Chapter XXXI
Security Measures for Mobile Ad-Hoc Networks (MANETs)

Sasan Adibi
University of Waterloo, Canada

Gordon B. Agnew
University of Waterloo, Canada

ABSTRACT

Mobile ad hoc networks (MANETs) have gained popularity in the past decade with the creation of a variety of ad hoc protocols that specifically offer quality of service (QoS) for various multimedia traffic between mobile stations (MSs) and base stations (BSs). The lack of proper end-to-end security coverage, on the other hand, is a challenging issue as the nature of such networks with no specific infrastructure is prone to relatively more attacks, in a variety of forms. The focus of this chapter is to discuss a number of attack scenarios and their remedies in MANETs including the introduction of two entities; ad hoc key distribution center (AKDC) and decentralize key generation and distribution (DKGD), which serve as key management schemes.

INTRODUCTION

There are two classes of attacks on a network: *passive* and *active* attacks. In passive attacks, the intruder poses as an observer and only audits the information exchanged between communicating parties, without any intervention. Whereas in active attacks, the intruder actually takes part actively and performs actions such as additions, deletions, or delays.

The most basic requirements of a secure system should prevent common passive and active attacks, through the following functionalities:

- **Confidentiality:** Confidentiality or *privacy* is the ability to secure the content of the information communicated between authorized parties. When confidentiality is in place, the intruder should not be able to recover any information (part of the definition for pas-

sive attacks). In a broader sense, an intruder should not be able to determine the parties involved or whether a communication session occurred (anonymous routing). There are two levels of confidentiality:

- **Data confidentiality:** In which the unauthorized users are unaware of the existing protected data and their nature. This is further subcategorized as:
  - *Confidentiality of existing protected information*
  - *Confidentiality of protected data exposure*
- **Address confidentiality:** Which hides the identity of participating parties

- **Data integrity:** Integrity of data ensures the authorized recipient that data have not been altered in any sense, including addition, deletion, and undue delays. This requires data authentication. The following scenarios are associated with data integrity:
  - **Unauthorized modification protection:**Protecting against any illegitimate alteration.
  - **Detection of unauthorized protected data modification:** Detecting that a protected data has been modified in an unauthorized manner.
  - **Detection of a data deletion in a sequential order:** In a serial transmission (one bit at a time), it is important to detect if any part of the transmission has been deleted.
- **Authentication:** Authentication is a very important security requirement, which provides the facility to verify the identity of parties taking part in a communication. There are three types of authentication procedures (Kargl, 2006):
  - **Entity (user) authentication:** This type of authentication is used to authenticate an entity or a device to make sure entities wishing to communicate with other parties in the communication range are the ones they claim to be, such as people, clients, and servers.
  - **Geo-authentication:** In this type of authentication, the location of the nodes or any information about locations are to be verified and authenticated.
  - **Attribute authentication:** This is the process of establishing confidence in an attribute that applies to a specific device or entity.
  - **Data authentication:** Authentication of data is the ability of the authorized parties to ascertain the authenticity of data received from other authorized parties.
- **Nonrepudiation:** This is the ability to prevent an authorized user from denying the involvement in previous communications or activities. This is further subcategorized as follow:
  - **Protection against sender denial:** Protecting the receiver from the send er's denial that the data were sent by the sender.
  - **Protection against forward denial:** Protecting against the denial of forwarding entities on the path, disputing their forwarding actions.
  - **Protection against delivery denial:** Protecting against the delivery dispute of the data to the final destination.
  - **Protecting against receiving denial:** Protecting the sender from the recipient's denial of the fact that it has ever received the data.
- **Access control:** Access control is a mean for enabling the legitimate user to have access to the resources. Access control uses one or more of the other security mechanisms for granting access to the communications channel and/or applications. The following scenarios are categorized under access control:
  - **User identification:** Access control uti lizes user-authentication to grant access for legitimate individuals.