G is constantly obtained by multiplying the gain of the transmitter and receiver antenna.

It is therefore deduced that the ratio of the received to the transmitted power is therefore proportional to the square of the distance (d^2) as in Equation (2):

$$\frac{P_r}{P_t} \propto \frac{1}{d^2} \tag{2}$$

Considering equation (1), the distance transmitter-receiver d is expressed as in Equation 3:

$$d = M\sqrt{\frac{P_t}{P_r}} \tag{3}$$

where, M is a constant defined as $\sqrt{\frac{G\lambda^2}{(4\pi)^2}}$.

The transmitter-receiver distance d_i (i = 1, 2, ..., N) can be calculated using the primary user's transmission power ($P_{t(pu)}$), the transmission power of the attacker ($P_{t(att)}$) and the received power by the CR users ($P_{r(i)}$). The distance is, therefore, computed as given in Equation (4) in the case of PU's signal and as given in Equation (5) if the signal is from the attacker [31].

$$d_{i(pu)} = M\sqrt{\frac{P_{t(pu)}}{P_{r(i)}}} \tag{4}$$

$$d_{i(att)} = M\sqrt{\frac{P_{t(att)}}{P_{r(i)}}} \tag{5}$$

Where $P_{r(i)}$ is received signal power at the i-th receiver, $P_{t(pu)}$ is transmitted signal power from the PU, $P_{t(att)}$ is transmitted signal power from the attacker, $d_{i(pu)}$ is distance PU - i-th receiver, $d_{i(att)}$ is distance attacker - i-th receiver, $d_{i(fc)}$ is distance of i-th receiver to the fusion centre.

If $(d_i + d_{i,fc}) \geq |d_i - d_{i,fc}|$ $\forall i$ = 1, 2, ..., N, this means the source of the signal is situated outside the CRN environment, so it is detected to be a PU's signal. Otherwise, this means the source of the signal is located within the range of the CRN environment, and the signal is from an attacker. The position and distance representation of the legitimate primary user, the attacker, and the CR users in the design of HSPEAD are as presented in Figure 2.

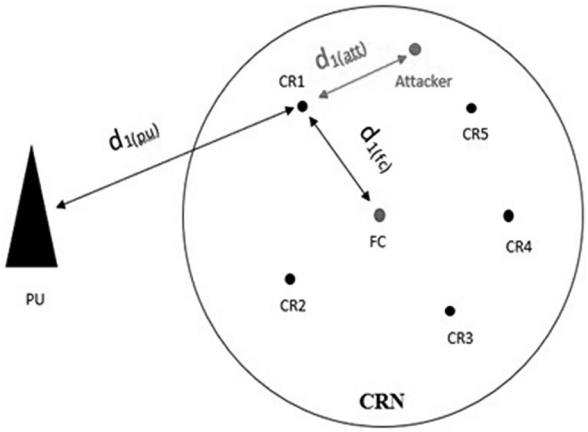

Figure 2. Distance and position representation in the network.

3.2. Energy Detection Model

In spectrum sensing, the energy detection process is a major theoretical advance used for detecting spectrum occupancy. The sensing theory and the decision theory formed the basis of the second phase of HSPEAD for energy detection. This is implemented to determine the accuracy based on a computed threshold. The sensing process converts the input signal to obtain the energy value, and the decision process uses the obtained energy value to derive the corresponding inference. The output can be a yes or a no ("yes, if the signal is present" or "no, if the signal is not present"). At least one parameter must characterize each of the processes: the sensitivity for the sensing and the response criteria for the decision process.

The estimation of thresholds can lead to an incorrect evaluation of the sensitivity of the sensing process compared with that of the response criteria of the decision process. Therefore, there is a need to set two aspects of detection capability to measure the sensitivity and decision criteria. The inference corresponding to "yes" when a signal is present is no longer sufficient to distinguish the signal of the genuine transmitter from the signal of an attacker.

