Chapter 11
Security and Privacy Challenges in Cognitive Wireless Sensor Networks

Jaydip Sen
Tata Consultancy Services Ltd., India

ABSTRACT

Wireless sensor networks (WSNs) have attracted a lot of interest in the research community due to their potential applicability in a wide range of real-world practical applications. However, due to the distributed nature and their deployments in critical applications without human interventions and sensitivity and criticality of data communicated, these networks are vulnerable to numerous security and privacy threats that can adversely affect their performance. These issues become even more critical in cognitive wireless sensor networks (CWSNs) in which the sensor nodes have the capabilities of changing their transmission and reception parameters according to the radio environment under which they operate in order to achieve reliable and efficient communication and optimum utilization of the network resources. This chapter presents a comprehensive discussion on the security and privacy issues in CWSNs by identifying various security threats in these networks and various defense mechanisms to counter these vulnerabilities. Various types of attacks on CWSNs are categorized under different classes based on their natures and targets, and corresponding to each attack class, appropriate security mechanisms are also discussed. Some critical research issues on security and privacy in CWSNs are also identified.

INTRODUCTION

Over the last decade, wireless sensor networks (WSNs) have attracted a lot of interest in the research community due to their wide range of potential applications. A WSN consists of hundreds or even thousands of small devices each with sensing, processing, and communication capabilities to monitor a real-world environment. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring (Akyildiz et al., 2002). Most of the WSN deployments operate in the unlicensed ISM bands (2.4GHz). Several other small range wireless protocols like Wi-Fi, Bluetooth etc. also use the same band. This has led to overcrowding in this band with the increasing deployment of WSN-based applications. As a result, coexistence issues in the ISM bands have attracted extensive research attention (Cavalcanti et al., 2007).
The increasing demand for spectrum in wireless communication has made efficient spectrum utilization a big challenge. To address this important requirement, cognitive radio (CR) has emerged as the key technology. A CR is an intelligent wireless communication system that is aware of its surrounding environment, and adapts its internal parameters to achieve reliable and efficient communication and optimum utilization of the resources (Mitola, 2000). With the advent of CR technology, we have a different perspective of the traditional WSNs. In the current cognitive wireless sensor networks (CWSNs), the nodes change their transmission and reception parameters according to the radio environment. Cognitive capabilities are based on four activities: (i) monitoring of spectrum sensing, (ii) analysis and characterization of the environment, (iii) optimization of the best communication strategy based on different constraints such as reliability, power, security and privacy issues etc., and (iv) adaptation and collaboration strategy. The cognitive technology will not only enable access to new spectrum but it will provide better propagation characteristics leading to reduction in power consumption, network life-time and reliability in a WSN. With cognitive capabilities, WSN will be capable of finding a free channel in the unlicensed band to transmit or could find a free channel in the licensed band for communication. A CWSN, therefore, will be able to provide access not only to new spectrum bands in addition to the available 2.4 GHz band, but also to the spectrum band that has better propagation characteristics. If a channel in a lower frequency band is accessed, it will certainly allow communications with higher transmission range in a CWSN, and hence fewer sensor nodes will be required to provide coverage in a specific area with a higher network life-time due to lower energy consumption in the nodes. CWNs will also provide better propagation characteristics by adaptively changing systems parameters like modulation schemes, transmit power, carrier frequency and constellation size. The result will be a more reliable communication with reduced power consumption, increased network life-time and higher reliability and enhanced quality of service (QoS) guarantee to applications.

In spite of the several advantages and benefits that CWSNs will bring forth (Cavalcanti et al., 2008), ensuring security will be a major challenge in these networks. Unless these challenges are solved to an effective level, deployment of CWSNs in real-world applications will face a serious impediment. As observed in (Burbank, 2008), the CR nature of a system introduces an entirely new gamut of threats and vulnerabilities that cannot be easily mitigated. These three salient characteristics of CR are its environmental awareness, learning and acting capabilities. Considering these characteristics from an attacker’s perspective, a CWSN will provide much more capability to an attacker to launch attacks that are long-lasting and catastrophic in nature and those which can be triggered by simple spectral manipulations (Araujo, et al., 2012).

Security had already been an extensive area of research in WSN (Sen, 2009; Zhou et al., 2009; Martins & Guyennet, 2010). With the advent of CWSN and the perspective of security taking a much wider and complicated scope, it is obvious that research on the security aspects on CWSNs will attract even more attention of the research community. However, despite considerable amount of research on CR networks and the new interest in CWSNs, security in CWSNs has been a vastly unexplored area. Sensor data privacy will be another critical area which will be increasingly relevant as these networks find more applications in deployments that deal with sensitive and critical data.

Keeping this emerging trend of technology in mind, this chapter intends to provide a panoramic view of security and privacy-related issues in WSNs with particular focus on CWSNs. In the following sections, we present an extensive discussion on various security issues in WSNs and CWSNs and present their appropriate defense mechanisms based on the current state of the art.