Chapter XXXVI
Routing Security in Wireless Sensor Networks

A.R. Naseer
King Fahd University of Petroleum & Minerals, Dhahran

Ismat K. Maarouf
King Fahd University of Petroleum & Minerals, Dhahran

Ashraf S. Hasan
King Fahd University of Petroleum & Minerals, Dhahran

ABSTRACT

Since routing is a fundamental operation in all types of networks, ensuring routing security is a necessary requirement to guarantee the success of routing operation. Securing routing task gets more challenging as the target network lacks an infrastructure-based routing operation. This infrastructure-less nature that invites a multihop routing operation is one of the main features of wireless sensor networks that raises the importance of secure routing problem in these networks. Moreover, the risky environment, application criticality, and resources limitations and scarcity exhibited by wireless sensor networks make the task of secure routing much more challenging. All these factors motivate researchers to find novel solutions and approaches that would be different from the usual approaches adopted in other types of networks. The purpose of this chapter is to provide a comprehensive treatment of the routing security problem in wireless sensor networks. The discussion flow of the problem in this chapter begins with an overview on wireless sensor networks that focuses on routing aspects to indicate the special characteristics of wireless sensor networks from routing perspective. The chapter then introduces the problem of secure routing in wireless sensor networks and illustrates how crucial the problem is to different networking aspects. This is followed by a detailed analysis of routing threats and attacks that are more specific to routing operation in wireless sensor networks. A research-guiding approach is then presented to the reader that analyzes and criticizes different techniques and solution directions for the secure routing problem in wireless sensor network. This is supported by state-of-the-art and familiar examples from the literature. The chapter finally concludes with a summary and future research directions in this field.

INTRODUCTION

Wireless sensor networks (WSNs) are gaining popularity due to the fact that they provide feasible and economical solution to many of the most challenging problems in a wide variety of applications such as military applications, healthcare, traffic monitoring, pollution/weather monitoring, wildlife tracking, remote sensing, and so forth. This has fuelled extensive research to address the critical issues of providing security, intrusion detection/tolerance, high availability, and survivability of the sensor network.

The issue of secure routing in wireless and mobile computing is a major challenging design factor in different networking aspects. However, the problem gets more complicated when considering infrastructure-less networks that exhibit even more constraints and new types of attacks. In the continuously and rapidly evolving area of wireless communication, the field of wireless sensor networks comes into the picture as a very hot area of research in all its aspects. WSN is a multihop network that is actually one type of ad hoc networks. However, WSN draws the special attention of researchers due to the fact that it exhibits more constraints and critical conditions than normal ad hoc networks in terms of power sources, computing capabilities, memory capacity, and other factors. This requires different approaches and protocol engineering directions from those applied to normal ad hoc networks.

WSNs are susceptible to several types of attacks at different layers of the network since they are normally deployed in open and unprotected environments and are constituted of cheap small devices with limited computational power, limited memory, and limited battery life. Nodes of a sensor network cannot be trusted for the correct execution of the critical network functions. Node misbehavior may range from simple selfishness or lack of collaboration due to the need for power saving, to active attacks aiming at denial-of-service and subversion of traffic. A sensor network without sufficient protection from these attacks may not be deployable in many areas. Intrusion preventive mechanisms such as encryption and authentication can be applied to protect WSNs against some types of attacks. Key management is the cornerstone of security services such as encryption and authentication in wireless sensor network. Research seeking low-cost key management techniques that can survive node compromises in sensor networks has been a very active area, yielding several novel key predistribution schemes. However, there are some attacks for which there is no known prevention method, such as wormhole attack. Moreover, there are no guarantees that the preventive methods will be able to hold the intruders. Hence it is necessary to use some mechanisms of intrusion detection. Besides preventing the intruder from causing damages to the network, the intrusion detection system can acquire information related to the attack techniques, helping in the development of better prevention systems.

One special aspect in WSN is the provision of secure routing. As mentioned previously, the nature of WSN complicates the security requirements and adds difficulties in solving security problems. In fact, secure routing in WSN is actually still not captured well in the research field. One main reason is that the design of a routing protocol is biased towards solving the problem of power limitations and reducing communication overhead while keeping security concerns at a later phase to be integrated with the current routing solutions.

Among different approaches in solving the problem of secure routing in WSN, reputation system-based solution is one technique that has generated enough interest among WSN researching community. Reputation systems attempt to provide security by allowing different nodes rate each other based on their routing activities and behavior analysis. When a node has an experience profile about its neighbors, it may select the node that it trusts more, and, hence, achieve a secure routing operation.

The rest of the chapter is organized as follows. Section 2 of the chapter provides the relevant background material covering an overview of WSN that includes WSN definition, sensor node structure, applications, and so forth. As WSN is a class of mobile ad hoc networks (MANET), the main differences between WSN and MANET will