Considering $x(t)$, $h(t)$ and $n_c(t)$ representing the transmitted signal, channel impulse response and the channel noise respectively. The basic additive Gaussian noise model is expressed as given in Equation (6) [33].

$$y(t) = \begin{cases} n_c(t) & only\ SU \\ h(t) * x(t) + n_c(t) & PU \\ h(t) * x_1(t) + n_c(t) & PUE\ Attack \end{cases} \quad (6)$$

Let $P_{t(pu)}(t)$ and $P_{t(att)}(t)$ be the signal transmitted by the PU and by attacker respectively. Thus, $x(t) = P_{t(pu)}(t)$ for the primary user's signal, $x_1(t) = P_{t(att)}(t)$ for the attacker's signal and $x(t) = 0$ when only secondary users are occupying the spectrum. The additive Gaussian noise model is then transformed as in Equation (7).

$$y(t) = \begin{cases} n_c(t) & SU\ or\ no\ signal \\ h(t) * P_{t(pu)}(t) + n_c(t) & PU \\ h(t) * P_{t(att)}(t) + n_c(t) & PUE\ Attack \end{cases} \quad (7)$$

In this study, each secondary user is considered a PUE attack detector. The received signal by the secondary users is then processed to obtain the energy value of the signal. Furthermore, the obtained energy value is compared to the defined threshold to identify the signal observed in the spectrum. The signal is then processed in these three steps: signal sampling, signal squaring, and signal aggregation.

The energy of the signal (E) is considered as input which is compared to a set of three energy thresholds: θ_0, θ_1, and θ_2. $\theta_0 < \theta_1 < \theta_2$, where θ_0 is the conventional energy detection threshold. E is obtained after sampling, squaring, and aggregating the signal been observed in the spectrum. If $E < \theta_0$, then, there are only secondary users occupying the spectrum otherwise θ_1 and θ_2 are implemented to identify the signal been observed. If $\theta_0 < E < \theta_1$ or $E > \theta_2$, then the signal is from an attacker, otherwise it is the genuine primary user. E is derived as in equation (8) as follow:

$$E = \sum_{s=1}^{ns} e_s \quad (8)$$

where e_s are vectors obtained after sampling and squaring the input signal. Thus, the proposed HSPEAD model is illustrated in Figure 3.

4. Simulation and Evaluation

The simulation of the HSPEAD model was carried out using MATLAB. The CRN was simulated in OMNET++ 4.6. In this study, an ad hoc architecture was used in a decentralized transmission mode using point-to-point topology. The secondary users can establish communication links among themselves or with the primary user without the need for an access point or a relay node. Radio and spread spectrum technologies in wireless local area networks were used to enable communication between multiple devices in a limited area.

4.1. Model Simulation

The performance of the model is evaluated using the detection probability based on the number of CR users and the velocity of the transmitter. Based on the number of CR users, the detection probability is derived as in Equation (9).

$$\begin{aligned} P_d &= 1 - P_{fn} \\ &= 1 - \left(1 - \left(\frac{r - \frac{\max\left(d_{i,fc} + d_{j,fc}\right)}{\sqrt{R}}}{r} \right)^2 \right)^N \end{aligned} \quad (9)$$

Where P_d is the detection probability, r is the radius of the CRN environment, N is the number of CR users, $d_{i(fc)}$ is the distance between CR users and the fusion centre, $d_{j(fc)}$ is the distance of the farthest CR to the fusion centre, R is the ratio of the transmitted power.

The detection probability with respect to the number of CR users is shown in Figure 4. The minimum detection probability of the proposed

