Chapter XIII
Security in Ad-Hoc Networks

Muhammad Mahmudul Islam
Monash University, Clayton, Australia

Ronald Pose
Monash University, Clayton, Australia

Carlo Kopp
Monash University, Clayton, Australia

ABSTRACT

Due to the nature of wireless media, dynamic network topology, resource constraints, and lack of any base station or access point, security in ad-hoc networks is more challenging than with cabled networks. In this chapter, we discuss various attacks on the network layer of ad-hoc networks. We also review security protocols that protect network layer operations from various attacks.

INTRODUCTION

An ad-hoc network consists of a set of nodes that communicate using a wireless medium over single or multiple hops and do not need any pre-existing infrastructure such as access points or base stations. Ad-hoc networks can comprise of mobile, static, or both types of nodes. Ad-hoc networks containing mobile nodes are known as MANETs (mobile ad-hoc networks). An example of ad-hoc networks with static nodes is SAHN (suburban ad-Hoc network) (Kopp & Pose, 1998). Since ad-hoc networks can be rapidly deployed, they are attractive for digital communication in battlefields, rescue operations after a disaster, and so forth. Ad-hoc networks are also useful in civilian forums for running demanding multimedia applications such as video conferencing.

Due to the lack of a clear physical boundary, a node in an ad-hoc network is very likely to hear the transmissions of a neighbouring node operating in the same frequency channel. If the

node cannot distinguish the packets transmitted by an authorised neighbour from the ones transmitted by a malicious node, then the malicious node can: (1) cause the node to accept misleading information, and (2) propagate unnecessary traffic and misleading information to other parts of the network. As a result normal network operation could be disrupted.

The wireless medium makes eavesdropping easier than with a cabled network. If the packets are not encrypted properly, eavesdroppers can make unauthorised use of the received information and cause trouble. For example, an eavesdropper can forward unencrypted routing information to an accomplice to disrupt the normal operation of the network.

For the aforementioned reasons security is a primary concern in ad-hoc networks in order to provide secure communication among the nodes in a potentially hostile environment (Yang, Luo, Ye, Lu, & Zhang, 2004). Resource constraints (e.g., battery or computational power), dynamic network topology, and lack of infrastructure (e.g., fixed trusted nodes, base stations, or access points) make the security issue more challenging.

Existing ad-hoc routing protocols, such as DSR (dynamic source routing) (Johnson & Maltz, 1996) or AODV (ad-hoc on-demand distance vector) (Perkins & Royer, 1999) assume a trusted and cooperative environment. These routing protocols have to be protected from malicious nodes that can disrupt the network operation by intentionally disobeying of the protocol specifications (Yang et al., 2004).

There are two main approaches to secure a network: (1) pro-active and (2) reactive. A pro-active approach tries to prevent any attacks happening in the first place. On the other hand, a security protocol using a reactive approach detects any anomaly in network operation and

Figure 1. Classification of network layer security protocols