Chapter 18
Modeling a Secure Sensor Network Using an Extended Elementary Object System

Vineela Devarashetty
University of Illinois at Chicago, USA

Jeffrey J. P. Tsai
University of Illinois at Chicago, USA

Lu Ma
University of Illinois at Chicago, USA

Du Zhang
California State University at Sacramento, USA

ABSTRACT

A sensor network consists of a large number of sensor nodes, which are spread over a geographical area. Sensor networks have found their way into many applications, from military domains to traffic or environmental monitoring, and as sensor networks reach toward wide spread deployment, security becomes a major concern. In this regard, one needs to be sure about the confidentiality, authenticity and tamper-proof of data. The research thus far has focused on how to deploy sensor networks so that they can work efficiently; however, the focus of this paper is on sensor networks' security issues. In this paper, the authors propose a formal model to design and analyze the secure sensor network system. The model is based on an augmented Petri net formalism called Extended Elementary Object System. This proposed secure sensor network model has a multi-layered structure consisting of sink node layer, sensor node layer and security mechanism layer. At the security mechanism layer, a synchronous firing mechanism is utilized as a security measure to detect malicious node attacks to sensor data and information flow. In addition, the model applies SNEP protocol for authentication and confidentiality of sensor data.

DOI: 10.4018/978-1-4666-1743-8.ch018

1. INTRODUCTION

Recent advances in wireless communications and mobile computing have enabled the development of low cost, low power, and multifunctional sensor nodes that are small in size and communicate un-tethered short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, form sensor networks (Akyldiz et al., 2002; Levis et al., 2005; Lewis, 2004; Romer & Mattern, 2004). A sensor network can provide access to information anytime, anywhere by collecting, processing, analyzing and disseminating data. Each sensor has wireless communication capability and intelligence for signal processing and data communicating. The positions of sensor nodes can be randomly deployed which implies that the sensor networks are self-organized. They can be easily deployed because no human intervention or infrastructure is needed. Hence, sensor networks can help pave the way for autonomic computing (Wang, 2007).

Although much research has thus far focused on making sensor networks feasible and useful, security has been receiving increasing attention (Karlof & Wagner, 2003; Perrig et al., 2002; Walters et al., 2007). As sensor networks reach towards wide spread deployment in different application domains, security issues become a central concern. Power and computation constraints are often high on the agenda in sensor networks, relegating security requirements to a lesser place. Given the fact that there has not been much attention on formal modeling and analysis of the security aspects in sensor networks and that little prior work exists in this area, we recognize the need to identify potential problems and challenges in the sensor network's security and propose solution techniques.

Before delving into the specifics in sensor network security, we first examine the security requirements for a sensor network. They include:

- Data Authenticity
- Data Confidentiality
- Data Integrity
- Data Freshness

Data Authenticity: Data authenticity in general is the requirement that the sender is a valid one and not a bogus one. Data authenticity serves as a prerequisite to access the data. It requires verifying the sender. In sensor networks, data authentication requires a message recipient to verify the identity of the message source to ensure the truthfulness of data origin. It requires a party to prove its identity. Ensuring data authenticity provides protection against forgery or masquerade and prevents injecting bogus messages.

Data Confidentiality: Data confidentiality in general is the requirement to make sure that data can be accessible only to those authorized to have access. It protects the data from intentional or accidental tampering. Data confidentiality covers the data in storage, during processing, and while in transit. It is necessary that the communication between the sensor nodes be private and the intended receiver of data should have confidence that the data is not modified during its transmission. A loss of data confidentiality affects data privacy. Ensuring data confidentiality provides protection against eavesdropping.

Data Integrity: Data Integrity requires that the data should not be modified or destroyed in an unauthorized manner to provide data consistency. It covers data in storage, during processing and while in transit. In sensor networks, data integrity requires that messages are not accidentally corrupted by an imperfect communications channel and not intentionally corrupted by an attacker during transmission.

Data Freshness: Data freshness, in sensor networks, requires the messages to be current, ordered and not to duplicate (replays)