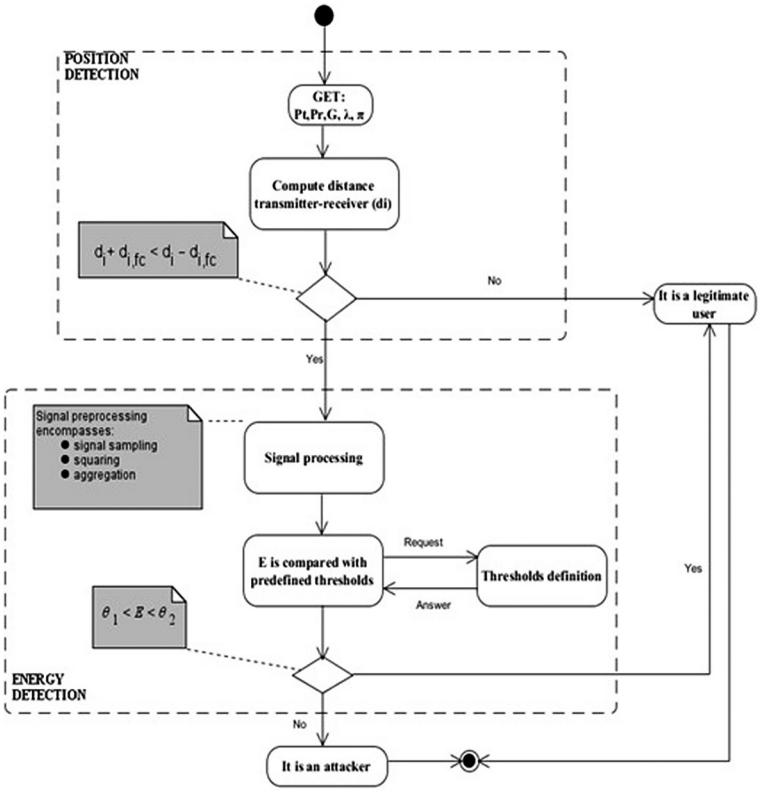

Figure 3. The Proposed Model (HSPEAD).

model is 57.5%, corresponding to a single secondary user, while in the existing RONG model [33] for the same number of secondary users the detection probability is null (0%), as is illustrated in Figure 4. This probability increases to a maximum of 96% and 94%, respectively, for the proposed and the existing RONG model [33].

Based on the transmitter's velocity, the detection probability is derived as in equation (10) where P_d is the detection probability, θ_1 and θ_2 are the defined thresholds, n_s is the total number of samples, $Q()$ is the standard Gaussian complementary cumulative distribution function, V is the maximum allowable speed of the signal's transmitter, I is the desired confidence interval, D is the minimum distance where the transmitter is considered to be stationary, ε is the acceptable error in the mean calculation.

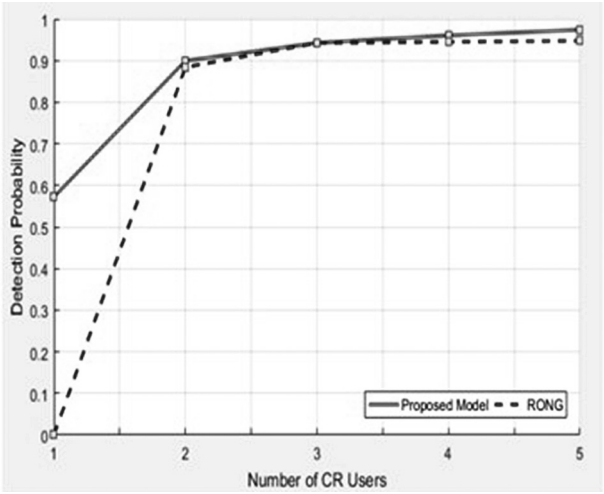

Figure 4. Detection probability based on number of CR users.

$$P_d = 1 - Q\left(\frac{\theta_1 - n_s}{\sqrt{2n_s}}\right)\left(2 - Q\left(\frac{\theta_2 - n_s}{\sqrt{n_s}}\right)\right) = 1 - Q\left(\frac{\theta_1 - f\dfrac{D\varepsilon^2}{VQ(I)^2}}{\sqrt{2f\dfrac{D\varepsilon^2}{VQ(I)^2}}}\right)\left(2 - Q\left(\frac{\theta_2 - f\dfrac{D\varepsilon^2}{VQ(I)^2}}{\sqrt{f\dfrac{D\varepsilon^2}{VQ(I)^2}}}\right)\right) \quad (10)$$

Figure 5 presents the detection probability with respect to the velocity of the transmitter. The existing RONG's model [33] with a stationary primary user detects the presence of an attacker at a minimum rate of 50%, while for the proposed model, the minimum detection rate is 72.3%. This detection accuracy increases with the velocity of the transmitter to 98%. Hence, HSPEAD can detect attackers even in mobile user scenarios. While in Figure 6, similar scenarios were observed from 0 to 92% in the Dong's model [31] and from 9% to 98% in the proposed model.

