Mitigating Primary User Emulation Attacks in Cooperative Spectrum Sensing

Momin Nadeem[*], Sana Ul Haq[†], Noor Gul[‡], Muhammad Wasimuddin[§],
Imtiaz Rasool[**]

Abstract

Similar to other wireless networks, the Cognitive Radio (CR) network is susceptible to several types of attacks. Common attacks on the CR Network include Miss-Detection (Primary User Emulation Attacker (PUEA), lazy-Secondary User (SU), and malicious-SU) and Noise (a network jammer is the attacker's tool). Given that it has an integrated sensor system, the PUEA is thought to be the most destructive of them all. It monitors the activity of Primary User (PU) and attempts to take over the spectrum even when the PU is on the network. It fools the Sensing Nodes, or SUs, by seeming to be the PU. This study proposes a method based on Time-of-Flight/Time-of-Arrival (ToF/ToA) to monitor PU position. Simulation results show improvement in network throughput when compared with conventional systems for location history technique.

***Keywords*:** Wireless Sensor Network; Cognitive Radio; Cooperative Spectrum Sensing; Primary User Emulation Attacker.

Introduction

The standard of living has improved with the technological advancements and the practice of smart devices. Systems and gadgets are transforming to self-sufficient and self-learning modes, where most devices and media on wired network are replaced by wireless ones. To identify physical changes and climate conditions, humans have been substituted with Wireless Sensor Networks (WSN). These sensors are monitoring anomalies in wireless network environments and sending this data to AI-enabled servers for detection of rogue vs benign traffic. The need for bigger frequency bandwidths has also increased with growing wireless devices. The fact that the allocated frequency spectrum is not being used to its full potential is another problem. A Federal Communications Commission (FCC) assessment states that the spectrum

[*] Department of Electronics, University of Peshawar, Peshawar 25120, Pakistan, momin_awan@uop.edu.pk

[††] Department of Electronics, University of Peshawar, Peshawar 25120, Pakistan, sanaulhaq@uop.edu.pk

[‡] Department of Electronics, University of Peshawar, Peshawar 25120, Pakistan, noor@uop.edu.pk

[§] Department of Electronics, University of Peshawar, Peshawar 25120, Pakistan, wasimuddin@uop.edu.pk

[**] Department of Electronics, University of Peshawar, Peshawar 25120, Pakistan, imtiazrasoolkhan@uop.edu.pk

available to licensed users is underutilized to the tune of almost 90% (Federal Communications Commission, 2021).

The CR network is conceived by Joseph Mitola in 1995. It is a cutting-edge method of wireless communication that could lessen the problem of underutilized spectrum without altering the deployed hardware. The CR network also made it possible to reuse current gear. Consequently, a free frequency band might be available to SUs for use in communication. Figure 1 shows the CR network.

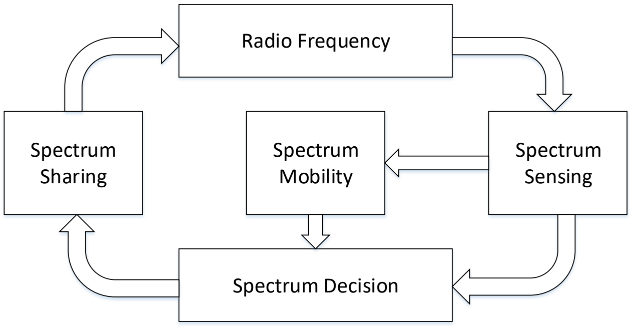

Figure 1: Cognitive Radio Network.

The word "cognitive" means "become aware of something" (Gul et al., 2017). The CR network's goal is to provide PUs with an interference-free wireless communication channel over Dynamic Spectrum Access (DSA). Users in DSA communicate their spectrum sensing findings to nearby PUs, SUs, or both. The CR network could allow PUs and unlicensed SUs to share the available spectrum opportunistically. CR networks are adaptable and self-aware, establishing them apart from traditional radio networks. In addition CR network identify spectrum gaps besides gathering information from the surroundings using frequency, power, bandwidth, and modulation scheme, it finds spectrum gaps. The SUs have access to the available frequency channel from the PUs. The impedance, false alarm rate, and detection probability of the PU-spectrum monitoring process should all be high (Wu et al., 2024; Zhu et al., 2024; Gul et al., 2018; Renk et al., 2007).

