ISSN (e): 2250 – 3005 || Volume, 15 || Issue, 4|| April – 2025 ||
International Journal of Computational Engineering Research (IJCER)

Defensive Strategies Against Primary User Emulation Attacks in Cognitive Radio Networks

S.Kanimozhi [1], K.Mahalakshmi [2]
Professor,
Annai College of Engineering and Technology, Kumbakonam, India
Associate Professor,
Annai College of Engineering and Technology, Kumbakonam, India

Abstract
Cognitive Radio Networks (CRNs) enhance spectrum utilization by allowing unlicensed users to access unused licensed bands. However, the integrity of this paradigm is threatened by Primary User Emulation Attacks (PUEAs), where malicious nodes imitate primary user signals to manipulate spectrum access. This paper presents a comparative review of three prominent defense strategies: an AES-encrypted synchronization approach for Digital TV systems, a localization-based detection scheme (LocDef), and a Latin Square-based signal tagging method integrated with SC-FDMA. Each technique is assessed based on accuracy, implementation complexity, scalability, and suitability for future wireless networks. The review provides insights into their relative strengths, limitations, and potential for integration in next-generation CRNs.
Keywords: Cognitive Radio, Primary User Emulation Attack, Spectrum Sensing, AES Encryption, Localization, Latin Square Tag, SC-FDMA, CRN Security

---

Date of Submission: 08-04-2025 Date of acceptance: 19-04-2025

I. Introduction

Cognitive Radio Networks (CRNs) represent a dynamic solution to spectrum scarcity by enabling secondary users (SUs) to opportunistically utilize underused licensed spectrum[1][2]. However, this flexibility introduces vulnerabilities, particularly to Primary User Emulation Attacks (PUEAs), in which adversaries mimic primary user (PU) signals to disrupt SU operations. To address this issue, researchers have proposed diverse defense strategies. This paper reviews three notable approaches: (1) a cryptographic method using Advanced Encryption Standard (AES), (2) LocDef, a transmitter verification scheme using localization, and (3) Latin Square tagging with SC-FDMA integration.

A potential remedy for the increasing spectrum shortage in wireless communications is Cognitive Radio Networks (CRNs). CRNs seek to improve spectrum efficiency without affecting primary users by allowing unlicensed secondary users to opportunistically use unused licensed spectrum areas. But because of their openness and adaptability, CRNs are vulnerable to a number of security risks, the most serious of which is the Primary User Emulation Attack (PUEA)[3].

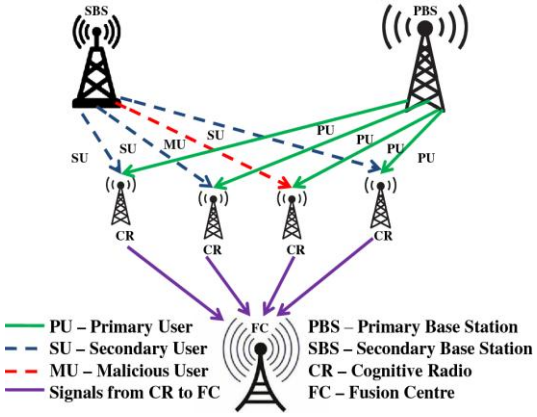

Fig 1 Primary User Emulation Attack

II. Defense Mechanisms

In a PUEA, a malicious node transmits signals mimicking a primary user (PU), deceiving secondary users (SUs) into vacating the channel. This not only disrupts SU communications but also reduces overall spectrum utilization. To mitigate PUEAs, researchers have proposed various strategies focusing on authentication, localization, and signal classification. This paper critically examines three such approaches: (1) an AES-assisted DTV synchronization scheme, (2) the localization-based LocDef system, and (3) a Latin Square tag-based method using Single Carrier-FDMA for green IoT applications.

This paper adopts a qualitative comparative approach. The three selected techniques were analyzed to extract key defense mechanisms, system models, assumptions, detection algorithms, simulation environments, and performance metrics. The comparison is focused on: type of defense strategy (cryptographic, localization, signal tagging), accuracy in detecting malicious users, implementation feasibility and system overhead, scalability to real-world deployments, robustness against smart attackers.

2.1AES- Assisted Digital TV Synchronization

This method suggests a dependable AES-assisted DTV technique in which the sync bits of the DTV data frames are an AES-encrypted reference signal that is created at the TV transmitter. The reference signal can be recreated at the receiver and utilized to accurately identify authorized primary users by permitting the transmitter and receiver to communicate a secret. Furthermore, regardless of whether the primary user is present or not, the presence of the malicious user may be precisely identified when paired with the examination of the auto-correlation of the received signal. The suggested strategy can successfully counteract PUEA. [4].

The approach achieves high accuracy in distinguishing between Primary Users (PUs) and attackers. It maintains the original synchronization functionality and requires no significant hardware changes, as a plug-in AES chip is sufficient. However, its applicability is limited to the DTV spectrum and cannot be generalized across all Cognitive Radio Network (CRN) bands.