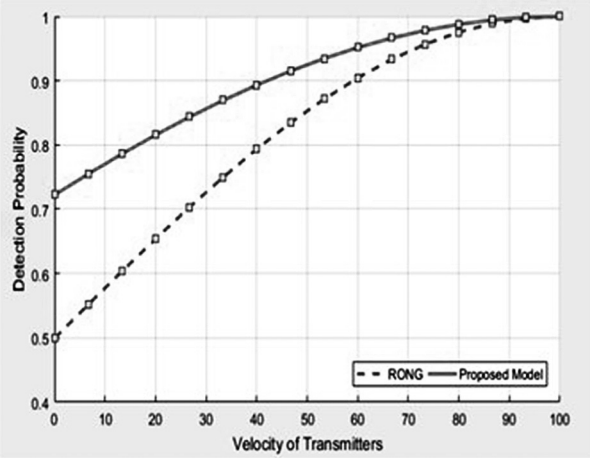

Figure 5. Detection probability based on transmitter's velocity.

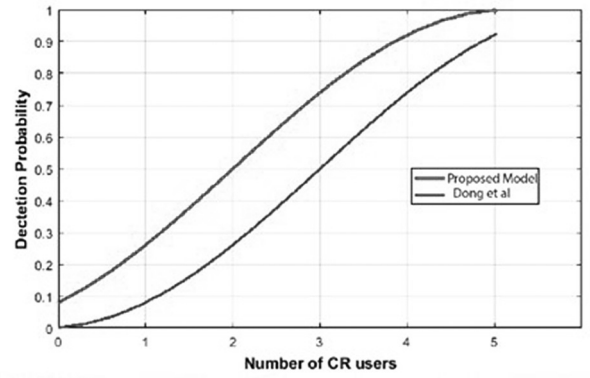

Figure 6. Detection Probability based on number of CR users.

4.2. Network Simulation

In the CRN simulation, the users (primary and secondary), the channels, and the functionalities modules (mobility and radio modules) are based on the existing modules from the INET-MANET framework with respect to cognitive radio technology requirement. The occupancy of primary user's channels, indexed as *i*, is modeled as two states: BUSY and IDLE.

The data transmission for both primary and secondary users is simulated using the ping protocol (*pingapp.cc*). The Ping protocol ensures the transfer of the primary user's state in order to trigger the sensing process of the secondary user. The tracking of the ping protocol event shows how the packet travels up to the Internet Control Message Protocol (ICMP) of the network module of the receiver. Thus, the SU uses the identification of primary packets to avoid collisions. The ping protocol is modified in this work to incorporate the primary user's state; thus, additional parameters are embedded in the *pingapp.cc*. These parameters (included in *phost.ned*, *shost.ned*, and *pingpayload.msg*) were also used to control the data transmission of both PU and SU.

In the process of simulating the network, the four layers of the TCP/IP model have been considered. At the physical layer level, the connections between nodes have been established by the topology of the network. At the network layer level, the network architecture was defined, including the path determination and the forwarding of the routing process. At the transport layer level, the data transmission was defined; the starting and ending transmission of each user, mainly the primary user, is noted by an acknowledgement to facilitate spectrum sensing. Finally, at the application layer level, the layout and design of the network were carried out. Figure 7 shows the design of the simulation process of opportunistic spectrum access by secondary users. Figure 8 shows the throughput based on the simulation time and Figure 9 shows the End-to-End delay of HSPEAD. Both throughput and delay are proportional to time.