Some of the commonly used sensing techniques include Matched Filter Detection (MFD), feature detection, Energy Detection (ED), Generalized Likelihood Ratio Test (GLRT) detection, and Cooperative Spectrum Sensing (CSS) (Ayoob, 2023; Maya et al., 2023; Gul et al., 2017). The CSS and ED are often applied, with CSS generally offers better sensing accuracy to mitigate sensing issues in faded and shadow environments and better performance than ED. Each SU conducts spectrum sensing in CSS and sends the sense data to a Fusion Center (FC) to make a collective decision (Marinho et al., 2015).

The CR network is often vulnerable to number of attacks that can degrade its performance and potentially lead to a denial of service (Gul et al., 2018; Mishra & Dewangan, 2015). Table 1 provides an overview of potential attacks on a CR network.

Table 1: Types of Attackers.

Types of Malicious Users	Responses
Always Yes Malicious User (AYMU) (Kaligineedi et al., 2010)	Indicating PU is consistently utilizing the spectrum.
Opposite Malicious User (OMU) (Gul et al., 2017)	The OMU reports are never in line with the actual amount of the PU activity.
Random Opposite Malicious User (ROMU)	The user transmits random statuses of PU regardless of its true status, making it challenging to identify in a report.
Always No Malicious User (ANMU) (Koo & Vu-van, 2012)	It reports that PU spectrum is available now regardless of the actual current situation.
Primary User Emulation Attacker (PUEA) (Sharifi et al., 2016)	It simulates the PU to free up the spectrum while the PU is present.

Table 1 lists five main classes of attackers. The simple identification of these malevolent users is due to the consistency of sensing reported by AYMU and ANMU (either 1 or 0). By comparing their reports, OMUs could also be identified. The most difficult attackers for the fusion center to deal with are ROMU and PUEA. Since PUEA is difficult to detect using traditional detection methods, it is thought to be the most harmful of them. The suggested methodology uses a hybrid approach to handle this, tracking the PUEA by combining traditional approaches with a localization mechanism. PUEA disrupts the network by deceiving both SUs and Pus (Chen & Park, 2026), leading to significant network interruptions and a sharp decline in available channel resources. The attacks can be of two types:

Selfish Approach: The entire spectrum is occupied by the attacker.

Malicious Approach: The attacker aims to impact overall efficiency of network negatively.

Several techniques have been proposed to prevent PUEA focusing on using TV transmitter as PU. Among such techniques (Chen et al., 2011) are the first to identify PUEA in the context of mobile FM microphones as PUs. Other techniques proposed the Transmitter Verification Scheme (Chen et al., 2008; Alahmadi et al., 2014), the Fenton Approximation Method (Pu et al., 2011), and Fingerprint Verification. Madbushi & Rukmini (2022) suggested a modified double threshold energy detection cooperative spectrum sensing method. The results of the simulation show that the suggested model has greatly reduced PUEA. Batool et al. (2023) presented a skillful Time Difference of Arrival (TDOA) based localization method that makes use of the differential evolution algorithm. Compared to the firefly optimization process, the differential evolution algorithm converge more quickly. Ambhika (2024) introduced a method that combined the Bayesian optimization technique and support vector machine (SVM). SVM uses a random selection process to identify primary and secondary users in order to identify fraudulent users. With 98% accuracy, the suggested method predicts the PUEA. Mazumdar et al. (2023) combine SC-FDMA with CR network. To lessen the impact of PUEA attacks, a Latin square (LS) matrix tag generating scheme is suggested. PUEA is less likely to affect the LS tag generation that is recommended.

Table 2: The HDF Conventional Rules.

Rule	Technique
AND Rule	The final decision is 1 at the Fusion Center if and only if all the sensing nodes report yes report.
OR Rule	The final decision could be 1 at the Fusion Center, even if a single sensing node reports yes.
Majority Voting	The decision is made my counting the votes of sensing nodes.

