Chapter 5
Key Establishment for Securing Pervasive Wireless Sensor Networks

Anusree Banerjee
M S Ramaiah Institute of Technology, India

Divya P.
M S Ramaiah Institute of Technology, India

Jeevan E. L.
M S Ramaiah Institute of Technology, India

Jibi Abraham
M S Ramaiah Institute of Technology, India

ABSTRACT

Technological growth in embedded systems has given a leading growth for pervasive computing in today's human world. But the possibility of leakage of private information necessitates the need for security. Confidentiality service allows concealment of messages transmitted between communicating parties from the outsiders. To achieve confidentiality, it should be able to encrypt and decrypt the messages using a secret key. The key used must be agreed upon by the parties before start transmission. This chapter gives an overview of the issues in establishing a secret key, a scheme to establish the key and its implementation results. The scheme utilizes the fact that communication in sensor networks follows a paradigm called aggregation. Keys are split into shares and forwarded using disjoint paths in the network to reduce the effect of node compromise attack. The implementation results show that even though the scheme fits properly with the available memory with the sensor nodes, its communication overhead is high.

DOI: 10.4018/978-1-61520-741-1.ch005

INTRODUCTION

Pervasive computing extends computing anywhere at anytime using embedded systems. A Wireless Sensor Network (WSN) is the building block for many pervasive computing applications (Zheng Yuan Zheng, 2007). Each node in a WSN combines sophisticated sensing, computing and low-range communication in a low-power, low-cost system. WSNs can be easily deployed to various environments for tracking targets and monitoring various conditions. The applications include military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc. (Akyldiz, 2002) When pervasive WSNs deals with information related to like military matters or human personal, security becomes extremely important, as the network and data are prone to different types of malicious attacks. Hence to provide security, communication should be authenticated and encrypted. An open research problem in this area is how to bootstrap secure communications among sensor nodes. That is how to set up secret keys (pair-wise keys) among the communicating nodes.

The various activities of key management service include initializing the end users of the key, generating the key, distributing the key to each user, installing the key at each user, controlling the usage of the key, updating the key, revoking the old key and destroying the old key. Key establishment is a fundamental prerequisite for secure communication and it includes the key generation and its distribution. The unavailability of network infrastructure, low cost requirement and node resource constraints make the security solutions currently existing for traditional networks useless in WSN. Many researchers have worked in this area and proposed key management solutions (Yang Xiao, 2007). But while choosing an appropriate key establishment scheme for a WSN, the foremost importance has to be given to choose a scheme which uses fewer node resources (to achieve energy efficiency) in order to provide long network life. Hence we have chosen an approach proposed in the paper (Blaβ, 2006) to find whether it is energy efficient and secure against security compromise in sensor networks. It uses the concept of a '*master-device*' and the nodes in the network establish keys by using the concept of aggregation.

The remaining chapter is structured as follows: Section on "Key Management Issues in Pervasive WSNs" presents a brief introduction to various key management issues in pervasive wireless sensor networks. An overview of the selected key establishment scheme is available in Section "Overview of the Key Establishment Scheme" and its implementation, testing and results are given in the next Section. Conclusion and future works are suggested later.

KEY MANAGEMENT ISSUES IN PERVASIVE WSNS

The primary task of pervasive computing is to provide smart and continuous services designed according to specific requirements of users in order to enable them to live comfortably. The sensor networks used here are assumed to be collecting the context information like status of computing, resource availability, personal information of users, environmental information and temporal information. This context information may be accessed by intruders to breach their privacy. For example, a thief could analyze the wireless communication from a home automation system to find out whether there is anybody inside the house or not. Hence it is essential for a pervasive computing system to make the context information rapidly and continuously available along with preventing the unauthorized persons from blocking, impersonating, understanding or using the information.

In wireless sensor networks, data is transmitted between the nodes by using wireless communication and the wireless communication is