5. Conclusion

This paper studied security issues in CRNs, particularly in spectrum sensing. The focus was on PUE attacks. An improved hybrid model was developed based on position detection aided with energy detection using multiple thresholds to detect PUE attacks in CRNs. The results of simulations carried out demonstrated that the proposed

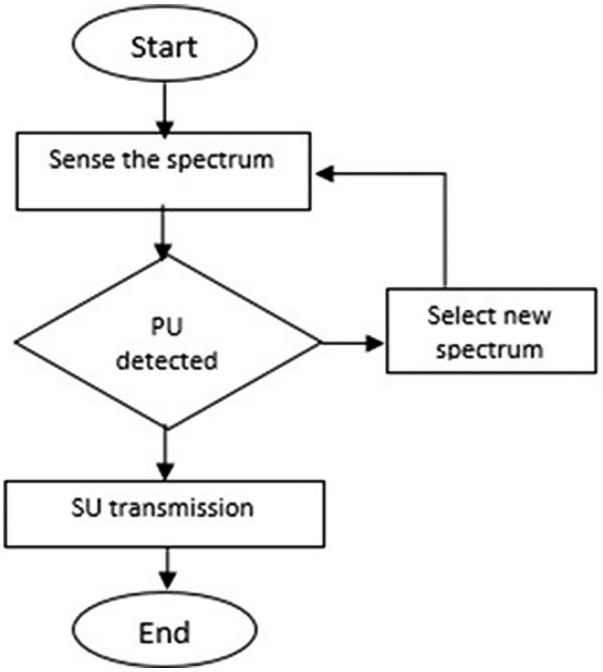

Figure 7. Network simulation process flow.

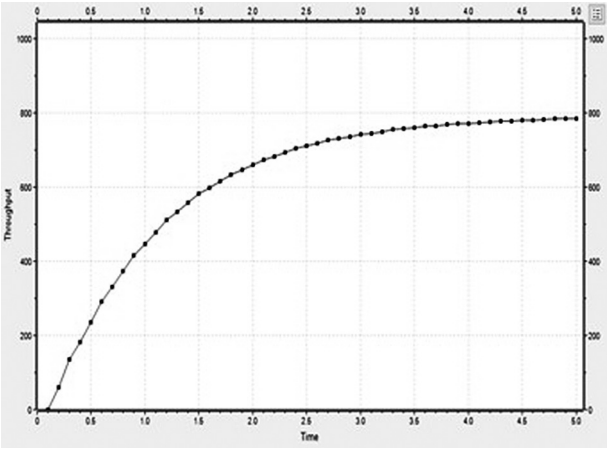

Figure 8. Throughput with respect to time.

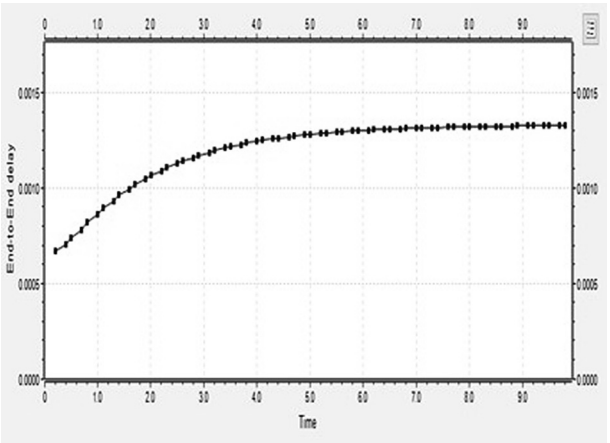

Figure 9. End-to-End delay with respect to time.

model is effective for detecting PUE attacks in CRNs, even for mobile and sparse populations of CR. Since spectrum sensing occupancy information is being received by secondary users in a CRN, it is imperative to verify if the received information is actually from a genuine primary user. Improved performance of secondary users' spectrum sensing is presented by proposing a novel technique to effectively detect attackers in a CRN. The proposed model, HSPEAD, aids in controlling the activities of PUE attacks, eliminates spectrum-sensing errors encountered by secondary users in a CRN, and enables the implementation of secured and trusted CRNs.

Acknowledgement

This work was supported by the World Bank Sponsored project of African Center of Excellence (ACE) of Obafemi Awolowo University's OAU ICT-Driven Knowledge Park (OAK-Park).

