OSI Layer Wise Security Analysis of Wireless Sensor Network

Shilpi Saha[1], Debnath Bhattacharyya[2], and Tai-hoon Kim[2,*]

[1] Computer Science and Engineering Department
Heritage Institute of Technology
Kolkata, India
shilpisaha7@gmail.com
[2] Department of Multimedia
Hannam University
Daejeon, Korea
debnathb@gmail.com, taihoonn@empal.com

Abstract. The security in wireless sensor networks (WSNs) is a critical issue due to the inherent limitations of computational capacity and power usage. While a variety of security techniques are being developed and a lot of research is going on in security field at a brisk pace but the fields lacks a common integrated platform which provides a comprehensive comparison of the seemingly unconnected but linked issues. In this paper, we have tried to analyze some attacks and their possible countermeasures in OSI layered manner.

Keywords: WSN, security, Sybil, wormhole, spoofing, eavesdropping, selective forwarding.

1 Introduction

Wireless sensor networks (WSN) are quite useful in many applications since they provide a cost effective solution to many real life problems. But it appears that they are more prone to attacks than wired networks. They are susceptible to a variety of attacks, including node capture, physical tampering and denial of service [1]. An attacker can easily eavesdrop on, inject or alter the data transmitted between sensor nodes. Security allows WSNs to be used with confidence and maintains integrity of data. Without security, use of WSN in any application domain would result in undesirable consequences. Particularly in military based projects where a compromise in security can lead to disastrous consequences. Thus security must be addressed in such critical sensor applications. It turns out that providing security in wireless sensor networks is pivotal due to the fact that sensor nodes are inherently limited by resources such as power, bandwidth, computation and storage. Efficiency is thus a crucial issue as sensors are usually deployed in remote area for a long time. Although a lot of progress has been made for the past few years, the field remains fragmented, with contributions scattered over seemingly disjoint yet actually connected areas. As for

[*] Corresponding author.

T.-h. Kim et al. (Eds.): SIP/MulGraB 2010, CCIS 123, pp. 275–282, 2010.

example, key management only makes sure the communicating nodes possess the necessary keys, at the same time protecting the confidentiality, integrity and authenticity of the communicated data. However, it only assures a sense of security in one layer whereas the security of the network can be ruptured in other layers as well like network layer, physical layer, etc.

In this paper, we have explored various security issues of wireless sensor network. Our contribution is therefore to identify and describe the threats and the preferable modes of countermeasures according to the OSI layer.

2 WSN Architecture

In a typical WSN (shown in Fig. 1), we can see the following components:

- Sensor motes (Field devices): Sensor motes are mounted in the process and must be capable of routing packets. In most cases they characterize or control the process or process equipments. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself.
- Gateway or Access points: A gateway enables communication between host application and field devices.
- Network manager: A network manager is responsible for configuration of the network, scheduling communication between devices, management of the routing tables and monitoring and reporting the condition of the network.
- Security manager: The security manager is responsible for the generation, storage and management of keys.

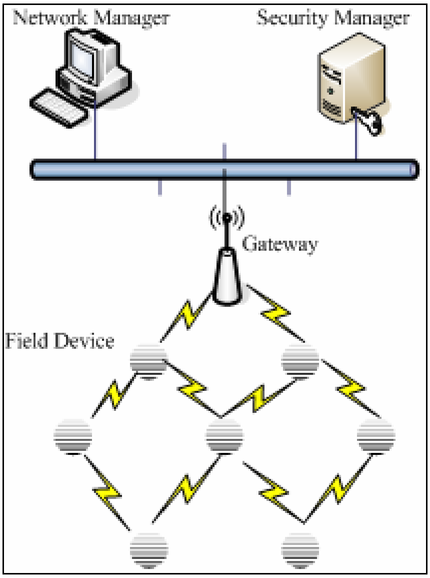

Fig. 1. WSN Architecture