Chapter 12

Security Threats in Wireless Sensor Networks

Alekha Kumar Mishra
VIT University, India

ABSTRACT

Most of the applications of wireless sensor networks have critical tasks to be fulfilled; thus they must be secured. Recent studies focus on securing the communication between sensors and with the base station. An adversary can launch various types of attack on WSN depending on its ability and objective. These attacks can be broadly classified into two categories: 1) layer-dependent, and 2) layer-independent. Layer-dependent attacks are specific to communication protocol layers. They mostly target a node’s functionality such as routing, availability, time synchronization, and data aggregation. Layer-independent attacks are not restricted to any communication protocol layers. These attacks can be launched independent of the communication protocol stack. In this chapter, we study the various attacks possessed by WSN and classify them based on their strength, action, security requirements and impact at different layers of WSN. We define metrics to evaluate the characteristic, behavior, and dependency of these attacks followed a discussion on various countermeasures to defend them.

1. INTRODUCTION

Small size sensors not only ease the process of deployment but also reduce the manufacturing cost and power consumption. That is why, wireless sensor networks (WSN) (Rezazadeh et al., 2012) have become a demanding field of wireless networks. Because of its low-cost sensors and simple deployment process, WSN supports a broad range of applications (Hadjidj et al., 2013). A major group of these applications involves acquiring confidential data from the remote environment. Sensors are often deployed unattended and unsupervised in such environments to reduce the cost of deployment. This allows an adversary to perform malicious activities in the deployed environment. In unattended environments, an adversary can not only physical access or damage the sensor nodes, but also may deploy its own device to participate in network communication. In the latter case, the adversary can monitor network activities access sensed data using its deployed device. In these scenarios, security of the sensor nodes is essential and crucial
design requirements of WSN. Since, sensor nodes have limited computation and communication ability, the standard security mechanisms of wireless ad hoc network are not suitable for WSN. This chapter provides a detailed analysis of security issues and threats of WSN. Since the characteristic of WSN is dissimilar to wireless networks up to a greater extent, we first discuss the security requirements of WSNs.

2. SECURITY REQUIREMENTS IN WSN

In applications, such as military, wild-life monitoring, and traffic monitoring, it is possible to secure the base station (BS). However, the major challenge is to protect the tiny sensors that are deployed either in the enemy territory, open space, or in hazardous areas. Therefore, the sensor nodes and their sensed data must be secured. A number of sophisticated and highly efficient security architectures are available for traditional networks. However, these are unsuitable for WSN due to following reasons. Security in sensor networks is resource constrained and depends on deployment characteristics. Asymmetric key cryptography becomes expensive for sensor networks due to limited energy resources. In this case, symmetric cryptography is a better choice for faster computation. However, symmetric key cryptographic techniques lack versatility compared to their counterparts. Sensor nodes cannot be equipped with tamper-resistant hardware due to low-cost node constraint. Therefore, it is assumed that nodes are also prone to physical attacks. Sensor nodes rely on wireless medium to communicate among themselves. This makes the task of an adversary easier to eavesdrop on network communication. An attacker also can inject malicious information into the wireless network with a little effort.

It is also requires that security mechanism supports large scale networks. Most common security frameworks do not support large number of users. Considering all the above cases, a secured WSN must satisfy the following security requirements (Claycomb & Shin, 2011):

1. Information confidentiality and privacy,
2. Data integrity,
3. Entity authentication,
4. Key distribution and management,
5. Secure routing,
6. Resilience to node capture,
7. Secure data aggregation, and
8. Intrusion detection.

In the following subsections, we discuss the above security requirements in details.

2.1 Information Confidentiality and Privacy

In WSN, it is obvious that an adversary may deploy its sensor nodes to secretly monitor the network activity of either a single node or a group of nodes. Since, the data transmission in sensor networks is done through wireless medium; an adversary may easily use the transmitted data in unanticipated and illegal ways. Therefore, it is required that the privacy of the data is maintained. The security mechanism to achieve confidentiality and privacy in wireless networks are complex and requires enormous computational tasks. Therefore, implementation of these mechanisms may lead to additional overheads. To