Threats Advancement in Primary User Emulation Attack and Spectrum Sensing Data Falsification (SSDF) Attack in Cognitive Radio Network (CRN) for 5G Wireless Network Environment

A.H.Fauzi and A.S.Khan
Faculty of Computer Science and Information Technology,
Universiti Malaysia Sarawak, Sarawak, Malaysia.
hadinata@unimas.my

***Abstract*—Primary User Emulation (PUE) attack and Spectrum Sensing Data Falsification (SSDF) attack on Data Fusion Centre and attack on Common Control Channel (CCC) is a serious security problems and need to be addressed in cognitive radio network environment. We are reviewing the recent advances of threats for the future 5th Generation (5G) wireless radio network from these attacks. Several existing security schemes have been proposed and discussed to overcome these attacks. We propose new security scheme that able to mitigate the attacks and provide security solutions. This scheme intended to mitigate the threats from the attacks in CRN and improve the future 5G network security.**

***Index Terms*—CRN; Data Fusion; Radio Network; Wireless 5G; Secure; PUE; SSDF.**

I. Introduction

Cognitive Radio Network (CRN) was introduced as a promising technology to solve the issues of spectrum scarcity in cellular wireless network due to the increasing number demand of wireless services [1]. Cognitive Radio Network is part of the 5G initiative towards high speed and secure wireless radio network.

The concept of the 5G network is promising to satisfy the growing needs of mobile wireless communication. Along with increasing data rate, number of users, reliability and coverage of the mobile network, security is a matter of key importance that requires careful consideration. As with the upcoming spread of the Internet of Things (IoT) that the 5G network is going to propagate to almost all aspects of our lives, security will become even more crucial than it is now [2].

Security is one of the fundamental aspects of the next generation mobile network [3]. Many new technologies are emerging to be deployed in the 5G network and improve its performance. Their security issues should be examined so that appropriate countermeasures can be taken before new technologies are deployed into live operation. Novel approaches for security enhancement also have been proposed. In particular, physical layer security seems to offer reasonable solutions for many security requirements [4]. It is important to recognize its possible risks and point out topics for further research.

The rapidly growing number of mobile devices, capacious data and higher data rate are pushing to reconsideration the existing generation of the cellular mobile communication. The next or fifth generation (5G) wireless network is expected to meet high end requirements. The 5G networks would provide novel architecture and technologies beyond state of the art architecture and technologies. The new research track will lead the elementary changes in the design of fifth generation (5G). The 5th generation mobile network signifies the next foremost phases of mobile telecommunications standards beyond the current 4G. 5G has speeds beyond what the current 4G can offer.

The Next Generation Mobile Networks Alliance realizes that 5G should be rolled out by 2020 to meet the business and consumer demands. In addition to providing simple faster speeds, they expect that 5G networks also will need to meet the needs of new use case, such as Internet of Things (IoT) as well as broadcast-like services and lifeline communication in times of natural misfortune. Cognitive Radio Network will help 5G by Device-to-device (D2D) communication [5], Moving Network (MN) [6], Ultra Dense Network(UDN) [7] and Self Organizing Network(SON) [8].

Cognitive Radio Network consist of two type of users that are licensed primary user (PU) of the cellular network and unlicensed secondary user (SU). Secondary user constantly observed the licensed spectrum band by performing spectrum sensing to check the availability of the channel for them to use. When vacant spectrum channel discovered, secondary user will transmit using the available channel. However, in a legitimate manner, if secondary user sense any PU signal which indicates that PU wants to use the channel, SU will need to back off and find another available channels [9]. There are several well-known challenges CRN. Among them are:

- Performance degradation overall Cognitive Radio Net-work Quality of Service (QoS) and underutilized channel usage in Cognitive Radio Network due to attack from malicious user.
- Protecting the Data Fusion Centre becomes target for false data input and data manipulation. Data fusion centre used to store information from legitimate user details and makes global decision
- Denial of Service attack on Data Fusion and Common Control Channel.

In this paper we will address the security issues in 5G wireless network. In particular, we study the security challenges of CRN in 5G. This paper aims to review the advances of threats in primary user emulation attack, spectrum sensing