Methodology

Imagine a network of 200 SUs that continuously monitor the activity and location coordinates of the PU. The PU's status is represented by a one-bit mechanism (0 or 1), where "0" denotes that the spectrum is unoccupied and "1" indicates that spectrum is occupied by the PU. Every SU first decides locally about the PU's activity, and the FC receives this information for a final judgment. To reach this choice, the FC may employ the Soft Decision Fusion (SDF) or Hard Decision Fusion (HDF) methods.

Several researchers have adopted the SDF method (Haldorai & Kandaswamy, 2019). Information is transmitted to FC using two bits in SDF model. As suggested by Thomopoulos et al., the first bit represents the presence of the PU, while the second bit conveys the signal quality information (Mao et al., 2007).

$$P_e = P_f + P_m \tag{1}$$

Equation (1) defines the error probability P_e, where P_f is the probability of false alarm, and probability of missed detection is represented by P_m in the CR network. The detection probability P_d is given as follows:

$$P_d = \{decision\ H_1 \mid H_0\} \text{ or } P_d = \{decision\ H_0 \mid H_0\} \tag{2}$$

Global decision is calculated by FC after receiving the local decision from SUs, as shown in equation (3) below.

$$x_j(l) = \{H_0, n_j(l)\ H_1, h_j(l) + \ n_j(l)\ \} \tag{3}$$

In this context, $x_j(l)$ represents the energy received by the j^{th} SU during a given time slot, while H_0 and H_1 are the absence and presence variables of the PU signal, respectively. The term $n_j(l)$ represents the Additive White Gaussian Noise (AWGN), and h_j is the channel gain of the PU relative to the j^{th} SU, which remains constant throughout the detection interval. Variable $s(l)$ denotes the PU transmission during time slot l (Abdelhakim et al., 2014). The detection probability P_d^j for an effected channel by AWGN is provided in equation (4) below.

$$P_d^j = \left(Q_b\left(\sqrt{2_n}, \sqrt{\gamma_j}\right)\right) \tag{4}$$

Figure 2 presents the flowchart for the proposed scheme. Local decision is calculated by processing predefined values of corresponding location coordinates against sensed data received from multiple SUs sensing the PU signal. These results are then sent to the FC, where HDF schemes are employed to make a final global decision.

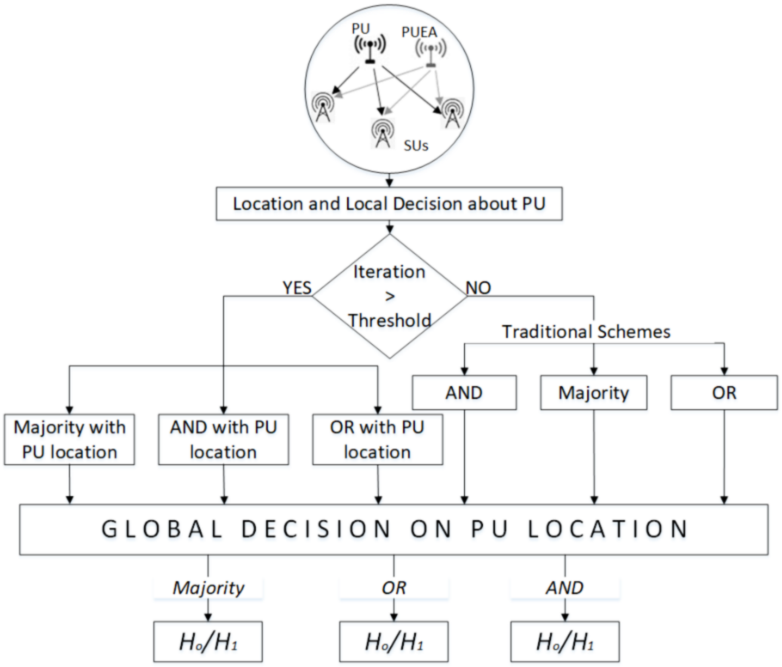

Figure 2: Proposed Technique.

Experimental Results

The results section presents proposed system where Majority voting techniques are combined with the conventional AND, OR, and the Time-of-Flight (ToF) technique to make it an enhanced method.

$$Dist_{xy} = (t_2 - t_1) * v \tag{5}$$

$$Dist_{xy} = \text{ToF} * v \tag{6}$$

$$Dist_{xy} = (v_2 - v_1) * (t_4 - t_2 - t_{wait}) \tag{7}$$

The ToF method could be applied in three different ways by using equations (5), (6), and (7) which define the Time Difference Of Arrival (TDOA). In these equations, t_1 represent node transmit times & t_2 represent the node receive time with the velocity of signal as v.

