Chapter 10
A Survey on Security in Wireless Sensor Networks:
Attacks and Defense Mechanisms

Ilker Korkmaz
Izmir University of Economics, Turkey

Orhan Dagdeviren
Ege University, Turkey

Fatih Tekbacak
Izmir Institute of Technology, Turkey

Mehmet Emin Dalkilic
Ege University, Turkey

ABSTRACT

Wireless Sensor Network (WSN) is a promising technology that has attracted the interest of research in the last decade. Security is one of the fundamental issues in sensor networks since sensor nodes are very resource constrained. An attacker may modify, insert, and delete new hardware and software components to the system where a single node, a specific part of the sensing area, and the whole network may become inoperable. Thus, the design of early attack detection and defense mechanisms must be carefully considered. In this chapter, the authors survey attacks and their defense mechanisms in WSNs. Attacks are categorized according to the related protocol layer. They also investigate the open research issues and emerging technologies on security in WSNs.

INTRODUCTION

In the last few years, with the advancements in technology, new device designs that are different than the personal computers, laptops and servers have been introduced and used extensively all over the world. These devices are smaller and cheaper, and use less energy than the ordinary designs. Besides, they are designed on the integrated circuits having a low power communication unit. Their design techniques provide the use of Wireless Sensor Networks (WSNs). A microprocessor of

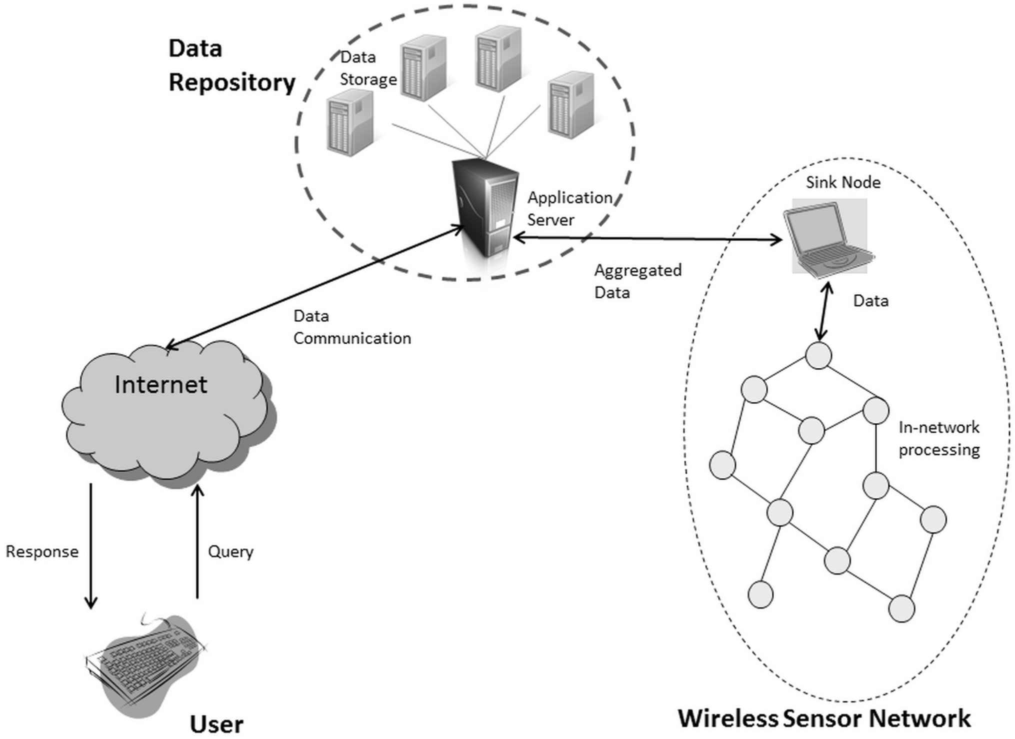
DOI: 10.4018/978-1-4666-4030-6.ch010

a sensor node not only includes volatile memory and processor but also includes non-volatile memory, digital to analog converter, analog to digital converter, universal asynchronous receiver transmitter and interrupt controller interfaces. In addition, low range radio frequency, infra-red and optical communication techniques are used in these nodes. Moreover nodes can sense heat, light, acceleration and chemical contaminants from the environment and can send these information through a wireless communication channel.

WSNs are ad hoc networks that are composed of hundreds to thousands self-organizing sensor nodes. An example WSN is given in Figure 1. Each sensor node may collect information from the sensing area and relay its data to the sink node on a multi-hop path. Sink is a gateway node that collects data from the other nodes located on sensing area and aggregates the delivered data. Sink node may communicate with a repository in order to deliver its collected data. The data repository may store data in various forms in order to give query service to the users through Internet.

WSNs have many application areas in today's world (Garcia-Hernandez, 2007). One of the most important applications is habitat monitoring. In the Great Duck Island (GDI) application, the life cycle of storm petrel birds are monitored by researchers from UCB and Intel (Mainwaring, 2002). In the PODS application (Biagioni, 2002) developed in Hawaii University, some endangered plant species are investigated. ALERT system is developed for the early detection of flood threat by measuring water level, heat and wind power. Another application area of WSN is patient's health monitoring. Schwiebert (2001) developed a system for blind people to sense the objects in their environment. Remote patient monitoring and management of drug usage are the other type of health-based applications (Akyildiz, 2002).

Figure 1. WSN integrated information system example


Data Repository
Data Storage
Application Server
Aggregated Data
Sink Node
Data
Data Communication
Internet
In-network processing
Response
Query
User
Wireless Sensor Network