Chapter 2
Wireless Sensor Network Security Attacks: A Survey

Dennis P. Mirante
Hofstra University, USA

Habib M. Ammari
University of Michigan – Dearborn, USA

ABSTRACT

Wireless Sensor Networks (WSNs) are a rapidly growing area for research and commercial development. Originally used in military applications, their commercialization offers potential low cost solutions for real-world monitoring and process control. Since they may be deployed in hostile, unattended, environments and may collect sensitive data, they may be prone to attack by entities that wish to interfere with their operation and/or usurp or alter the information they collect. While their low cost enhances their desirability as a monitoring solution, it also presents inherent resource and computing constraints. These constraints are major obstacles for the implementation of traditional security paradigms. Consequently, one of the most active areas of research in Wireless Sensor Networks is security. This chapter takes a representative survey of the types of security attacks WSNs may be subjected to. Additionally, steps that may be taken to mitigate these attacks are also discussed. Intrusion Detection Systems, a paradigm for monitoring network activities for malicious behavior, are introduced, and specific examples of them are discussed.

INTRODUCTION

Security in Wireless Sensor Networks (WSNs) presents a challenging problem. In military applications, such as battlefield surveillance, networks are typically injected into hostile environments. Applications of this type require that an adversary's ability to determine and interfere with the extent and type of monitoring must be minimized. In this case, it is obvious that security is paramount. Security may also be required in environments where physical threats do not exist, i.e., in the healthcare industry, where access to patient information obtained during health monitoring must be restricted

DOI: 10.4018/978-1-4666-4707-7.ch002

and safeguarded. WSNs may also be deployed in applications where physical protection is lacking, such as traffic control, electrical power generation and distribution, and factory infrastructure and process management. Depending on the specific application at hand, such networks require security to preclude anarchists or terrorists from causing mayhem, competitors from obtaining knowledge of secret product formulations, competitors from disrupting product manufacture or surreptitiously introducing faults into products. As WSNs become increasingly assimilated into modern society, new types of applications will surface, each with their attendant security problems and requirements.

Security issues in WSNs are exacerbated by the constraints imposed on each individual node's resources. Available battery power (or energy), memory, and computational speed are limited. Hence, complex data processing and data encryption requiring significant processing power are not typically employed. In applications where data confidentiality is paramount, data encryption may be performed by special purpose hardware, designed to consume minimal energy. Such hardware may significantly increase the cost of each sensor node. Additionally, the increased energy consumption, despite being minimized, reduces the node's longevity. The tradeoff between performance, longevity, and security, must be carefully weighed by the network designer.

The objective of this chapter is to study the types of security attacks WSNs may be subjected to and the methodologies that may be employed to mitigate them. Most existing security research in the WSN arena has dealt with the prevention of particular types of classic attacks, such as Denial of Service (DoS), wormhole, Byzantine, injected false data, man-in-the-middle, replay, to name a few. This chapter surveys the latest literature concerning these attacks, and discusses the means by which these attacks, or hybrids of them, may be prevented. When pertinent, the attacks will be discussed relative to the communication layer in the Internet Model at which the attack takes place. For instance, DoS attacks may occur at the Physical Layer when RF (radio frequency) jamming is employed against a WSN containing non-frequency agile sensor nodes. Alternatively, the attack may take place at the Data Link Layer, when an attacker induces collisions by initiating a transmission of a bogus packet after detecting that a node has begun sending valid data. On detection of the collision, the node sending the valid data will typically execute a random back-off algorithm, then attempt to retransmit its data. The random back-off algorithm will have no effect on the attacker, who will continue to induce collisions. Ultimately, the battery power of the legitimate sensor node is not conserved and will be reduced to the point of failure.

The introduction of new types of WSN applications will result in new types of security attacks. It is impossible to know or predict the characteristics of these future attacks. As a result, it would seem that WSN researchers and designers will always be playing catch up in their attempts to find and plug the latest security holes used by attackers. New research into the area of cooperative intrusion detection indicates that generic algorithms for the detection of aberrant nodes may be definable. In some cases, the use of these algorithms may allow researchers and designers to dispense with having to find a specific solution to each new attack type. Using these algorithms, an attack may be detected and the sensors and operator may be alerted. Attacking nodes may then be identified and isolated from the WSN by such an Intrusion Detection System (IDS). Additionally, this chapter discusses intrusion detection and presents examples of past and current work in this area.

CHARACTERISTICS OF WIRELESS SENSOR NETWORKS AFFECTING SECURITY

The driving force behind sensor node construction is cost. Node designers strive to limit sensor node