The PU is located within the network using the two-way ToF method, as shown in Figure 3, in the proposed architecture. The SUs are arranged in a planned layout with predetermined separations between them. The geographical coordinates are initially provided to FC for the PU with respect to the SU in order to find if the channel is available or occupied and whether the PU or the PUEA attacker is utilizing the spectrum.

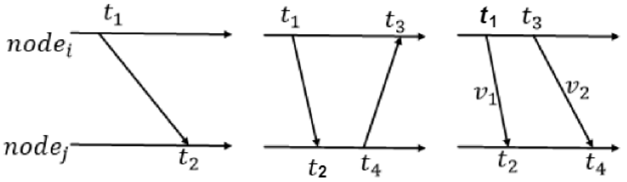

Figure 3: Two way Time-of-Flight.

Once PU's signal is received at the sensing nodes, FC makes the final decision after the local decision is finalized based on detecting the PU's signal. The FC uses SDF and HDF methods to make final decisions. SDF is used when there are less than 100 reports, while HDF is used when there are more than 100 reports. Three HDF techniques, i.e., majority voting, AND, and OR rules, are used in the proposed scheme.

$$G_d = \begin{Bmatrix} H_1 : & \sum_{j=1}^{n} Z_j(l) = n \\ H_0 : & Otherwise \end{Bmatrix} \tag{8}$$

Equation (8) presents the AND rule and SUs reported higher consistency when AND rule is applied. $Z_j(l)$ represents the reports received from all the SUs during the i^{th} time interval. When all SUs report that spectrum is occupied, the channel is considered as occupied. In such cases, the FC generates a global decision H_1 as G_d. If the reports are not unanimous, the FC generates H_0.

$$G_d = \begin{Bmatrix} H_1 : & \sum_{j=1}^{n} Z_j(l) \geq n \\ H_0 : & Otherwise \end{Bmatrix} \tag{9}$$

When the OR rule is applied, and SUs confirms the channel is occupied, FC generates the global decision of H_1 as defined in equation (9). On the other hand, based on the general voting concept is the majority voting rule, in which the overall number of votes determines the outcome. The majority voting rule is used by FC to make decisions in CR networks. In particular, H_1 is only generated if the presence of the PU is approved by more than 50% of the SUs.

$$G_d = \begin{Bmatrix} H_1 : \displaystyle\sum_{j=1}^{n} Z_j(i) \geq k \\ H_0 : \quad Otherwise \end{Bmatrix} \tag{10}$$

Equation (10) represents majority rule, where $Z_j(i)$ represents the reports received from all the SUs during the i^{th} time interval. In this context, k denotes the number of PUs and n is number of Sus present in total.

Results

The proposed research aims at mitigating the harmful effects in CR network for PUEA, the simulation results also compares the conventional HDF technique. The first steps are to create an H-matrix that has been tainted with PUEA attempts. In the next step, three traditional procedures, i.e., majority voting, AND, and OR rules, are applied considering the real position of the PU. The Signal-to-Noise Ratio (SNR) measurement range is -30dB to 0dB, with 270Hz as a sampling frequency and a sensing interval of 1ms. There are 200 iterations carried out in all. The number of iterations can be adjusted to achieve improved results. For the proposed technique, 200 iterations are determined to be optimal, as this yielded the best outcomes. Plots of the results for the traditional HDF are made from iterations 0 to 99, while those for the suggested technique are made from iterations 100 to 200. The y-axis shows the likelihood of a wrong detection with amplitude of error caused by PUEA malicious activities in the network.

Figure 4 shows the results obtained for the PUEA free network, depicting similar results from both sets. The suggested technique is retested on a network with 200-subscriber using single PUEA, yielding distinct error probability and a modification in the graph's behavior from the first effort. Figure 5 displays the test's outcomes. The suggested OR rule has a lower probability of wrong detection compared to traditional OR rule. Figure 6 shows the results for network with ten PUEAs tested with the proposed technique. The probability of error increases when signal-to-noise ratio increases for traditional HDF, whereas the proposed technique keeps the error probability comparatively lower. Figure 7 shows the chance of erroneous detection for the classical HDF approach vs. the proposed technique at various SNR levels. The classical HDF exhibits a higher error probability as SNR increases. On the other hand, the proposed technique has a lower error probability over the SNR range. These results indicate that the proposed strategy is more effective to decrease errors caused by the PUEA, particularly at higher SNR levels.

