Authentication in Wireless Sensor Networks

A thesis submitted to the Electrical Engineering Department
Faculty of Engineering – Alexandria University
in partial fulfillment of the requirements for the degree of
Master of Science
in
Electrical Engineering
by

Eng. Nagwa El-Meniawy

2015

Abstract

In Wireless Sensor Networks, nodes are microcontroller-based devices that are small in size and low in cost. These nodes, also called motes, have limited resources in terms of energy, computational capacity and wireless communication capabilities. Motes are deployed in an environment to perform an application-specific task. For instance, vibration sensors may be spread over a large structure like a bridge to collect information about it and relay it to a base station.

Security of WSNs is an important issue in their operation, since motes are usually left to operate unattended in the environment where they were deployed. This makes them vulnerable to attacks from malicious intruders who may wish to read sensitive data being transmitted or alter these data. Security mechanisms, therefore, need to be implemented in order to protect the network. These mechanisms are meant to achieve security goals such as the secrecy of a piece of communicated information or the authenticity of an agent's identity. They rely on the design of security protocols that are meant to secure communication between motes.

We focus on entity authentication protocols, where the goal is to verify the identities of motes in the network. This is crucial for secure communication, since, without it, an intruder can inject false data or interrupt network operation by introducing the intruder's own motes into the network. We propose an authentication protocol for WSNs and show how it can be executed as an integral part of a routing protocol. The authentication protocol is implemented using the NesC programming language and the TinyOS operating system for motes. Simulations of protocol execution are carried out using the TOSSIM simulator of WSNs.