References

[1] S. M. Elghamrawy, "Security in Cognitive Radio Network: Defense against Primary User Emulation Attacks Using Genetic Artificial Bee Colony (GABC) Algorithm", *Future Generation Computer Systems*, vol. 109, pp. 479–487, 2020. http://dx.doi.org/10.1016/j.future.2018.08.022

[2] M. Mahmoudi *et al.*, "Defense against Primary User Emulation Attackers Based on Adaptive Bayesian Learning Automata in Cognitive Radio Networks", *Ad Hoc Networks*, vol. 102, p. 102147, 2020. http://dx.doi.org/10.1016/j.adhoc.2020.102147

[3] A. A. Sharifi *et al.*, "Secure Cooperative Spectrum Sensing under Primary User Emulation Attack in Cognitive Radio Networks: Attack-Aware Threshold Selection Approach", *AEU-International Journal of Electronics and Communications*, vol. 70, no. 1, pp. 95–104, 2016. https://doi.org/10.1016/j.aeue.2015.10.010

[4] F. Jin *et al.*, "Improved Detection of Primary User Emulation Attacks in Cognitive Radio Networks", in *Proc. of the IEEE International Telecommunication Networks and Applications Conference (ITNAC)*, 2015, pp. 274–279. http://dx.doi.org/10.1109/ATNAC.2015.7366825

[5] L. Chouhan and A. Trivedi, "Cognitive Radio Networks: Implementation and Application Issues in India", in *Proc. of the Next Generation Network-Implementation and Implication Telecom Regulatory Authority of India (TRAI)*, 2011.

[6] S. Parvin *et al.*, "Conjoint Trust Assessment for Secure Communication in Cognitive Radio Networks", *Mathematical and Computer Modelling*, vol. 58, no. 5-6, pp. 1340–1350, 2013. http://dx.doi.org/10.1016/j.mcm.2013.01.001

[7] J. Mitola, "Cognitive Radio for Flexible Mobile Multimedia Communications", in *Proc. of the 1999 IEEE International Workshop on Mobile Multimedia Communications, (MoMuC'99)*, 1999, pp. 3–10. http://dx.doi.org/10.1109/MOMUC.1999.819467

[8] D. Das and S. Das, "An Intelligent Resource Management Scheme for SDF-Based Cooperative Spectrum Sensing in the Presence of Primary User Emulation Attack", *Computers & Electrical Engineering*, vol. 69, pp. 555–571, 2018. http://dx.doi.org/10.1016/j.compeleceng.2017.06.024

[9] Z. Jin *et al.*, "Detecting Primary User Emulation Attacks in Dynamic Spectrum Access Networks", in *Proc. of the IEEE International Conference on Communications*, pp. 1–5, 2009. http://dx.doi.org/10.1109/ICC.2009.5198911

[10] O. O. Abiona *et al.*, "Architectural Model for Wireless Peer-to-Peer (WP2P) File Sharing for Ubiquitous Mobile Devices", in *Proc. of the IEEE International Conference on Electro/Information Technology*, 2009. http://dx.doi.org/10.1109/EIT.2009.5189580

[11] M. L. Sanni *et al.*, "Gateway Placement Optimisation Problem for Mobile Multicast Design in Wireless Mesh Networks", in *Proc. of the International Conference on Computer and Communication Engineering, ICCCE*, Kuala Lumpur, Malaysia, 2012. http://dx.doi.org/10.1109/ICCCE.2012.6271227

[12] E. Orumwense *et al.*, "Impact of Primary User Emulation Attacks on Cognitive Radio Networks", *International Journal on Communications Antenna and Propagation*, vol. 4, no. 1, pp. 19–26, 2014.

[13] R. Chen and J. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks", in *Proc. of the IEEE Workshop Networking Technologies for Software Defined Radio Networks (SDR)*, pp. 110–119, 2006. http://dx.doi.org/10.1109/SDR.2006.4286333

[14] O. León *et al.*, "Cooperative Detection of Primary User Emulation Attacks in CRNs", *Computer Networks*, vol. 56, no. 14, pp. 3374–3384, 2012. http://dx.doi.org/10.1016/j.comnet.2012.05.008

[15] R. Chen *et al.*, "Defense Against Primary User Emulation Attacks in Cognitive Radio Networks", *IEEE Journal on Selected Areas of Communication*, vol. 26, no. 1, pp. 25–37, 2008. http://dx.doi.org/10.1109/JSAC.2008.080104

[16] M. V. Rajagopala and C. L. Sanjeev, "Detection and Prevention of Primary User Emulation Attack in Cognitive Radio Networks Using Secure Hash Algorithm", *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 2, pp 136–146, 2020.

