Chapter 10
Key Management Protocols in Mobile Ad Hoc Networks

Mohamed Elboukhari
University Mohamed Ist, Morocco

Mostafa Azizi
University Mohamed Ist, Morocco

Abdelmalek Azizi
University Mohamed Ist, Morocco & Academy Hassan II of Sciences & Technology, Morocco

ABSTRACT

Mobile ad hoc networks (MANETs) have received tremendous attention in recent years because of their self-organization and self-maintenance capabilities. MANETs are networks that do not have an underlying fixed infrastructure. However, these networks tend to be vulnerable to a number of attacks. They don't obey a centralized network management functionality; furthermore, the network topology changes dynamically. Therefore, security has become a primary concern in MANETs. The major problem in providing security services in such networks is how to manage cryptography keys, making key management a central component in MANETs. This chapter gives an overview of security in this kind of network and presents a number of MANETs key management protocols according to recent literature.

INTRODUCTION

Mobile Ad Hoc Networks

MANETs are a new paradigm of wireless communication for mobile hosts (which we call nodes). A MANET is a self-configuring and self-maintaining network composed of mobile nodes that communicate over wireless channels (Perkins, 2001). Mobile nodes communicate directly via wireless links, while those located farther apart rely on other nodes to relay messages as routers. Thus, an ad hoc network is a collection of autonomous nodes that form a dynamic, purpose-specific, and multi-hop radio network in a decentralized fashion. These networks, by definition, possess no fixed support infrastructure such as mobile switching centers, base stations, access points, and other centralized machines. Each node in such a network operates not only as a host but also as a router, forwarding packets for other mobile nodes

DOI: 10.4018/978-1-60960-027-3.ch010

in the network that may be multiple hops away from each other.

Today, the main application of ad hoc networks is in military tactical operations. Military units, equipped with wireless devices, can form an ad hoc network when they roam the battlefield. Other examples of applications include business associates sharing information during a meeting or attendees using laptop computers to participate in an interactive conference.

Security Goals

MANETs, in early research, assumed a cooperative and trusted environment, which, unfortunately, is not always true. A variety of attacks can be launched in an unfriendly environment, ranging from passive attacks to active interference. Therefore, security has become a primary concern. Ad hoc networks must meet a number of security requirements including authentication, confidentiality, integrity, authorization, non repudiation, and availability.

Authentication: enables a node to ensure the identity of the peer node with which it is communicating. We assume initially that the two legitimate parties are authentic: each is the entity it claims to be, and that third parties do not interfere by impersonating one of the two legitimate parties.

Confidentiality: ensures that certain information is never disclosed to unauthorized entities. The network transmission of sensitive information requires confidentiality, and the leakage of such information to enemies could have devastating dangerous consequences, such as revealing tactical military information or making illegal access to bank accounts.

Integrity: guarantees that an exchanged message is not altered: the received data does not contain any modification, insertion, deletion, nor replay. A message could be corrupted because of a benign failure, such as radio propagation impairments, or because of a malicious attack on the network.

Authorization: establishes a set of roles that define what each network node is or is not allowed to do. So, a user must be first identified to gain access to the resource and then the corresponding access rights are guaranteed.

No repudiation: means that the sender of a message cannot later deny sending this information, and the receiver cannot deny its reception. In the case of public key cryptography, a node *A* signs the message using its private key. Other nodes can verify the signed message by using *A*'s public key, and *A* cannot then deny the message because of its signature.

Availability: ensures the survivability of the network despite malicious incidences. For example, an attacker can use jamming to interfere with communication at the physical layer, or it can make unworkable the routing protocol at the network layer by disrupting the route discovery procedure.

Security Challenges

MANETs have specific features that pose both challenges and opportunities in achieving the security goals which are an important issue for those in security-sensitive environments.

First, the use of wireless links renders an ad hoc network accessible to both legitimate users and malicious attackers. A malicious node is susceptible to impersonation by other nodes even without gaining physical access to its victims. An eavesdropping process might give an attacker access to secret information, and violate the security goal of confidentiality. Also, an active attack might allow the adversary to delete messages, inject erroneous messages, modify messages, and so. As a result, there is no clear line of defense in MANETs from the security design perspective. The boundary that separates the inside network from the outside world becomes complex and blurred. And, therefore, there is no well-defined infrastructure where we may deploy a simple security solution.