Chapter 108
Security of Wireless Sensor Networks: The Current Trends and Issues

Mumtaz Qabulio
https://orcid.org/0000-0002-9294-2657
Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan

Yasir Arfat Malkani
Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan

Muhammad S. Memon
Department of Information Technology, University of Sindh, Dadu Campus, Pakistan

Ayaz Keerio
Institute of Mathematics and Computer Science, University of Sindh, Jamshoro, Pakistan

ABSTRACT

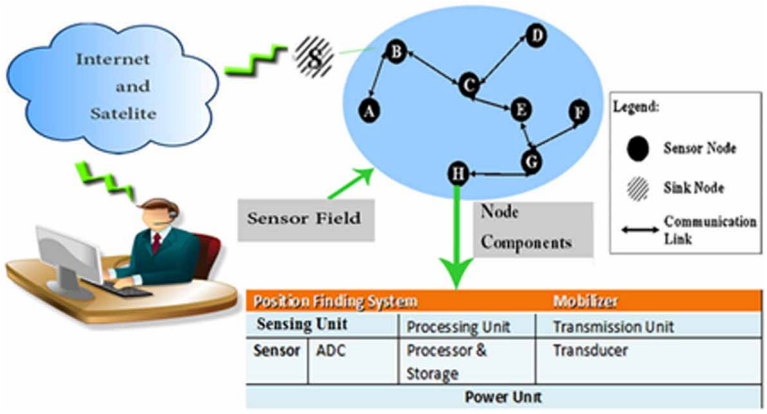
Wireless sensor networks (WSNs) are comprised of large collections of small devices having low operating power, low memory space, and limited processing capabilities referred to as sensor nodes. The nodes in WSNs are capable of sensing, recording, and monitoring environmental conditions. Nowadays, a variety of WSNs applications can be found in many areas such as in healthcare, agriculture, industries, military, homes, offices, hospitals, smart transportation, and smart buildings. Though WSNs offer many useful applications, they suffer from many deployment issues. The security issue is one of them. The security of WSNs is considerable because of the use of unguided medium and their deployment in harsh, physically unprotected, and unattended environments. This chapter aims to discuss various security objectives and security attacks on WSNs and summarizes the discussed attacks according to their categories. The chapter also discusses different security protocols presented to prevent, detect, and recover the WSNs from various security attacks.

DOI: 10.4018/978-1-7998-5339-8.ch108

INTRODUCTION

The WSNs are closely deployed self-organizing and self-healing networks. WSNs are composed of tiny devices called sensor nodes. Those nodes are equipped with limited power, memory and processing capabilities (Mumtaz Qabulio, 2015). The sensor nodes are designed to measure environmental conditions such as light, temperature, heat, pressure, smoke, fire, dust, humidity, soil, object motion and human activity recognition (Jordao, Torres, & Schwartz, 2018), etc. Nowadays, the WSNs are getting popular and are being deployed extensively due to the range of applications they support and due to the decline in their costs. Some of the attractive and emerging applications of WSNs are found in environment monitoring, in environmental control (e.g. fire detection, air pollution monitoring, flood, traffic control Systems) in military (e.g. monitoring of equipments), in wearable computing (e.g. wrist-worn integrated health monitoring device), in context-aware ubiquitous applications (e.g. Sentient Computing, Ambient Intelligence, Interactive Games and Toys, Augmented reality). The WSNs are also powerful technology in enabling Internet of Things (IoT) (Khalil, Abid, Benhaddou, & Gerndt, 2014; Patil & Chen, 2017). Figure 1 presents an abstract architecture of the WSNs which is comprised of three layers (e.g. sensor field layer, end-user layer and internet/satellite layer). The sensor field is composed of sensor nodes; sensor nodes are basic and essential part of the wireless sensor networks (Michal, 2013) because they are responsible to perform core tasks for the network (e.g. sensing, communication, processing).

Figure 1. High Level Architecture of WSNs



The sensor nodes are equipped with various units (e.g. sensing, processing, communication and power units). These nodes might have position finding and mobilizer modules too (Mishra & Thakkar, 2012). All sensor node units and modules are also presented in figure 1. Each of the unit and module is supposed to perform specific task such as the sensing unit accommodates sensors in order to measure environmental conditions and analogue-to-digital converter in order to convert received analogue signal in the digital form. The processing-unit is comprised of a processor and multiple memories such as RAM and ROM for storing the data and for performing data processing operations. The communication unit constitutes of a radio transceiver for sending and receiving data to and from other network nodes. The power-unit accommodates the energy-source and is ought to provide uninterrupted power supply to all sensor node