Chapter 61
Towards Security Issues and Solutions in Cognitive Radio Networks

Saed Alrabaee
Concordia University, Canada

Mahmoud Khasawneh
Concordia University, Canada

Anjali Agarwal
Concordia University, Canada

ABSTRACT

Cognitive radio technology is the vision of pervasive wireless communications that improves the spectrum utilization and offers many social and individual benefits. The objective of the cognitive radio network technology is to use the unutilized spectrum by primary users and fulfill the secondary users' demands irrespective of time and location (any time and any place). Due to their flexibility, the Cognitive Radio Networks (CRNs) are vulnerable to numerous threats and security problems that will affect the performance of the network. Little attention has been given to security aspects in cognitive radio networks. In this chapter, the authors discuss the security issues in cognitive radio networks, and then they present an intensive list of the main known security threats in CRN at various layers and the adverse effects on performance due to such threats, and the current existing paradigms to mitigate such issues and threats. Finally, the authors highlight proposed directions in order to make CRN more authenticated, reliable, and secure.

1. INTRODUCTION

Nowadays, there is an unexpected explosion in the demand for wireless network resources. This is due to the intense increase in the number of the emerging services. For wireless computer network, limited bandwidth along with the transmission quality requirements for users, make quality of service (QoS) provisioning a very challenging problem as highlighted by Bhargavaand et al. (2007). To overcome

DOI: 10.4018/978-1-4666-9840-6.ch061

spectrum scarcity problem, Federal Communications Commission (FCC) has already started working on the concept of spectrum sharing where unlicensed users (also known as secondary users or SUs) can share the spectrum with licensed users (also known as primary users or PUs), provided they respect PUs rights to use spectrum exclusively. The underutilization of the allocated spectrum has been also reported by the Spectrum Policy Task Force appointed by Federal Communications Commission (FCC) (2002).

In spectrum sharing based CR networks, secondary users (SUs) coexist with a primary user (licensed) system. A fundamental challenge is how to serve SUs while ensuring the quality of service (QoS) of the primary user (PU).

Cognitive radio networks (CRNs) are smart networks that automatically sense the channel and adjust the network parameters accordingly. In CRN, the unlicensed user (SU) has the possibility of using large amounts of unused spectrum in an efficient way while reducing interference with other licensed user (PU). The key technology in CRNs that enables the SUs to sense and utilize the spectrum is the radio technology. This technology is an emerging technology that enables the dynamic deployment of highly adaptive radios that are built upon software defined radio technology (SDR) as mentioned in Dhar et al. (2006) and Qusay et al. (2007). Moreover, it allows the unlicensed operation to be in the licensed band. We show the tasks in cognitive radio network that have been conducted from 2006 to 2014 in Table 1.

Hence, a crucial requirement of cognitive radio networks is their ability to utilize the whole spectral band during the presence/absence of primary users. This process is called spectrum sensing and is performed either locally by a secondary user or collectively by a group of secondary users as showed in Dhar et al. (2006). Hence, the cognitive radio network paradigm raises many technical challenges such as the power efficiency, spectrum management, spectrum detection, environment awareness, distributed spectrum measurements, admission control, and the security issues like the unauthorized intrusion and malicious users. Most of the previous works on CRN do not consider security issues which are more challenging since the security problems faced by a CRN are unique as compared to the ones in conventional Wireless Networks.

In CRN, security threats are much more complex and possibility of an attack is higher than in other networks since the network nodes are much more intelligent by design. Hence, security measurements and polices should be developed to reduce the opportunity that malicious nodes attack the CR network. Here we will be considering different scenarios of the different attacks that target different layers of protocol stack in order to propose new models to detect and mitigate these attacks.

Table 1. Cognitive radio network research history

Year	Network Capabilities	System Capabilities	Platform Integration
2006	Not Applied	3) Throughput challenge 4) Radio Technology Management	Software Radio on general purposes CPUs
2007			
2008			
2009	4) Mobile Networks 5) Fixed Network Management 6) Radio Frequency (RF) management	Initial RF adaptive algorithm	Software Radio on general purposes CPUs, DSP, and FPGA radios
2010			
2011			
2012	Cognitive capability: Sense, Adapt, Configure, and Utilize	Throughput Competitive	Advanced Integrated RF control and management
2013			
2014			