A Survey of the Primary User Emulation Attack in the Cognitive Radio Networks

*Olaleru, G[1], Ohize H.O[2], Dauda U.S[3], Mohammed A.S[4]
[1]Electrical and Electronics Engineering Department, Federal University of Technology, PMB 65 Minna Niger State, Nigeria
[2]Electrical and Electronics Engineering Department, Federal University of Technology, PMB 65 Minna Niger State, Nigeria
[3] Federal University of Technology, PMB 65 Minna Niger State, Nigeria
[4] Federal University of Technology, PMB 65 Minna Niger State, Nigeria.
Corresponding author email: graceolaleru9@gmail.com +2348164649551

ABSTRACT

Cognitive Radio Technology (CRT) helps alleviate the spectrum scarcity and spectrum underutilization problems experienced by wireless networks and wireless devices by enabling the intelligent and opportunistic use of the licensed frequency band by unlicensed users. However, due to its wireless nature, it is subject to some security threats that affect the practical implementation of the CRT. In this paper, we have discussed some of the security threats affecting the protocol stack and the five layers of the Cognitive Radio Network (CRN), with a focus on the Primary User Emulation Attack (PUEA). The PUEA is one of the most common attacks on the CRN's physical layer. In this attack, a selfish or malicious user mimics the primary user's (PU) signal features to fool the legitimate secondary users (SUs), causing the legitimate SUs to leave the available channel while the real PU is absent. Although many review papers enhanced our knowledge of the PUEA, in this paper we meld new research findings with the old ones to keep up the pace in the research community. Also, we discussed some detection and countermeasures for the PUEA in the CRN. Finally, a summary of the findings on how best to mitigate the effect of PUE attacks in the CR is presented.

Keywords: *Cognitive Radio, Primary User, Primary User Emulation Attack, Secondary User, Security threats.*

1 INTRODUCTION

The radio spectrum used for wireless communications is a scarce resource due to the dramatic increase in the number of wireless devices and more bandwidth-demanding multi-media services [1-4]. These wireless devices use either the licensed spectrum or the unlicensed spectrum. The unlicensed bands are becoming overcrowded because all wireless users can connect. However, the licensed bands are either unused or underutilized at some geolocation and time. To address the problem of frequency scarcity and spectrum underutilization, Cognitive Radio (CR) was introduced by Joseph Mitola in 1999 [5]. The CR is a software-defined radio that enables Dynamic Spectrum Access (DSA) which enables unlicensed users to intelligently and opportunistically access and utilize the spectrum without disrupting the licensed users and therefore a better service to achieve improvement in frequency usage [2, 6]. The CR performs four basic functions that allow it to address spectrum shortages and channel underutilization [7]. These functions are (a) Spectrum Sensing which involves identifying the primary user's spectrum occupancy status, (b) Spectrum management, which captures the best available spectrum to meet users' communication needs and avoid collisions with other CRs (c) spectrum sharing: this relates to the provision of fair spectrum scheduling, and (d) spectrum mobility: defined as the process of a CR user changing its operating frequency to meet the quality of service. However, due to the wireless nature of CRT and the priority given to licensed users or primary users (PUs) over secondary users (SUs) in spectrum usage, CRN faces several security threats. One of these threats is PUEA, in which a malicious user fools the SU by mimicking the PU's signal features in relation to the PU's occupancy status. The impacts of PUEA include denial of service, wasted bandwidth, connection unreliability, and degrading the practical implementation of the CRN. Other threats that the CRN faces are classified as they affect the protocol stack and the five layers of the CR network. These include, but are not limited to: Common Control Data Attack (CCDA), Sinkhole Attack, Hello flood attack, lion attack, and jellyfish attack. These threats aim to reduce the possibility of building a real CRN, so, threat mitigation is crucial to building a real CRN.

In this paper, we have highlighted the security threats affecting the CRN with a focus on the PUEA. We also highlighted some of the detection and countermeasures used for the PUEA in the CR networks. This paper has the following research contributions:

- A detailed discussion of the security threats affecting the protocol stack and the five layers of the CRN.
- A detailed review of the PUEA in CRN stating its classification, its impacts, methods for its detection, and countermeasures.
- A summary of the findings on how best to mitigate the impact of PUE attacks in the CR.
- Meld new research findings with the old ones to keep up the pace in the research community.