Chapter 22
Applied Cryptography in Wireless Sensor Networks

Dulal C. Kar
Texas A&M University-Corpus Christi, USA

Hung Ngo
Texas A&M University-Corpus Christi, USA

Clifton J. Mulkey
Texas A&M University-Corpus Christi, USA

ABSTRACT

It is challenging to secure a wireless sensor network (WSN) because of its use of inexpensive sensor nodes of very limited processing capability, memory capacity, and battery life that preclude using traditional security solutions. Due to perceived excessive computational and architectural overhead, public key algorithms are altogether avoided for WSNs. Currently security in WSNs is provided using only symmetric key cryptography, but it requires keys to be embedded in sensor nodes before deployment and the entire network has to go through a key establishment phase after deployment. Accordingly, in this chapter, we summarize, discuss, and evaluate recent results reported in literature on sensor network security protocols such as for key establishment, random key pre-distribution, data confidentiality, and broadcast authentication. In addition, we discuss promising research results in public key cryptography for WSNs, particularly related to elliptic curve cryptography and its application for identity based encryption.

INTRODUCTION

A wireless sensor network consists of sensor nodes that communicate wirelessly using multi-hop network. Sensor nodes are typically deployed in an area to collect data as well as monitor and control activities. Specific applications of wireless sensor networks include wildlife monitoring, seismic activity monitoring, volcanic activity monitoring, target tracking, battlefield reconnaissance and surveillance, and emergency rescue operations (Akyildiz, Sankarasubramaniam, & Cayirci, 2002). It is envisioned that wireless sensor networks will be ubiquitous in every day aspects of our life and even be integrated to and accessible from the Internet.

DOI: 10.4018/978-1-4666-2919-6.ch022

A wireless sensor is a simple data sensing, computing, and communicating device which is designed to be powered by battery. As such, it has very limited memory capacity and processing and communicating capabilities. Because of their simple architecture, wireless sensor nodes are inexpensive and can be deployed in large numbers cost-effectively in many situations. As for operation of a simple wireless sensor network, all sensor nodes communicate with their neighbors and a base station. A base station is a relatively powerful computing and communicating node which often acts as a gateway or a storehouse of collected data. Figure 1 shows a typical configuration of a sensor network. However, it is possible to have a complex communicating configuration of a network with multiple base stations and multiple levels of communications among the sensor nodes.

Security of a wireless sensor network is crucial as it is typically deployed in an accessible area where there is no physical security thus making it very vulnerable for easy attacks (Huang, Cukier, Kobayashi, Liu, & Zhang, 2003; Perrig, Szewczyk, Tygar, Wen, & Culler, 2002; Zhu, Setia, & Jajodia, 2006). It is very challenging to secure a wireless sensor network mainly due to its resource-constrained sensor nodes which cannot run the conventional cryptographic algorithms or protocols that are being used to guarantee security of traditional network communications. *Data aggregation* (ability to aggregate reported values from other nodes) and *passive participation* (ability to not send overhead values) are also the crucial issues for sensor network security. Often implementing security on resource-starved sensor devices imposes extra computational and communication overhead that can be viewed excessive in some applications. This is due to the fact that a security application has to compete for resources with the main application. As such, a lightweight yet effective security solution is sought for wireless sensor networks. Fortunately, recent research on security of wireless sensor networks has produced many promising results. For example, two symmetric key algorithms, Skipjack and RC5 are found to be very suitable for resource constrained wireless sensor networks. Similarly, elliptic curve based public key cryptosystems (e.g., identity based encryption) are found to be very promising for wireless sensor networks. A good number of security schemes of significant performance using Skipjack, RC5, Elliptic Curve Cryptography (ECC), and Identity Based Encryption (IBE) for sensor network applications have been proposed in literature particularly with some pioneering contributions in the areas of key distribution, key management, and authentication. In this chapter, we discuss the results of these key and pioneering contributions of the contemporary research in applied cryptography for wireless sensor networks and illustrate their operations, scopes, and limitations for wireless sensor networks.

In the following, we describe and analyze security protocols for key establishment, key distribution, confidentiality, authentication, and

Figure 1. A typical sensor network