2. 2 Localization-Based Defense (LocDef)

[5] suggest a transmitter verification method called LocDef (localization-based defense), which verifies primary signal transmitters by using the transmitter's location as well as its signal characteristics. To identify and track down PUE attackers, a strong non-interactive localization system is presented. To gather snapshots of received signal strength (RSS) measurements throughout a CR network, the localization approach makes use of an underlying wireless sensor network (WSN). The transmitter locations can be estimated by smoothing the gathered RSS readings and locating the RSS peak.

This method provides localization in static PU scenarios and shows robustness against attacks that attempt to emulate signals near known PU towers. It is particularly effective in hostile environments. However, its performance is constrained by the accuracy of localization algorithms and the feasibility of widespread WSN deployment.

2.3 Latin Square Tagging with SC-FDMA

[6] integrates Latin Square matrices within a Single Carrier Frequency Division Multiple Access (SC-FDMA) framework to generate unique authentication tags. These tags are embedded in PU signals and decoded by Secondary Users (SUs) to verify their authenticity. The method offers high resilience against emulation attacks in SC-FDMA networks and achieves improved Bit Error Rate (BER) performance with increasing Signal-to-Noise Ratio (SNR). It is also energy-efficient, making it well-suited for Green Internet of Things (IoT) applications. Nonetheless, the technique involves significant computational complexity, which may pose challenges for implementation in resource-constrained devices.

III. Discussion

The reviewed techniques demonstrate promising solutions to combat PUEAs, each with distinct advantages and challenges:

Security Mechanism: AES tagging provides strong cryptographic assurance but relies on secret key distribution. LocDef uses physical layer cues (location) but depends on dense sensor networks. Latin Square tagging is mathematical and lightweight, suitable for structured communication frameworks.

Deployment Scope: While the AES method is limited to DTV systems, LocDef and SC-FDMA can be extended to broader CRN contexts with suitable modifications.

Table 1.

Metric	AES Tagging	LOC Def	LS Tagging and SC-FDMA
Detection Accuracy	High	Moderate to High	High
Hardware Requirement	AES Chip	WSN sensors	SC-FDMA Support
Generalization	Low (DTV-Specific)	Moderate	High (IoT & CRNs)
Energy Efficiency	High	High	Moderate
Complexity	Moderate	Limited by deployment	High

Comparative Analysis

Scalability: LocDef may face scaling challenges in large or mobile networks. LS tagging, though efficient, may suffer from increased complexity under dynamic traffic.
Resilience: All methods offer robustness, but none is completely foolproof against highly adaptive attackers employing Machine Learning or GAN-based strategies.

IV. Research Gaps

Several important research gaps remain in the current approaches to defending against Primary User Emulation Attacks (PUEAs) in Cognitive Radio Networks. One significant gap is the absence of hybrid defense frameworks that combine cryptographic techniques, location-based verification, and behavioral analysis to enhance detection reliability and adaptability.

Additionally, there is a clear need for lightweight defense mechanisms that are specifically tailored for IoT-integrated CRNs, where devices often operate with constrained computational and energy resources. Furthermore, most existing studies rely heavily on simulations, highlighting a lack of real-world experimentation and validation in practical deployment scenarios. Addressing these gaps is essential for advancing robust and scalable PUEA defense strategies

V. Conclusion

Defending Cognitive Radio Networks against PUEAs is critical for the secure adoption of dynamic spectrum access. This review highlights that while current methods like AES tagging, localization-based verification, and Latin Square coding each offer unique advantages, a comprehensive defense strategy may require integrating multiple approaches. Future work should focus on hybrid, scalable solutions adaptable to evolving threat landscapes.

References

[1] 1. J Mitola, GQ Maguire, Cognitive radio: making software radios more personal. IEEE personal Commun J. 6(4), 13–18 (1999). doi:10.1109/98.788210

[2] S Haykin, Cognitive radio: brain-empowered wireless communications. IEEE J Sel Areas Commun. 23(2), 201–220 (2005)

[3] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," in Proc. IEEE Workshop Netw. Technol. Softw. Defined Radio Netw., Sep. 2006, pp. 110–119.Cabric, "Addressing the feasibility of cognitive radios," IEEE Signal

[4] A. Alahmadi, M. Abdelhakim, J. Ren, and T. Li, "Defense against primary user emulation attacks in cognitive radio networks using advanced encryption standard," IEEE Trans. Inf. Forensics Secur., vol. 9, no. 5, pp. 772–781, May 2014.

[5] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," IEEE J. Sel. Areas Commun., vol. 26, no. 1, pp. 25–37, Jan. 2008.

[6] H. Mazumdar, A. Kaushik, and H. A. Gohel, "To mitigate primary user emulation attack trajectory using cognitive single carrier frequency division multiple access approaches: Towards next generation green IoT," Engineering Reports, vol. 5, no. 12, pp. 1–23, 2023.

[7] F. Digham, M. Alouini, M. Simo "On the Energy Detection of Unknown Signals over Fading Channels," *in Proc., IEEE International Conference Communications*, Anchorage, AK, vol. 5, pp. 3575-3579, May 2003.

[8] Y. Wu, B. Wang, K. J. Ray Liu. "Optimal Defense against Jamming Attacks in Cognitive Radio Networks using the Markov Decision Process Approach". IEEE Globecom 2010 proceedings.