[17] S. A. Adebo *et al.*, "Cooperative-Hybrid Detection of Primary User Emulators in Cognitive Radio Networks", *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3116–3124, 2020. http://dx.doi.org/10.11591/ijece.v10i3.pp3116-3124

[18] A. Alahmadi *et al.*, "Mitigating Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard", in *Proc. of the IEEE Global Communications Conference (GLOBECOM)*, pp. 3229–3234, 2013. http://dx.doi.org/0.1109/GLOCOM.2013.6831569

[19] Z. Yuan *et al.*, "Defeating Primary User Emulation Attacks Using Belief Propagation in Cognitive Radio Networks", *IEEE Journal on Selected Areas Communication*, vol. 30, no. 10, pp. 1850–1860, 2012. http://dx.doi.org/10.1109/JSAC.2012.121102

[20] S. Reisenfeld and S. Maric, "Mitigation of Primary User Emulation Attacks in Cognitive Radio Networks Using Belief Propagation", in *Proc. of*

the International Conference on Cognitive Radio Oriented Wireless Networks, pp. 463-476, 2015. http://dx.doi.org/10.1007/978-3-319-24540-9_38

[21] N. Goergen *et al.*, "Physical Layer Authentication Watermarks Through Synthetic Channel Emulation", in *Proc. of the IEEE International Symposium on New Frontiers (DySPAN)*, pp. 1–7, 2010. http://dx.doi.org/10.1109/DYSPAN.2010.5457897

[22] W. R. Ghanem *et al.*, "Defence Against Selfish PUEA inCognitive Radio Networks Based on Hash Message Authentication Code", *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 12–21, 2016.

[23] M. V. Rajagopala and C. L. Sanjeev, "Detection and Prevention of Primary User Emulation Attack in Cognitive Radio Networks Using Secure Hash Algorithm", *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 2, pp 136–146, 2020.

[24] A. Ghasemi and E. Sousa, "Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments", in *Proc. of the IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pp. 131–136, 2005. http://dx.doi.org/10.1109/DYSPAN.2005.1542627

[25] G. Ganesan and Y .Li, "Cooperative Spectrum Sensing in Cognitive Radio, Part II: Multiuser Networks", *IEEE Transactions on Wireless Communications*, vol.6, no. 6, pp. 2214–2222, 2007. http://dx.doi.org/10.1109/TWC.2007.05776

[26] Z. Quan *et al.*, "Optimal Linear Cooperation for Spectrum Sensing in Cognitive Radio Networks", *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 28–40, 2008. http://dx.doi.org/10.1109/JSTSP.2007.914882

[27] C. Chen, *et al.*, "Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack", *IEEE Transaction on Wireless Communication*, vol. 10, no. 7, pp. 2135–2141, 2011. http://dx.doi.org/10.1109/TWC.2011.041311.100626

[28] B. Chhetry and N. Marchang, "Detection of Primary User Emulation Attack (PUEA) In Cognitive Radio Networks Using One-Class Classification", arXiv:2106.10964v1 [cs.NI], pp 1–7, 2021.

[29] C. Zhao *et al.*, "Anti-PUE Attack Base on the Transmitter Fingerprint Identification in Cognitive Radio", in *Proc. of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, 2009, pp.1–5. http://dx.doi.org/10.1109/WICOM.2009.5305529

[30] W. L Chin *et al.*, "Channel-Based Detection of Primary User Emulation Attacks in Cognitive Radios", in *Proc. of the 75th Vehicular Technology Conference (VTC Spring)*, pp. 1–5, 2012. http://dx.doi.org/0.1109/VETECS.2012.6239877

