Chapter XXXV
Security and Privacy in Wireless Sensor Networks:
Challenges and Solutions

Mohamed Hamdi
University of November 7th at Carthage, Tunisia

Noreddine Boudriga
University of November 7th at Carthage, Tunisia

ABSTRACT

The applications of wireless sensor networks (WSNs) are continuously expanding. Recently, consistent research and development activities have been associated to this field. Security ranks at the top of the issues that should be discussed when deploying a WSN. This is basically due to the fact that WSNs are, by nature, mission-critical. Their applications mainly include battlefield control, emergency response (when a natural disaster occurs), and healthcare. This chapter reviews recent research results in the field of WSN security.

INTRODUCTION

The applications of wireless sensor networks (WSNs), which cover both the civil and military contexts, are continuously expanding. The ability to develop miniaturized, battery powered motes that combine sensing, correlation, fusion, and wireless communication capabilities makes the WSN technology cost-effective for being used in future. In fact, WSNs can be used to gather and analyze information about vehicular movement, humidity, temperature, pressure, as well as many other parameters.

However, the enormous potential of WSNs can be unlocked only if the corresponding infrastructures are adequately safeguarded. In fact, violating one or more security properties would lead to wrong decisions, and consequently wrong reactions. Hence, security should rank at the top of the issues that should be discussed when designing a WSN. Another motivation is that WSNs are, by nature, mission-critical, meaning that they are developed for sensitive tasks where error-tolerance is very small. The importance of security in the WSN context is exacerbated by certain factors including the following:

- Sensor nodes have limited storage, computation, and power resources. For this reason, security mechanisms should be adapted to the WSN capabilities.
- The network does not have a static infrastructure. WSN architectures can be only timely defined. This renders the application of existing robust cryptographic mechanisms (e.g., public key infrastructure [PKI], digital signature) more difficult than in customary networks.
- The sensing and communication tasks are often performed in a hostile environment where the gathered events are subjected to numerous threats that might affect the final decision.
- The detected events are forwarded through the sensor nodes themselves, preventing the application of strong communication security mechanisms.

This chapter surveys recent research activities in the area of WSN security. More accurately, the following aspects will be discussed:

1. **Wireless sensor networks:** This section addresses several WSN basic issues to highlight the related scientific challenges. Components, architecture, topology, routing, mobile target tracking, and alert management will be, among others, discussed.
2. **WSN security objectives:** Traditional security goals (i.e., confidentiality, authenticity, integrity, and availability) should be extended to fit the requirements of WSNs. Several particular concepts are introduced at this level. For instance, confidentiality, authenticity, and integrity, which have been customarily associated to data and node identity, should be extended to cover node location. This poses several new security challenges in the WSN context.
3. **Attacks against WSNs:** This section describes the most important attacks techniques concerning WSNs. Attacks are classified according to the basic security properties they violate. A taxonomy of these attacks will also be proposed. This taxonomy is based on three major attack activities: (1) attacks on transmitted information, (2) attacks on architecture, structure, protocols, and (3) attacks on the localization framework.
4. **Countermeasures:** Potential security solutions that allow countering the aforementioned threats will be proposed. They will be classified according to the level at which they act (e.g., link level, routing, and application). Countermeasures will be also categorized into preventive and reactive solutions. For example, robust localization (resp. fault-tolerance) schemes belong to the first (resp. second) category.
5. **Building security policies for WSNs:** Several key security processes, such as monitoring and incident response, can not be directly applied in the WSN field. They should therefore be heavily adapted in order to support WSN specific constraints.

WIRELESS SENSOR NETWORKS

Due to advances in wireless communications and electronics over the last few years, the development of networks of low-cost, low-power, multifunctional sensors has received increasing attention. These sensors are small in size and able to sense, process data, and communicate with each other, typically over an radio frequency (RF) channel. A sensor network is designed to detect events or phenomena, collect and process data, and transmit sensed information to interested users. Basic features of sensor networks are:

- Self-organizing capabilities
- Short-range broadcast communication and multihop routing
- Dense deployment and cooperative effort of sensor nodes
- Frequently changing topology due to fading and node failures
- Limitations in energy, transmit power, memory, and computing power