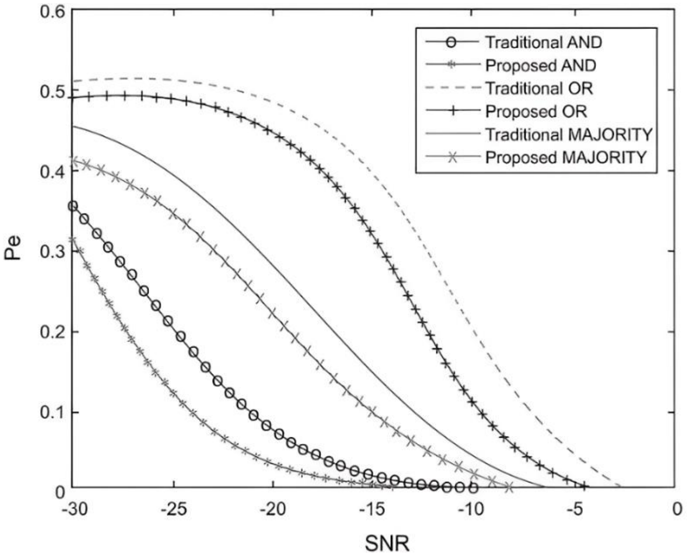

Figure 4: System with no PUEA.

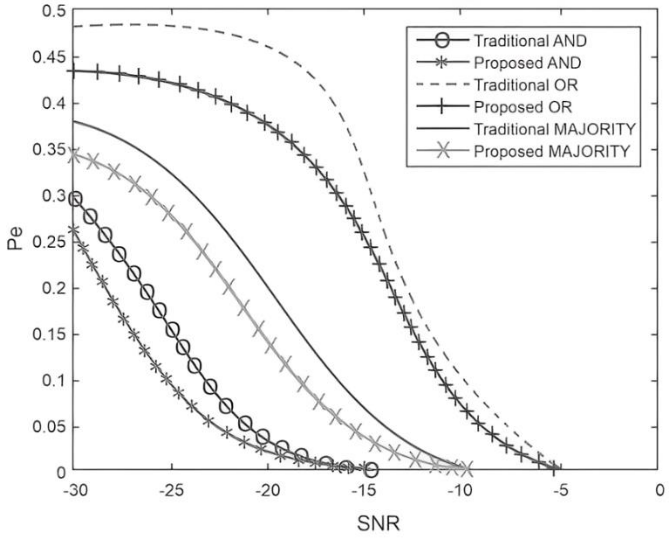

Figure 5: System using single PUEA.

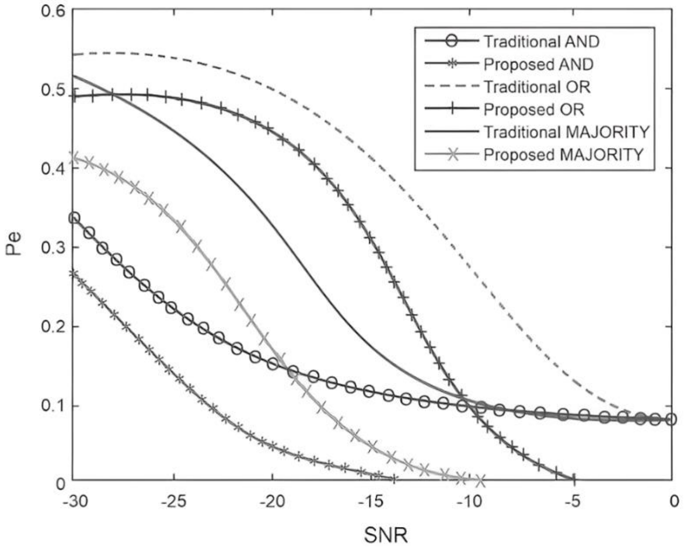

Figure 6: System using 10 PUEA.

