Chapter XXXIV
Security in Wireless Sensor Networks

Luis E. Palafox
CICESE Research Center, Mexico

J. Antonio Garcia-Macias
CICESE Research Center, Mexico

ABSTRACT

In this chapter we present the growing challenges related to security in wireless sensor networks. We show possible attack scenarios and evidence the easiness of perpetrating several types of attacks due to the extreme resource limitations that wireless sensor networks are subjected to. Nevertheless, we show that security is a feasible goal in this resource-limited environment; to prove that security is possible we survey several proposed sensor network security protocols targeted to different layers in the protocol stack. The work surveyed in this chapter enable several protection mechanisms vs. well documented network attacks. Finally, we summarize the work that has been done in the area and present a series of ongoing challenges for future work.

INTRODUCTION

Recently, wireless sensor networks (WSN) have gained great popularity, mainly because they provide a low cost alternative to solving a great variety of real-world problems (Akyildiz, Su, & Sankarasubramaniam, 2003). Their low cost enableds the deployment of large amounts of sensor nodes (in the order of thousands, and in the future perhaps millions), which most of the time operate under harsh environments. WSN present extreme resource limitations, mainly in available memory space and energy source. Both limitations represent great obstacles for the integration of traditional security techniques. The highly unreliable communication channels that are used in WSN and the fact that they operate unattended make the integration of security techniques even harder.

Wireless sensor networks today offer the processing capabilities of computers of a few decades ago and the industry's trend is to reduce the cost of wireless sensing nodes while maintaining the

same processing power. Based on this idea, many researchers have started to face the challenge of maximizing processing capabilities and reducing energy consumption while protecting sensor networks from possible attacks.

BACKGROUND

WSN have many more limitations than other traditional computer networks. Due to these limitations, it is unfeasible to use the traditional security approaches in these resource-constrained networks. Thus, to develop efficient security techniques, it is imperative to consider the limitations involved.

Extremely Limited Resources

Every security mechanism requires a certain amount of resources for its implementation, these resources include data memory, program memory, and energy source to power the sensor node; however, these resources are very scarce in sensor nodes.

- Memory limitations. In order to implement an efficient security mechanism, the algorithm used for such implementation must have a small footprint.
- Energy limitations. When including security mechanisms, careful attention should be paid to energy-depleting factors including the consumed energy in computation of the security functions (i.e., encrypt, decrypt, data signatures, signature verification), the consumed energy of additional security related data transmissions or overhead (i.e., initialization vectors required for encrypt/decrypt), and the energy spent in storing the security related parameters (i.e., cryptographic keys).

Highly Unreliable Communication Medium

Unreliable communication is another threat to WSN. The security relies heavily on a defined protocol, which depends on communication.

- Unreliable transfers. The packets can be corrupted or even discarded due to errors in the communication channel or to congested nodes which results in packet loss; as a consequence, application developers are forced to allocate extra resources for error handling. Most importantly is the fact that if a protocol does not have the appropriate mechanisms for error handling, packets including critical security information could be lost (e.g., a cryptographic key).
- Conflicts. Even if we had a reliable communication channel, the communication still could be unreliable due to the broadcast nature of sensor networks. If a collision occurs in the middle of a transfer, there would be conflicts and the transfer itself would fail. On a highly populated network this can be a big problem, as has already been pointed out (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002).
- Latency. Multihop routing, network congestion, and in-network processing can introduce latency to the network, making synchronization difficult between nodes. Synchronization problems can be critical for network security mechanisms that rely on error reporting and cryptographic key distribution. Some real/time communications techniques could be used in WSN (Stankovic, Abdelzaher, Lu, Sha, & Hou, 2003).

Unattended Operation

On most wireless sensor network applications, nodes are left unattended for long time periods. The three main disadvantages of leaving the network unattended are:

- Exposure to physical attacks. The network can be deployed in an environment open to adversaries, in undesirable climatologic conditions, and so forth. Thus, the probability of a node suffering a physical attack is much higher than in typical computers on traditional networks, which normally are placed on a secure location and only face attacks through the network.