Chapter 9
An Overview of Security Issues in Cognitive Radio Ad Hoc Networks

Noman Islam
Karachi Institute of Economics and Technology, Karachi, Pakistan

Muhammad Furqan Zia
https://orcid.org/0000-0003-2769-6610
Koc University, Istanbul, Turkey

Darakhshan Syed
Bahria University, Pakistan

ABSTRACT

Cognitive radio ad hoc network (CRAHN) is an emerging discipline of network computing. It combines the advantages of cognitive radio networks and mobile ad hoc networks. This chapter starts with an overview of various research issues of CRAHN along with representative solutions for these research issues. Among the various research issues presented, security is discussed in detail due to its prime importance. A review of existing literature reveals that not much work on security has been reported for cognitive radio networks. Specifically, an overview of security issues in CRAHN, presented in this article, is a novel work of this kind. A major part of this article highlights the importance of security in CRAHN and presents an overview of major security issues and the solutions proposed to address these issues in CRAHN.

1. INTRODUCTION

A cognitive radio (CR) is a communication device that can adjust its operating properties based on its environment. It proactively observes the unlicensed communication channels in surroundings that are not in use. It then tunes itself on these free channels, and then utilizes them for communication (Yu

DOI: 10.4018/978-1-6684-7684-0.ch009

et al., 2020). This process, called dynamic channel selection, solves the spectrum scarcity issue of the wireless network. However, due to high variation in the availability of channels and various quality of service (QoS) requirements in the available spectrum, CR networks face several unique challenges. For instance, dynamic spectrum access (DSA) is required to optimize spectrum usage to solve the spectrum insufficiency issue. In DSA, there is an unlicensed device known as the secondary user (SU) or cognitive radio user. This SU leaves the band when a licensed device known as the primary user (PU) is detected.

To enable DSA, two main aspects of CR need to be considered. These are cognitive capability and re-configurability (Zhou et al., 2018). Cognitive capability enables spectrum awareness by sensing the statistics from its radio environment. Using the cognitive capability, the secondary users of the cognitive network becomes ascertain about the status of various channels and can optimally decide the spectrum to use along with its operating parameters. Re-configurability denotes the ability of a node to adjust its transmission parameters. Re-configurability of a CR demands it to be programmed dynamically for enabling transmission and reception of signals on various operating parameters and make it capable of working on multiple access technologies.

More complex strategies such as autonomous learning and action decisions are required to acquire the cognitive capability, which the system cannot learn by noticing the power of specific spectrums (Peng et al. 2020). In autonomous learning, each node autonomously learns based on its experiences and feedback obtained from the environment. Action decision techniques enable a user to achieve spatiotemporal variations in radio environment. Also, this capability provides interference avoidance between users.

Another primary concern in CR networks is to share spectrum sharing without causing interception to other nodes. The unused spectrum is represented by spectrum hole or white spaces. If the license user wants to further utilize its spectrum, the CR user has to move on to some other spectrum hole. Alternatively, if a user still wishes to continue in the same spectrum without letting the nodes to intercept, it must change the power level of transmission or modulation technique. In order to adapt the dynamic spectrum environment, the cognitive radio ad-hoc networks necessitate spectrum-aware operations, which form a cognitive cycle (Onem et al., 2013). The basic steps of the cognitive cycle consist of four spectrum management functions: spectrum sensing, spectrum decision, spectrum sharing, and spectrum mobility.

We can classify CR networks into two types based on architecture: infrastructure-based cognitive radio and cognitive radio ad-hoc networks (CRAHN). The infrastructure-based cognitive radio networks are controlled from a central location. For example, in cellular networks, the core network component is called the base station, whereas, in wireless local area networks (WLAN), it is known as an access point. On the other hand, the cognitive radio ad hoc network (CRAHN) has no infrastructure and is formed among a set of communication entities equipped with cognitive radios.

This paper discusses the security issues in CRAHN. The novelty of the paper lies in discussing not only the technical issues in CRAHN, but also social and policy issues. The next section presents an overview of security challenges pertaining to CRAHN. Then, security challenges are presented. Discussion on CRAHN security issues is presented. Finally, social and policy making issues are discussed.