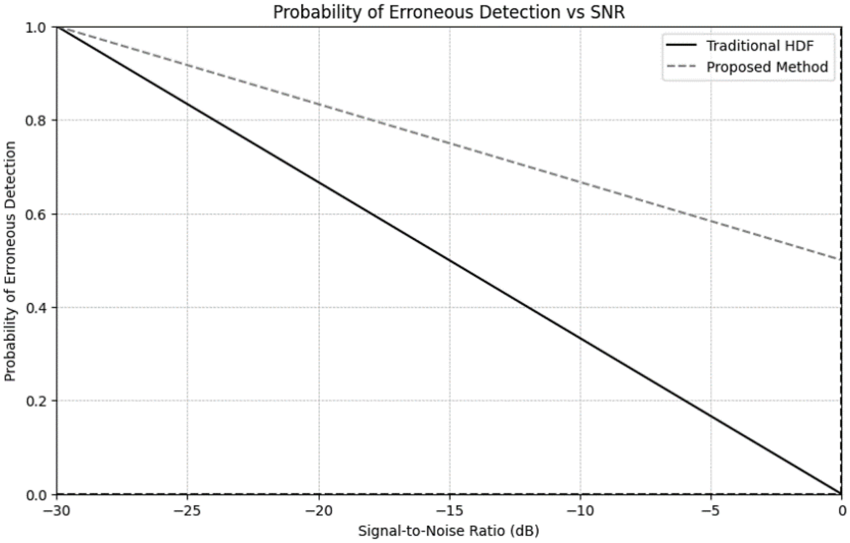

Figure 7: Comparison of error probabilities of traditional HDF vs. Proposed Method.

Conclusion

The CR network represents a more effective solution for the shortage of radio spectrum since it can handle it without requiring costly hardware. It optimally utilizes the available spectrum resources. However, in the presence of emulation attackers, distinguishing between genuine and counterfeit PUs becomes challenging for the FC, which could lead to suboptimal decision-making. This research aims to enhance spectrum sensing strategies to improve the performance of conventional techniques. The reduced processing time and cost is observed by simple techniques of majority voting, AND, and OR Rule, integrating with localization method. Proposed and conventional methods are evaluated using an H-matrix containing PUEA attempts. Comparative analysis of the results indicated that the proposed methodology performs superiorly, providing better outcomes. While traditional methods offer lower processing costs and simplified the implementation, the enhanced approach demonstrate improved effectiveness in spectrum sensing. During natural disasters or emergencies, traditional communication networks may become overloaded or collapse outright. CR technology enables emergency responders to dynamically access available frequencies, ensuring that crucial communications continue to function even when primary channels are congested or unavailable. This skill has the potential to dramatically improve coordination and response operations during crises, eventually saving lives and resources.

References

Abdelhakim, M., Lightfoot, L., Ren, J., & Li, T. (2014). Distributed Detection in Mobile Access Wireless Sensor Networks under Byzantine Attacks. *IEEE Transactions on Parallel and Distributed Systems, 25*(4), 950-959.

Alahmadi, A., Abdelhakim, M., Ren, J., & Li, T. (2014). Defense Against Primary User Emulation Attacks in Cognitive Radio Networks Using Advanced Encryption Standard. *IEEE Transactions on Information Forensics and Security, 9*(5), 772-781.

Ambhika, C. (2024). Discrimination of primary user emulation attack on cognitive radio networks using machine learning based spectrum sensing scheme. *Wireless Networks, 30,* 3135-3147.

Ayoob, A., Khalil, G., & Ayoub, Z. (2023). Spectrum Sensing Using Cooperative Energy and Matched Filter Detectors in Cognitive Radio. *International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 45-49). Bangkok, Thailand: IEEE.

Batool, R., Bibi, N., Muhammad, N., & Alhazmi, S. (2023). Detection of Primary User Emulation Attack Using the Differential Evolution Algorithm in Cognitive Radio Networks. *Applied Sciences, 13*(1), 571.

Chen, R., & Park, J. M. (2006, September). Ensuring trustworthy spectrum sensing in cognitive radio networks. In 2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks (pp. 110-119). IEEE.