[31] Q. Dong *et al.*, "An Adaptive Primary User Emulation Attack Detection Mechanism for Cognitive Radio Networks", in *Proc. of the International Conference on Security and Privacy in Communication Systems*, pp. 297–317, 2018. http://dx.doi.org/10.1007/978-3-030-01701-9_17

[32] K. Gokulakrishnan et al, "Detection & Defensive Approach for Primary User Emulation Attacking Cognitive Radio Network", *IOP Conference Series: Materials Science and Engineering*, vol. 1055 (012070), pp 1–8, 2021. http://dx.doi.org/10.1088/1757-899X/1055/1/012070

[33] R. Yu *et al.*, "Securing Cognitive Radio Networks Against Primary User Emulation Attacks", *IEEE Network*, vol. 30, no. 6, pp. 62–69, 2016. http://dx.doi.org/10.1109/MNET.2016.1200149N

Received: September 2021
Revised: December 2021
Accepted: February 2022

Contact addresses:
Diafale Lafia
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: dlafia@pg-student.oauife.edu.ng

Mistura Laide Sanni
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: msanni@oauife.edu.ng

Rasheed Ayodeji Adetona
Department of Mathematics
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: adetonara@oauife.edu.ng

Bodunde Odunola Akinyemi
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: bakinyemi@oauife.edu.ng

Ganiyu Adesola Aderounmu
Department of Computer Science and Engineering
Obafemi Awolowo University
Ile-Ife
Nigeria
e-mail: gaderoun@oauife.edu.ng

Diafale Lafia received a BSc degree in computer science from IUT, Parakou, Benin Republic, in 2013, and a MSc degree in computer engineering from Obafemi Awolowo University, Ile Ife, Nigeria, in 2019. He is currently pursuing a PhD degree in computer engineering at Obafemi Awolowo University, Ile Ife, Nigeria. He was a computer scientist at the National Agency of Data Management (Benin Republic) from 2014 to 2016 and a computer engineer at System and Orbit from 2019 to 2021. He is also an assistant lecturer at IUT and LCS Benin. His current research interests include cyber-physical systems (CPS) and CPS cybersecurity, automation and control systems, and networking. He is a member of the ANS Laboratory Research Network Section.

Mistura Laide Sanni is a senior lecturer in the Department of Computer Science and Engineering, at Obafemi Awolowo University, Ile-Ife, Nigeria. She obtained a BSc degree in computer engineering at Obafemi Awolowo University, Ile-Ife (1992). She had MSc degrees in physics (1998) and computer science (2006). She holds a PhD degree in engineering at the International Islamic University, Malaysia (IIUM), Kuala Lumpur (2015). She is a registered engineer with COREN and a registered computer professional with CPN. Her research focuses on data communication, wireless networking, embedded systems, and cyber security.

Rasheed Ayodeji Adetona is an assistant lecturer in the Department of Mathematics at Obafemi Awolowo University (OAU), Ile-Ife, Nigeria. He obtained both his BSc and MSc degrees in Mathematics from OAU, Ile-Ife. He specializes in fluid dynamics and numerical computing.

Bodunde Odunola Akinyemi holds a B.Tech (2005) in computer science from Ladoke Akintola University, Ogbomosho, Nigeria, a MSc (2011) degree and a PhD (2014) degree in computer science from Obafemi Awolowo University, Ile-Ife, Nigeria. She is a member of the International Association of Engineers, IEEE, Nigeria Computer Society (NCS), and the Computer Professional Registration Council of Nigeria (CPN). She is a senior lecturer and member of the Data Communication Group in the Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria. Her major research areas are in data communication, network security and performance management, software development, and blockchain technology.

Ganiyu Adesola Aderounmu is a professor of computer science and engineering at Obafemi Awolowo University, Ile-Ife, Nigeria. He is a full member of the Nigeria Society of Engineers (NSE) and a registered computer engineer with the Council for Regulation of Engineering Practice in Nigeria (COREN). He is also a full member of the Nigerian Computer Society (NCS) and the Computer Professional Registration Council of Nigeria (CPN). He has over 30 years of experience in teaching and research. He is the author of many journal articles in Nigeria and abroad. His special interests include computer communications and networking.