Chapter 2.6
How Trust and Reputation-Based Collaboration Impact Wireless Sensor Network Security

Noria Foukia
University of Otago, New Zealand

Nathan Lewis
University of Otago, New Zealand

ABSTRACT

Like wired network security, wireless sensor network (WSN) security encompasses the typical network security requirements which are: confidentiality, integrity, authentication, non-repudiation and availability. At the same time, security for WSNs differs from traditional security designed for classical wired networks in many points because of the new constraints imposed by WSN technology. Many aspects are due to the limited resources (memory space, CPU ...) and infrastructure-less property of WSNs. Therefore traditional security mechanisms cannot be applied directly and WSNs are more prone to existing and new threats than traditional networks. Typical threats are the physical capture of sensor nodes, the service disruption due to the unreliable wireless communication. Parameters specific to WSN characteristics may help to reduce the effect of threats. Examples of existing measures are efficient WSN power management strategies that can dynamically adjust the node cycles (sleeping or awake mode) based on the current network workload or the use of redundant information to locally detect lying nodes. In addition to adjusting existing WSN characteristics that impact security, establishing trust and collaboration is essential in WSNs for many reasons such as the high distribution of sensor nodes or the goal-oriented nature of many sensing applications. This chapter emphasizes the need of collaboration between sensor nodes and shows that establishing trust between nodes and using reputation reported by collaborating nodes can help mitigate security issues.

DOI: 10.4018/978-1-61350-101-6.ch206

INTRODUCTION

Wireless Sensor Networks (WSNs) are getting popular due to the many advantages that they provide for a lot of application domains (military, healthcare, emergency and disaster …). Mainly, WSNs are easy and fast to deploy in hostile environments and will not depend on pre-existing infrastructure (infrastructure-less nature of WSN). These properties considerably reduce the deployment cost of WSNs. Other characteristics make WSN technology attractive but at the same time more vulnerable than traditional wired network technology.

Security for WSN differs from traditional security designed for classical wired network in many points due to new constraints imposed by WSN technology. Therefore new solutions need to be implemented to provide WSN security or existing security solutions need to be adapted (Ng. H.S., Sim. M.L., & Tan. C.M., 2006: Karlof. C., & Wagner. D., 2003).

This chapter reviews threats targeted to WSNs. It briefly describes the components of a WSN and provides details on constraints imposed by WSN technology and their impact in WSN security.

Then, the chapter will focus on trust and reputation-based collaboration for WSN and its relation to security. The chapter finishes with a section about privacy issues in WSN before concluding.

DESCRIPTION OF A TYPICAL WIRELESS SENSOR NETWORK INFRASTRUCTURE

A Wireless Sensor Network (WSN) consists of spatially distributed autonomous nodes called sensors that monitor physical or environmental conditions, such as temperature or pressure at different locations (Römer. K., & Mattern. F., December 2004). They are used in a variety of applications, such as climate sensing and control in office buildings. A WSN is often composed of many (from a dozen to thousands) tiny sensors that are dispatched in an ad hoc way throughout a physical environment (house, battlefield) or inside the phenomenon to sense (human body). Each sensor is powered by a battery and collects data, such as temperature, pressure, heart rate, or other environmental data. Collected data is relayed to neighbor nodes and via the neighbor nodes to a destination node called the base station (BS) or sink (Karlof. C., & Wagner. D., 2003). At the BS, the data coming from several nodes is aggregated before being processed in order to provide the desired output corresponding to the phenomenon being sensed.

Components of a Sensor Node

A typical sensor node is composed of (Akyildiz. F., Su. W., Sankarasubramaniam. Y., & Cayirci. E., 2002):

- A sensing unit (or sensor) which is deployed either inside the phenomenon to be sensed or very close to it. This unit measures physical information about the event that it senses, such as pressure, light, heat, sound, etc.
- A microcontroller with a simple processing unit that is limited in terms of computations and memory. Therefore, sensor nodes often locally carry out simple computations and transmit partially processed data to special nodes called fusion nodes. A fusion node collects and combines data from several nodes and gathers that information with its own collected data before sending it to another node or to the BS.
- A transceiver that combines transmitting and receiving capabilities of the sensor node. The transceiver can also stop transmitting/receiving and switch to a sleeping mode.