Chapter 7.6
Security and Attacks in Wireless Sensor Networks

Murat Al
University of Arkansas at Little Rock, USA

Kenji Yoshigoe
University of Arkansas at Little Rock, USA

ABSTRACT

Understanding data security is crucial to the daily operation of Wireless Sensor Networks (WSNs) as well as to the further advancement of security solutions in the research community. Unlike many surveys in literature that handle the topic in close relationship to a particular communication protocol, we provide a general view of vulnerabilities, attacks, and countermeasures in WSNs, enabling a broader audience to benefit from the presented material. We compare salient characteristics and applications of common wireless technologies to those of WSNs. As the main focus of the chapter, we thoroughly describe the characteristics of attacks and their countermeasures in WSNs. In addition, we qualitatively illustrate the multi-dimensional relationship among various properties including the effectiveness of these attacks (i.e., caused damage), the resources needed by adversaries to accomplish their intended attacks (i.e., consumed energy and time), and the resources required to defend against these attacks (i.e., energy overhead).

INTRODUCTION

First version of the current generation sensor devices was introduced in mid 1990s with Wireless Integrated Network Sensors (WINS) at the University of California, Los Angeles UCLA). As computation power, communication range, and lifetime of the devices have increased, the node sizes have significantly decreased. These changes have led to better performance of WSN devices resulting in better performance of existing applications as well as possible exploration of new application areas. In 2003, MIT's Technology Review had included Wireless Sensor Network (WSN) technology in its annual list of the ten most important technologies that will change the world

DOI: 10.4018/978-1-61350-101-6.ch706

(Huang, 2003). With new application areas and developments in wireless technologies, WSNs will gain more popularity and take more roles in our everyday lives.

WSNs are often deployed in areas where constant power is not available and recharging of batteries is not an option. Hence, the most important design aspect of a sensor network is its energy efficient operation to provide a long network lifetime. At present, with a pair of AA batteries a sensor node can operate several years. This comes at the cost of very constrained resources. Protocol designs in WSNs have to consider many constraints of the sensing devices such as limited battery power, memory size, and computing capacity. This makes a WSN more vulnerable to attacks than a wired or less energy constraint wireless network such as a Wireless Local Area Network (WLAN) or a Mobile Ad-hoc Network (MANET). On the other hand, the ever-increasing computational power of personal computers and laptops along with better performing decryption algorithms pose greater threats to wireless communication. For instance, various sniffing and wireless key hacking software is freely available on the Internet.

The objective of this book chapter is to make practical information on security in resource constrained wireless sensor networks available to a wide audience, ranging from practitioners to academic researchers. We explain security associated terms with respect to WSNs and present security relevant services. As the focus of the chapter, we thoroughly describe the characteristics of attacks and their countermeasures in WSNs. We qualitatively analyze and illustrate the multi-dimensional relationship of the discussed attacks. This allows a simplified comparison of relevant properties such as the effectiveness of a particular attack, the resources needed by the adversary to mount it, and the cost for the network to counter this attack.

BACKGROUND

Common Wireless Technologies and Their Typical Characteristics

This section provides an overview of common wireless technologies with their typical characteristics for a quick comparison. It does not attempt to cover all aspects of wireless technologies, nor does it give an exhaustive list of devices, protocols and applications that can be used with a particular wireless technology. Rather it helps broach the subject of wireless sensor networks by comparing it to prevalent technologies, such as WLAN and MANET.

Table 1 lists general properties of WLANs, MANETs, and WSNs for a comparison. WLANs and MANETs have many properties in common; hence, they are listed together in one column.

For the sake of completeness, we will briefly describe Wireless Mesh Networks (WMNs) that can be implemented using one or a combination of various technologies such as IEEE 802.11 (Wireless Local Area Network), 802.15 (Wireless Personal Area Network), 802.16 (Wireless Metropolitan Area Networks, also called WiMAX), cellular networks such as GSM (Global System for Mobile Communications) or CDMA (Code Division Multiple Access). Network components usually include end nodes or mesh clients, routers, and gateways. If the same type of hardware is used, mesh clients can be configured to act as routers or end nodes. Routers and gateways serve as access points for end nodes to the network, whereas the gateway additionally is a bridge between the mesh network and an external network such as the Internet. While in traditional networks the small number of access points or hotspots needs a wired connection to an external network, in a wireless mesh network access points themselves are wirelessly connected to each other forming a mesh. The advantages of WMNs include