Chapter XXVI
Security in Mobile Ad Hoc Networks

Bin Lu
West Chester University, USA

ABSTRACT

Mobile ad hoc network (MANET) is a self-configuring and self-maintaining network characterized as dynamic topology, absence of infrastructure, and limited resources. These characteristics introduce security vulnerabilities, as well as difficulty in providing security services to MANETs. Up to date, tremendous research has been done to develop security approaches to MANETs. This work will discuss the existing approaches that have intended to defend against various attacks at different layers. Open challenges are also discussed in the chapter.

INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring and self-maintaining network composed of mobile nodes that communicate over wireless channels (Perkins, 2001). MANETs are characterized as infrastructure-less with rapid topology change, high node mobility, and stringent resource constraints. A MANET is usually used in situations such as military battles, disaster recovery, and emergent medical situations. While applications in these areas still dominate the research needs for MANETs, commercial applications (such as home networking and personal area networks) have also been brought to attention with the rapid research progress in mobile telephony and personal digital assistants.

Early research in MANETs assumed a cooperative and trusted environment, which unfortunately is not always true. In an unfriendly environment, a variety of attacks can be launched, ranging from passive eavesdropping to active interference. The attacks could target a number of devices or services in MANETs, such as wireless channels, routing protocols, high-level applications, or even security mechanisms themselves. A misbehaving node can be *selfish* or *malicious*, based on their intensions. A selfish node can simply deviate

from network protocols in order to maximize its own profit, while a malicious node may intend to corrupt some services or bring down some other nodes. Both selfish and malicious misbehaviors are dangerous in that they could cause degradation in the network performance, or even paralyzation of the entire network. Therefore security has become a primary concern, especially for security-sensitive applications in a noncooperative or hostile environment.

However, introducing security features to MANETs is not a trivial task. The lack of a fixed infrastructure determines that MANETs do not have a clear physical line of defense, unlike their wired counterparts, who can deploy security defense mechanisms (e.g., firewalls) at network devices such as gateways or routers. The decentralized manner of operations also implies that a central administration point is not realistic for MANETs. Moreover, all security services come with a price. The security mechanisms will share with other services the precious communication and computation resources, which may consequently affect the performance of the node, or even the entire network. Performance is also a basic concern for ad hoc networks, which means a tradeoff has to be made between security and other services such as computation and communication. Therefore, minimum consumption of resources is one of the most important requirements for security solutions in MANETs.

This chapter will discuss security issues in MANETs, including security attacks, security requirements, security solutions, and their advantages and weakness.

The remainder of this chapter is organized as follows: the following section will discuss the security vulnerabilities, security services, and security challenges for MANETs; the third section will focus on the security solutions that have been proposed for MANETs. The security mechanisms to protect MAC (medium access control) layer communications and routing protocols will be described. Intrusion detections, authentication, and key management will be also discussed in this section. In the last section we will discuss the open research issues for MANET security and then we will conclude the chapter.

VULNERABILITIES, SECURITY SERVICES, AND CHALLENGES

MANETs Vulnerabilities

MANETs suffer from all the vulnerabilities that their wired counterparts encountered. An adversary may launch various attacks ranging from *passive* eavesdropping to *active interference* such as traffic jamming, packet modification and fabrication, message replay, denial-of-service (DoS), and so forth. Some of these vulnerabilities are aggravated in a wireless context due to the characteristics of MANETs, such as the lack of a clear line of defense and the in-the-air communications.

Besides, ad hoc networks are susceptible to vulnerabilities that are inherent to wireless networks, which reside in their routing and autoconfiguration mechanisms. The MAC (medium access control) protocols (such as IEEE [1999] 802.11 series) and most of the routing protocols for MANETs are designed with the assumption that all the nodes will cooperate and would not intentionally deviate from the protocols. However, this is not always true, especially in an autonomous network where nodes belong to different self-profited organizations.

Eavesdropping is generally easier in MANETs than in the Internet due to the open nature of the communication medium in MANETs. Passive attacks are by nature difficult to detect, not mentioning in MANETs where many mobile devices support promiscuous mode. Like in the wired networks, cryptographic operations are used to prevent ad hoc networks from eavesdropping.

The MAC protocols in MANETs are vulnerable to traffic jamming, which is caused by nodes who fail to follow the protocols in order to maximize their own profit or simply to disrupt network operations. A node can obtain an unfair share of the bandwidth by transmitting without waiting its turn, or interrupt signal transmissions by injecting bogus signals into the network. Communication channels in MANETs are open and shared, therefore it is difficult to prevent and detect this kind of attacks. Moreover, ad hoc nodes are usually battery-powered, which makes energy a precious resource in MANETs. An adversary could launch a new type