Chapter 15
Key Management in WSN Security:
An Attacker's Perspective

Priyanka Ahlawat
National Institute of Technology Kurukshetra, India

Mayank Dave
National Institute of Technology Kurukshetra, India

ABSTRACT

To create a secure communication among the sensor nodes, a key establishment scheme is very important. Wireless sensor networks (WSN) are usually left unattended and thus may attract the adversary to launch several attacks to the network operation. The exposure of the key during a node capture may disturb a large part of network communication. If there is a reliable, efficient, and secure KMS, disruption in the network to such an extent may not occur during a node capture attack. Several researchers have presented several key agreement schemes, but still the area is open to design an efficient attack resistant KMS. Sometimes, during the design of security protocols, the assumptions taken for the adversary behavior in sensor field may not reflect their actual behavior of the adversary in sensor field making these schemes less feasible in many real-world WSN applications. This chapter first discusses the challenges and security requirements, node capture attacks, its impact on the network, and some open issues of KMS solutions to this problem.

1. INTRODUCTION

Wireless sensor networks (WSNs) have emerged as an important class of networks with extensive range of applications. A typical WSN is a collection of very tiny resource inhibited sensors capable of gathering, forwarding it to a central authority for further processing (Neidermeier & Meer 2013, Akyildiz, Su, Sankarasubramaniam & Cayirci 2002) The sensors communicate in an adhoc manner and usually monitor different environmental parameters such as pressure, humidity, optic, acoustic, seismic, acceleration etc. Sensor nodes perform many real time applications such as smart sensing, localization and

DOI: 10.4018/978-1-5225-7335-7.ch015

routing, aggregation of sensed data and synchronization. In order to extend security to WSN services, we need to provide confidentiality, integrity and availability. To ensure peer to peer WSN communication, there is a need to share communication keys among the sensor nodes. Dynamic WSN topology, no fixed infrastructure, limited computational power and memory makes the traditional security solutions unsuitable for WSN (Xiao, Rayi, Sun, Du, Hu & Galloway, 2007). Key management helps in establishing the secure communication among sensor nodes. Deployment in hostile environments makes WSN vulnerable to node capture attacks in which the attacker physically capture the secret keying information.

This chapter aims to provide a comprehensive overview of different KMSs, challenges faced by KMS in WSN, node compromise attacks in WSN and their impact on the security of sensors along with key management solutions and some open issues in this area. This chapter is structured as follows: Related work is presented in Section 2. Section 3 presents various issues of key management in WSN. The problem of node compromise in WSN, its impact on WSN security and different node capture attack models are explored in Section 4. Various key management solutions for node compromise are discussed in section 5. Section 6 presents open ended questions and future challenges in area of KMS based WSN security. Section 7 concludes the chapter.

2. BACKGROUND

WSN is a extremely disseminated and unified network that can be abstracted in to two elements namely sensor nodes and base stations. Sensor nodes get the physical information from surrounding, process it and communicate it using wireless channel. It is a dynamic network of sensor nodes having the limited capabilities of computation to a central authority. A WSN may have huge number of sensor nodes that communicates over a small range of wireless network interface. For economic reasons, sensor nodes are made of highly resource constrained making public-key encryption difficult. The central authority or base station (BS) acts as a entry of forwarding the collected data to some higher authority. Individual sensors communicate locally with neighboring sensors and send readings in peer to peer network to BS. Data packets are broadcast over the air, so an adversary can easily eavesdrops the communication channel. The communication pattern within sensor network has three categories namely node to node communication (aggregation of sensor readings), BS to node communication (specific queries), node to BS (sensor readings) (Simplício, Barreto, Margi & Carvalho 2010). The architecture of WSN is depicted by Figure 1.

The sensors are equipped with three units namely sensing, processing and communication units. The sensing unit is dedicated for sensing the environment data and transfer to processing unit. The processed data is given to BS by communication unit. The sensor nodes are generally placed in a hostile environment so vulnerable to being physically tampered. There is an uncontrollable change in topology due to node failures.

WSN can hierarchical or distributed depending on the role of nodes. In hierarchical, we have BS, cluster head or sensor nodes. The sensor nodes gather the data from surroundings and send to nearest cluster head. The cluster heads have more resources, thus merge the sensor readings. The BS collect the data from cluster head and forwards to other networks. The sensors typically lacks a defined structure and have limited computation power, hence key predistribution seems to be the most preferential for key establishment in sensor nodes. The sensor nodes constraints have a major implications on the design of the security protocols for WSN. Such networks can be categorized in to hierarchical or flat