جامعة الإسكندرية
ALEXANDRIA
UNIVERSITY

Wireless Sensor Networks Security

A thesis

submitted to the Electrical Engineering Department

Faculty of Engineering – Alexandria University

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in

Electrical Engineering

by

Sanaa Said Abd El-Dayem

February 2017

Abstract

Wireless sensor networks are a challenging field of research when it comes to security issues. Using low cost sensor nodes with limited resources makes it difficult for cryptographic algorithms to function without impacting energy consumption and latency. In this thesis, we focus on key management issues in multi-hop wireless sensor networks. These networks are easy to attack due to the open nature of the wireless medium. Intruders could try to penetrate the network, capture nodes or take control over particular nodes. In this context, it is important to revoke and renew keys that might be learned by malicious nodes. Cryptographic mechanisms can be employed to protect against some of the possible attacks: eavesdropping on messages is countered by encryption, and the injection of messages by the attacker is prevented by authentication. In particular, nodes could be compromised and then made to execute malicious code injected by the attacker. However, the attacks cannot be completely prevented and therefore, any communication security scheme being used must be sufficiently resilient to tolerate a certain amount of compromised nodes. Thus, novel mechanisms are required that provide a sufficient level of security while respecting the constraints in Wireless Sensor Networks.

This thesis proposed several secure protocols for key revocation and key renewal based on symmetric encryption. Because that the energy of sensor nodes is the major role in Wireless Sensor Networks, where mostly the network failure happens because of security attack and lack of energy of sensor nodes, so WSNs should efficiently use the sensor nodes and the power or energy and also the throughput should be efficient. All protocols are secure, but have different security levels. In particular, the present contributions are: key management schemes designed to satisfy security requirements of Wireless Sensor Networks and three protocols have been proposed for authentication of both message and entity in the Wireless Sensor Networks using shared-key discovery and path-key establishment. The introduced protocols reduced the energy consumption by reducing the CPU time and the size of messages needed for adding security requirements. The execution of the proposed authentication protocols is integrated within routing which is a novel idea in authentication of WSNs.

In addition, the work also deals with node mobility issues by proposing a re-authentication protocol which be executed by the initial authenticated node when its position changed. Each proposed protocol is analyzed and implemented using C++ programming language. The simulation of protocols execution are carried out using NS-2 simulator for Wireless Sensor Networks.