Chen, R., Park, J.-M., & Reed, J. (2008). Defense against Primary User Emulation Attacks in Cognitive Radio Networks. *IEEE Journal on Selected Areas in Communications, 26*(1), 25-37.

Chen, S., Zeng, K., & Mohapatra, P. (2011). Hearing is believing: Detecting mobile primary user emulation attack in white space. *Proceedings IEEE INFOCOM,* (pp. 36-40). Shanghai: IEEE.

Gul, N., Mansoor Qureshi, I., Akbar, S., Kamran, M., & Rasool, I. (2018). One-to-Many Relationship Based Kullback Leibler Divergence against Malicious Users in Cooperative Spectrum Sensing. *Wireless Communications and Mobile Computing, 2018*.

Gul, N., Naveed, A., Elahi, A., Saleem Khattak, T., & Qureshi, I. (2017). A combination of double sided neighbor distance and Genetic Algorithm in cooperative spectrum sensing against malicious users. *International Bhurban Conference on Applied Sciences and Technology (IBCAST)* (pp. 746-753). Islamabad: IEEE.

Haldorai, A., & Kandaswamy, U. (2019). Secure Distributed Spectrum Sensing in Cognitive Radio Networks. In *Intelligent Spectrum Handovers in Cognitive Radio Networks* (pp. 175-191). Springer.

Kaligineedi, P., Khabbazian, M., & Bhargava, V. (2010). Malicious User Detection in a Cognitive Radio Cooperative Sensing System. *IEEE Transactions on Wireless Communications, 9*(8), 2488-2497.

Koo, I., & Vu-van, H. (2012). A Robust Cooperative Spectrum Sensing Based on Kullback-Leibler Divergence. *IEICE Transactions on Communications, 95*(4), 1286-1290.

Madbushi, S., & Rukmini, M. S. (2022). Mitigation of primary user emulation attack using a new energy detection method in cognitive radio networks. *Journal of Central South University, 29*, 1510-1520.

Mao, G., Fidan, B., & Anderson, B. D. (2007). Wireless sensor network localization techniques. *Computer Networks, 51*(10), 2529-2553.

Marinho, J., Granjal, J., & Monteiro, E. (2015). A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. *EURASIP Journal on Information Security, 2015*.

Maya, J. A., Vega, L. R., & Tonello, A. M. (2023). Asymptotically Equivalent GLRT Test for Distributed Detection in Wireless Sensor Networks. *IEEE Transactions on Signal and Information Processing over Networks, 9*, 888-900.

Mazumdar, H., Kaushik, A., & Gohel, H. A. (2023). To mitigate primary user emulation attack trajectory using cognitive single carrier frequency division multiple access approaches: Towards next generation green IoT. *Engineering Reports, 5*, e12672.

Mishra, P., & Dewangan, N. (2015). Survey on Optimization Methods For Spectrum Sensing in Cognitive Radio Network. *International Journal of New Technology and Research, 1*(6), 23-28.

Pu, D., Shi, Y., Ilyashenko, A. V., & Wyglinski, A. M. (2011). Detecting Primary User Emulation Attack in Cognitive Radio Networks. *IEEE Global Telecommunications Conference* (pp. 1-5). Houston: IEEE.

Renk, T., Kloeck, C., & K. Jondral, F. (2007). A cognitive approach to the detection of spectrum holes in wireless networks. *4th IEEE Consumer Communications and Networking Conference* (pp. 1118-1122). UK: IEEE.

Sharifi, A., Sharifi, M., & Niya, J. (2016). Collaborative Spectrum Sensing under Primary User Emulation Attack in Cognitive Radio Networks. *IETE Journal of Research, 62*(2), 205-211.

Wu, J., Liu, T., & Zhao, R. (2024). Beta Distribution Function for Cooperative Spectrum Sensing Against Byzantine Attack in Cognitive Wireless Sensor Networks. *Electronics, 13*(17), 3386.

Zhu, G., Wu, J., Liang, H., Tang, J., Xia, L., Bao, J., et al. (2024). Cost and Benefit Tradeoff of SSDF Attack in Cooperative Spectrum Sensing in Cognitive Wireless Sensor Networks. *IEEE Sensors Letters, 8*(5), 1-4.