Chapter 6

Sensors Network: In Regard with the Security Aspect and Counter Measures

Mamta Bachani
Mehran University of Engineering and Technology, Pakistan

Ahsan Memon
Mehran University of Engineering and Technology, Pakistan

Faisal Karim Shaikh
Mehran University of Engineering and Technology, Pakistan & Umm Al-Qura University, Saudi Arabia

ABSTRACT

This chapter aims to develop an understanding of sensor networks and the security threats posed to them, owing to the inherently insecure wireless nature. It also highlights the current security issues associated with the exchange of information and presents respective countermeasures that can be used to secure the network of malevolent behavior. It builds the reader’s understanding of security threats by presenting an idealistic security mechanism and comparing it to currently practiced security mechanisms. Doing so, it identifies the security flaws in each mechanism, henceforth, enumerating a list of well-known security attacks that are connected to the respective security flaws. To provide a better understanding of security threats, the security attacks, in general, are discussed in the perspective of a network administrator, and an adversary. Their impact is also considered from the side of a network administrator and its respective benefits to the adversary. The chapter is later concluded along with future directives and an insight on requirements of forthcoming technologies.

INTRODUCTION

This chapter aims to construct a fundamental understanding of sensors, the respective wireless sensor networks formed with these sensors and the security concerns that arise from such networks along with the classical countermeasures that can be put into effect to detect, prevent and counter the security

DOI: 10.4018/978-1-4666-8761-5.ch006
Sensors Network

The text in this chapter is hence, mainly consistent of: 1) Sensors, 2) Security Attacks and 3) Respective countermeasures. We begin the chapter with the introduction to the scenario which we will be using to construct viability for the aim of Chapter.

Sensors have had great impact on our everyday lifestyle with the list of implementations from personal gadgets to commercial applications. When in swarms, sensors have demonstrated even better results and displayed tremendous potential of monitoring and analyzing an area under surveillance especially when the networks of wireless nodes are formulated to being. Such wireless networks are broadly categorized under the umbrella of Wireless Networks However, we will be discussing a subset of this category, named Wireless Sensor Networks (WSNs) that consist of battery powered sensing nodes comprised deployed in an environment to perform a task mainly relating to surveillance. While wireless medium presents many advantages over wired medium, its wireless nature inherently offers challenges to the security of transmitted data. The increased use of wireless channels increases the risk of being spoofed and attacked by an introduction of a third person who can easily overhear the wireless traffic if it is not adequately protected. It poses a considerable threat to the flow of information. This threat evolves a possibility of corruption of authentication, integrity and privacy. The main aim of this chapter is make the reader aware of the sensor network security and its usage in modern technology. Also to highlight the current security issues associated with the sensors installment and the transfer of data among multiple nodes in a network. We discuss some of the techniques that can be used to overcome these issues and provide secure ways that can be used for exchange of information throughout the sensor network.

Researchers from around the world have used wireless sensor networks in various sets of applications. Some of the commercial applications include smart parking (S. Lee, D. Yoon & A. Ghosh, 2008), security of intracar (K. P. Shih, S. S. Wang, H. C. Chen & P. H. Yang, 2008), event detection (E. Hussain, G. Chow, V. C. M. Leung, R. D. McLeod, J. Misic, V. W. S. Wong & O. Yang, 2010), health monitoring (R. Tan, G. Xing, J. Wang, & H. C. So, 2008), vehicle telematics (G. Y. Ming & J. Rencheng, 2008) etc. Environmental applications such as greenhouse monitoring (J. F. Martinez, M. S. I. Familiar, Corredor, A. B. Garcia, S. Bravo & L. Lopez, 2011), habitat surveillance (Q. Wang, S. Zhang, Y. Yang & L. Tang, 2011) and variety of applications in military (L. Cao, J. Tian, & Y. Liu, 2008) and industries (N. Alsharabi, L. R. Fa, F. Zing & M. Ghurab, 2008). Most of the applications are based on wireless networks or at least, tend to be wireless due to the easier deployment and cost effectiveness. With regards to some of these applications, later in this chapter, we analyze the security threats and then discuss relevant counter measures.

We also focus on the security challenges posed to the transfer of information in a Wireless Sensor Networks (WSNs). We notice that there are number of routing protocols designed to serve the application goals like sensing data in a particular fashion and triggering events on specified conditions. In addition to which, the routing protocols serve the general requirements of keeping the application low cost and low power consuming, but few of the applications regard security as its major requirement. The advancements in the field WSN are also leading to insecurity with conventional techniques, as there are powerful decoders available to flaw security of such networks. Nonetheless, in majority of the applications, security is handled by key cryptography, which provides security to the network but is expensive in terms of processing and power constraint and can be cracked (Karlof, 2003). Based on the network description provided in the preceding text, we try to develop an understanding about the security concerns in a WSN. A background summary of the mentioned network is illustrated in the following network assumptions.