Chapter 14
Security Challenges in Wireless Sensor Network

Meenakshi Tripathi
Malaviya National Institute of Technology, India

M.S. Gaur
Malaviya National Institute of Technology, India

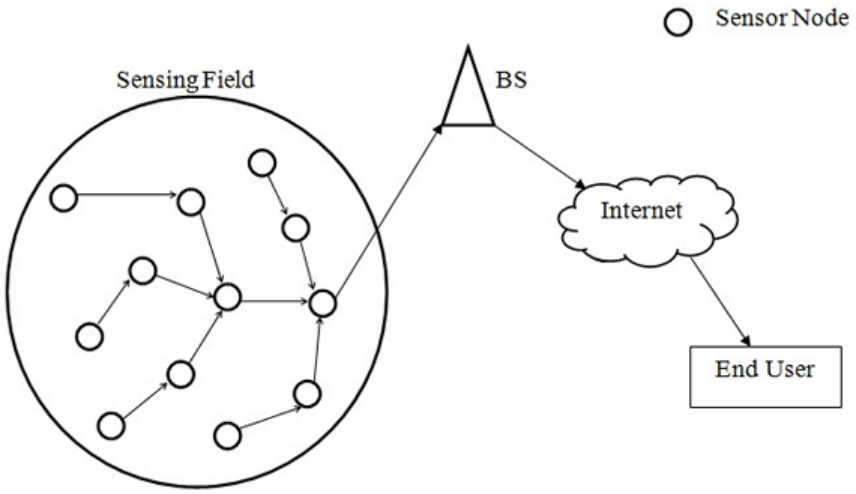
V.Laxmi
Malaviya National Institute of Technology, India

ABSTRACT

Wireless Sensor Networks are a subset of ad hoc networks. Their unique characteristics are smaller node size, high node density, unattended operation in remote areas. Dynamic topology and wireless communication make them vulnerable to numerous types of attacks. In addition to that, memory, processing, and energy constraint make it difficult to incorporate compute-intensive security solutions in these networks. Existing solutions for developing cost and energy efficient algorithms do not fit the security parameters for these resource constrained networks. As a result, these networks remain vulnerable to several types of attacks. This chapter presents a survey of various attacks at the different layers of WSN protocol stack, their detection, and countermeasures. Although every layer of the stack has its own security challenges, the network layer is most vulnerable to many security attacks because it provides an excellent basis for traffic monitoring activities, which helps the attacker form a strategy to perform the attack. The most common attacks on this layer are the Sybil attack, selective forwarding attack, wormhole attack, sinkhole attack, etc. This survey provides a comprehensive view of present attacking strategies to disrupt the normal functioning of WSN.

DOI: 10.4018/978-1-4666-4691-9.ch014

Figure 1. A typical Wireless Sensor Network



INTRODUCTION

In the 1980's when Defense Advanced Research Project Agency (DARPA) started its research on Distributed Sensor Network (DSN), the size of the sensors were large (i.e- shoe-box and up), which limited the potential application of these networks. Further in these DSNs the sensor nodes were using wired connectivity among them. Recent technological advancements have caused a significant shift in WSN (Matin and Islam, 2012; Wang and Balasingam, 2010) and nowadays, sensor nodes are much smaller in size (pack of cards or dust particle), distributed in nature and communicate with each other using wireless medium only. In a typical Wireless Sensor Network, sensor nodes sense the physical phenomenon, compute some result and transfer the result to the base station (BS), which is connected to the end user via internet (Akyildiz, Sankarasubramaniam, & Cayirci, 2002; Ahem, 2004; Elson & Estrin, 200) as shown in Figure 1.

The hardware component of a sensor node include one or more sensors to sense the physical phenomenon (e.g. Light, temperature, pressure, etc.), transceiver for wireless communication, a processing unit to convert sensed data into suitable format for transmission, used to log the sensed data. Batteries act as power source. Figure 2 shows the schematic diagram of a sensor node.

WSN has been viewed as one of the most emerging technology for the 21'st century (Coy et al, 1999). Upcoming companies like Crossbow, Smart Dust Networks, Berkley etc. are also working hard in accelerating the commercialization of WSN by reducing the chip size (Coin size). Figure 3 shows the photographs of some modern sensor nodes.

The sensor node senses the required phenomena and sends the data to the base station or sink by a multihop infrastructure less architecture. The

Figure 2. Schematic diagram of a sensor node