Chapter 24
An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations

M. Yasir Malik
Institute of New Media and Communications, Seoul National University, Korea

ABSTRACT

With the expansion of wireless sensor networks, the need for securing the data flow through these networks is increasing. These sensor networks allow for easy-to-apply and flexible installations, which have enabled them to be used for numerous applications. Due to these properties, they face distinct information security threats. Security of the data flowing through across networks provides the researchers with an interesting and intriguing potential for research. Design of these networks to ensure the protection of data faces the constraints of limited power and processing resources. The author provides the basics of wireless sensor network security in this chapter to help researchers and engineers in better understanding of this applications field. In this chapter, the author provides the basics of information security, with special emphasis on WSNs. The chapter also gives an overview of the information security requirements in these networks. Threats to the security of data in WSNs and some of their counter measures are also presented.

1. INTRODUCTION

Wireless sensor networks (WSNs) attract the attention of researchers and engineers thanks to their vast application scope. These allow for easy and flexible installation of wireless networks composed of large number of nodes. This gives WSN the capability to be used in unimaginable applications. They are finding their usages in habitat monitoring, manufacturing and logistics, environmental observation and forecast systems, military applications, health, home and office applications and a variety of intelligent and smart

DOI: 10.4018/978-1-4666-0101-7.ch024

systems. Multimedia wireless sensor networking is a relatively new branch in this domain, which can process multimedia content i.e. still images, audio and video to name a few.

Such a sensor network is typically composed of hundreds, and sometimes thousands of nodes. These nodes are capable of receiving, processing and transmitting information, as based on the assigned tasks. Information flowing through WSN may be susceptible to eavesdropping, retransmit previous packets, injection of redundant or causeless bits in packets and many other threats of diverse nature. To ensure that the data being received and transmitted across these networks is secure and protected, information security plays a vital role.

As contrary to the Moore's law, there has been not much development in the hardware capacity and computational capabilities of the sensors being deployed in wireless sensor networks. These networks are kept inexpensive, thus introducing many constraints in the performance parameters. Low cost sensors incorporate shortcomings in their storage capacity, power requirements and processing speed. This poses a unique dilemma for researchers as they have to design efficient and distinct information security schemes which work seamlessly with the resource constrained sensor networks.

Sensors in the network are mostly exposed to open environment as they have to interact with either other sensors or human beings. Physical security of these sensors is always vulnerable and thus poses an unprecedented threat to the overall security of the network. Advances in power analysis and time based attacks enable the malicious entities to perform various hazardous activities.

Wireless channels are still considered unreliable and the same is the case with wireless sensor networks, which may contain a very large number of nodes and sinks, thus giving rise to concerns about the validity of the communications in the network. Trust models for the nodes have to be developed to make sure that all the nodes taking part in the communications are trustworthy.

All these unique features of wireless sensor networks changes the way we look at their security. These networks face different kinds of threats from those of computer, wired, network or even the high-bandwidth wireless models. Thus, these intimidations are coped in distinctive manners.

This chapter will be beneficial in equipping the readers with the basic concepts of security and WSN security. Readers will be able to realize the strengths and weaknesses of WSN with respect to security. Some of the famous and latest attacks and their countermeasures will help in better understanding of the threats and our capabilities to cope with them. Readers with lesser or no prior knowledge of information security will be able to understand this chapter, because basic concepts needed for better apprehension of security issues will be defined.

We are hopeful that the basics provided in this chapter will help the readers to grasp the fundamental concepts of Wireless Sensor Network Security (WSNS), which will empower them to embark on their journey to further explore this ever-expanding field and to find new problems and their solutions in this interesting research and applications field.

General characteristics of WSN are presents in Section 2 of the chapter. These are the properties of these networks which make them the preferred solution in many applications, though they also present limitations on the viable solutions to the security issues in WSN. These attributes are studied with an emphasis on their importance in the security of WSN.

For reliable and secure communications in WSNs, there are some security qualifications that must be fulfilled. These security requirements are given in Section 3.

Threats in WSN are of diverse natures and kinds. Some of the important threats will be discussed in section 4 of this chapter. Counter-