DESIGN AND ANALYSIS OF KEY MANAGEMENT SCHEMES FOR DISTRIBUTED WIRELESS SENSOR NETWORKS

By

Seyit Ahmet Çamtepe

An Abstract of a Thesis Submitted to the Graduate

Faculty of Rensselaer Polytechnic Institute

in Partial Fulfillment of the

Requirements for the Degree of

DOCTOR OF PHILOSOPHY

Major Subject: Computer Science

The original of the complete thesis is on file
in the Rensselaer Polytechnic Institute Library

Examining Committee:

Bülent Yener, Thesis Adviser
Boleslaw Szymanski, Member
Kenneth S. Vastola, Member
Malik Magdon-Ismail, Member

Rensselaer Polytechnic Institute
Troy, New York

April 2007
(For Graduation May 2007)

ABSTRACT

Secure communications in distributed *Wireless Sensor Networks* (WSN) operating under adversarial conditions necessitate efficient key management schemes. In the absence of a priori knowledge of post-deployment network configuration and due to limited resources at sensor nodes, key management schemes cannot be based on post-deployment computations. Instead, a list of keys, called a *key-chain*, is distributed to each sensor node before the deployment. For secure communication, either two nodes should have a key in common in their key-chains, or they should establish a key through a *secure-path* on which every link is secured with a key.

We first provide a comparative survey of well known key management solutions for WSN. Probabilistic, deterministic and hybrid key management solutions are presented, and they are compared based on their security properties and resource usage. We provide a taxonomy of solutions, and identify trade-offs in them to conclude that there is no one-size-fits-all solution. Second, we design and analyze deterministic and hybrid techniques to distribute pair-wise keys to sensor nodes before the deployment. We present novel deterministic and hybrid approaches based on *combinatorial design theory* and *graph theory* for deciding how many and which keys to assign to each key-chain before the sensor network deployment. Performance and security of the proposed schemes are studied both analytically and computationally. Third, we address the key establishment problem in WSN which requires key agreement algorithms without authentication are executed over a *secure-path.* The length of the secure-path impacts the power consumption and the initialization delay for a WSN before it becomes operational. We formulate the key establishment problem as a constrained bi-objective optimization problem, break it into two sub-problems, and show that they are both *NP-Hard* and *MAX-SNP-Hard.* Having established inapproximability results, we focus on addressing the authentication problem that prevents key agreement algorithms to be used directly over a wireless link. We present a fully distributed algorithm where each pair of nodes can establish a key with authentication by using their neighbors as the witnesses.