Chapter 7.3
Applied Cryptography for Security and Privacy in Wireless Sensor Networks

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

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

Geetha Sanapala
Texas A&M University-Corpus Christi, USA

ABSTRACT

It is challenging to secure a wireless sensor network (WSN) because its inexpensive, tiny sensor nodes do not have the necessary processing capability, memory capacity, and battery life to take advantage of the existing security solutions for traditional networks. Existing security solutions for wireless sensor networks are mostly based on symmetric key cryptography with the assumption that sensor nodes are embedded with secret, temporary startup keys before deployment thus avoiding any use of computationally demanding public key algorithms altogether. However, symmetric key cryptography alone cannot satisfactorily provide all security needs for wireless sensor networks. It is still problematic to replenish an operational wireless sensor network with new sensor nodes securely. Current research on public key cryptography for WSNs shows some promising results, particularly in the use of elliptic curve cryptography and identity based encryption for WSNs. Although security is essential for WSNs, it can complicate some crucial operations of a WSN like data aggregation or in-network data processing that can be affected by a particular security protocol. Accordingly, in this paper, we summarize, discuss, and evaluate recent symmetric key based results reported in literature on sensor network security protocols such as for key establishment, random key predistribution, data confidentiality, data integrity, and broadcast authentication as well as expose limitations and issues related to those solutions for WSNs. We also present significant advancement in public key cryptography for WSNs with promising results from elliptic curve cryptography and identity based encryption as well as their limitations for WSNs.

INTRODUCTION

Significant advancements in hardware technology have propelled the existence of Wireless Sensor Network (WSN). A WSN consists of simple, low cost yet powerful sensors. Each sensor has the ability to sense, process, and communicate data collected from the environment, in which it is deployed.

Sensors usually draw energy from a small battery, and thus energy efficiency emerges as the key issue in any WSN. The basic idea of a WSN is to employ a large number of sensors to collectively monitor and disseminate information about a phenomenon of interest. WSNs have been designed to support a diverse range of applications. Some examples include military surveillance, habitat and weather monitoring, agricultural crop management, wildlife monitoring, target tracking, emergency rescue operations (Akyildiz, Su, Sankarasubram -aniam, & Cayirci, 2002), biosensors for health monitoring, etc. It is believed that WSNs will drastically change our lives. Not surprisingly, there is also an existing trend about integrating WSNs to the Internet (Su, & Almaharmeh, 2008).

The typical architecture of a wireless sensor node contains a sensing unit, a processing unit, a transceiver unit, a power unit, and an optional mobilizer, location finding system. The processing unit may contain a small memory unit. In addition to sensor nodes, the network may also contain a sink or base station. A sink is a node with relatively powerful communication and computation ability. It generally serves as a gateway in the network. Different kinds of communication patterns are possible between the sink and sensor nodes (Demirkol, Ersoy, & Alagoz, 2006). However, the most common type of communication is convergecast, in which, a group of sensors communicate to a sink.

The security aspect of WSNs is very crucial and is the main focus of this paper. Security in WSNs is associated with a unique set of challenges for several reasons. Firstly, since the network is usually deployed in a hostile unattended environment, there is no physical security for the network thereby exposing it to easy attacks (Huang, Cukier, Kobayashi, Liu, & Zhang, 2003; Perrig, Szewczyk, Tygar, Wen, & Culler, 2002; Zhu, Setia, & Jajodia, 2006). Secondly, sensors are severely resource constrained. Therefore, existing security solutions are impractical and need be revised to accommodate the inherent resource constraints of WSNs. Finally, there is no trustable entity in a WSN unlike in a wired network where nodes rely on a trusted authority to securely communicate with other nodes.

Data aggregation and **passive participation** are two widely used techniques in WSN that are closely intertwined with security. Data aggregation is a method of modifying data as it flows through the network, to increase energy efficiency of the network. If encrypted data is being transmitted, the aggregating nodes must be able to access decrypted data to be able to perform aggregation. Similarly, in passive participation, a node that overhears another node transmitting the same value can choose not to transmit it. Passive participants should be able to decrypt data transmitted by neighbors, which means that the data should be encrypted with a locally shared key. However, implementing security measures on resource constrained sensor devices will further add to computation and communication overhead.

Much work has been going on in the field of security for WSNs. Cryptographic techniques such as Skipjack, RC5, Elliptic Curve Cryptography (ECC) and Identity Based Encryption (IBE) are found to be very promising for WSNs. This paper provides a comprehensive survey of these key contributions of research in applied cryptography and discusses their operations, applications, scopes, and limitations in WSNs. Some existing security protocols for WSNs and their limitations are also presented in this paper.