Chapter 13
Security for Cognitive Radio Networks

Rajni Dubey
Shri Ram College of Engineering & Management, India

Sanjeev Sharma
SOIT, UIT, Rajiv Gandhi Proudyogiki Vishwavidyalaya, India

Lokesh Chouhan
ABV-Indian Institute of Information Technology and Management, India

ABSTRACT

Most of the frequency spectrum bands have already been licensed, and the licensed spectrum is not being utilized efficiently. Cognitive Radio Networks (CRNs) are the kind of full duplex radio that automatically altered its transmission or reception parameters, in such a way that the entire wireless communication network of which it is a node communicates efficiently, while avoiding interference with primary or secondary users. In this chapter, the authors introduce the concept of security threats that may pose a serious attack in CRN. Due to the unique characteristics of CRN, such network is highly vulnerable to security attacks compared to wireless network or infrastructure-based wireless network. The main objective of this chapter is to assist CR designers and the CR application engineers to consider the security factors in the early development stage of CR techniques. Challenges and various security issues are explored with respect to OSI (Open Systems Interconnection) reference model. Various possible and attacks are discussed broadly and respective solutions are also proposed by this chapter. Different architectures and models are also explained, and compared with the existing models.

13.1 INTRODUCTION

Today's wireless networks are characterized by a fixed spectrum assignment policy. However, a large portion of the assigned spectrum is used sporadically and geographical variations in the utilization of assigned spectrum ranges from 15% to 85% (FCC Std., 2003). The influence of CRNs functions on the performance of the upper layer protocols such as routing and transport are exigent and open research issues in these areas are also challenging issues in CRN (Q. Y. How & K.C.,

DOI: 10.4018/978-1-4666-2005-6.ch013

2011; E. Cesena & Cuomo, 2011). So there is always requirement of CR-MAC (Cognitive Radio Medium Access Control) protocol to provide efficient, fair, and seamless services to user. One of the factors which should be considered during design process of CR-MAC protocol is security of the network infrastructure and security of transmitted information. Without proper network security, attacker responsible for the disaster would be able to eavesdropping important information and utilize it for future attacks. Moreover, the network elements due to their poor security could become a target of attack itself (H. S. Lean, O., 2010; J. Burbank, 2008; G. X. Zhang, Y. 2008). Because cognitive radio constitutes a new approach for building wireless networks, it simultaneously opens a door for new methods of attacks on their physical infrastructure and architecture.

The recent years have been seen major and remarkable development in the field of CRN technologies. Cognitive radio is a revolutionary technology, they promise to improve the utilization of radio frequencies, making room for new and additional commercial data, emergency and military communication services. In this chapter we will introduce the concept of security threats that may pose a serious attack in Cognitive radio network. Due to the unique characteristics of cognitive radio network, such network is highly vulnerable to security attacks compared to wireless network or infrastructure based wireless network. We know that most of the frequency spectrum band has already been licensed and the licensed spectrum is not being utilized efficiently. Cognitive radio helps to efficiently utilize the spectrum band when the primary user is not using it. The main objective of this chapter is to assist CR designers and the CR application engineers to consider the security factors in the early development stage of CR techniques.

Cognitive radios facilitate in the secondary usage of the licensed spectrum (when not in use). When in use by a primary user, the secondary user cannot use it. Therefore, accurate spectrum occupancy information needs to be maintained by a secondary user. This minimizes the interference. A malicious user can try to falsify the spectrum occupancy information, which may cause interference.

This chapter has attempted to exemplify the multi-discipline nature of developing cognitive radio security models, and has attempted to outline analogies and comparisons to applicable research communities. This chapter has attempted to illustrate that the traits of a CR (awareness, adaptation, etc.) are human traits that we as designers are attempting to impose on machines. Frequency spectrum is a limited resource for wireless communications and may become congested owing to a need to accommodate the diverse types of air interface used in cognitive radio networks. However, since conventional wireless communications systems also utilize the frequency bands allocated by the Telecom Regulatory Authority of India (TRAI) and Federal Communications Commission (FCC) in a static manner, they lack adaptability (TRAI std., 2012). Also, several studies show that while some frequency bands in the spectrum are heavily used, other bands are largely unoccupied most of time. These latent vacant spectrums result in the under-utilization of available frequency bands. To defeat the overcrowding (Figure 1), different governing and non governing agencies and organization such as TRAI and Federal FCC have been investigating new ways to manage Radio Frequency (RF) resources (FCC Std., 2003). With advances in software and cognitive radio, practical ways of doing this are on the perspective. In 2003, the FCC released a memorandum seeking comment on the interference temperature model for controlling spectrum use (FCC Std., 2003). Spectrum Hole: In the literature (S. Haykin, 2005) Simon Haykin has defined (Figure 1), "A spectrum hole is a band of frequencies assigned to a primary user, but, at a particular time and specific geographic location, the band is not being utilized by that user (M. S. Tandra, R., 2009).