Chapter 7
Applied Cryptography in Infrastructure-Free Wireless Networks

Lei Zhang
Frostburg State University, USA

Chih-Cheng Chang
Rutgers University, USA

Danfeng Yao
Rutgers University, USA

ABSTRACT

This chapter presents the technical challenges and solutions in securing wireless networks, in particular infrastructure-less wireless networks such as mobile ad hoc networks and wireless sensor networks. Communications in infrastructure-less wireless networks are challenging, as there are no trusted base stations to coordinate the activities of mobile hosts. Applied cryptographic tools, in particular threshold cryptography, play an important role in the trust establishment, message security, and key management in such networks. We describe several technical approaches that integrate applied cryptography techniques into mobile ad hoc networks and wireless sensor networks. We also outline several research directions in these areas.

INTRODUCTION

Wireless networks can be generally categorized into infrastructure-based and infrastructure-less types according to their communication mechanisms. In either type, cryptographic protocols are needed to ensure the security of message flow within the network. The goal of this chapter focuses on the technical challenges and solutions in securing advanced infrastructure-less wireless networks, by surveying some of existing research papers that intersect applied cryptography and mobile ad hoc networks or wireless sensor networks.

Let's first briefly introduce basic cryptographic concepts. There are mainly two cryptographic systems, symmetric and asymmetric. Symmetric system is that both the sender and receiver of a message share a single, common key that is used

DOI: 10.4018/978-1-61520-783-1.ch007

to encrypt and decrypt the message. Symmetric-system is simple and fast, but its main drawback is that the two parties have to exchange the key in a secure way. Public-key encryption is typically asymmetric, which can avoid the problem above. In asymmetric system, the public key can be distributed in a non-secure way, and the private key is never transmitted.

A public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity — information. The certificate can be used to verify that a public key belongs to an individual. A certificate authority (CA) is an entity which issues digital certificates for use by other parties. The signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. We will describe more about these cryptographic concept in the context of wireless networks later.

The IEEE 802.11 is one of the conventional infrastructure-based wireless networks. Its specification identified several services to provide a secure environment. The security services are currently provided largely by the Wi-Fi Protected Access (WPA) protocol to protect link-level data during wireless transmission between clients and access points [45]. The three basic security services defined by IEEE for the wireless local area networks (WLAN) environment are authentication, confidentiality, and integrity. It is worth mentioning that the previous IEEE 802.11 standard, Wired Equivalent Privacy (WEP), has major security vulnerabilities due to the repetitive use of secret one-time keys [45].

A wireless ad hoc network is the most common kind of wireless networks. It is a decentralized wireless network without any predetermined infrastructure. The network is called ad hoc networks, because each node voluntarily forwards data to other nodes. The determination of which nodes forward data is made dynamically based on the network connectivity. In most cases, nodes in wireless ad hoc networks are mobile. This special kind of ad hoc network is called Mobile Ad Hoc Networks (MANET).

We call MANET infrastructure-less, because unlike traditional wireless networks, MANET does not have base stations to coordinate the activities of mobile hosts. Each node acts as a router to transmit messages from one node to another and also need to perform all other functions involved in any network. Therefore, this causes the network topology to change frequently and dynamically. These networks are useful in military environments or environments where geographical, terrestrial or time constraints make it difficult to have base stations or access points. MANET has many advantages in situations where a network needs to be configured on an ad hoc basis without the support of any fixed infrastructure.

Besides military applications, MANET has also been used in forming vehicular networks [31, 34] or to give One Laptop Per Child users Internet connections. One Laptop Per Child Association (OLPC) is a U.S. Non-profit organization to oversee the creation of an affordable educational device for use in the developing world. OLPC laptops connect to the Internet through a peer-to-peer fashion by forming a MANET. Figure 1 shows the MANET formed by OLPC laptops in a village. The laptops relay messages for each other. All OLPC laptops are connected to the Internet, as they route messages through a computer that connects to a satellite receiver, which serves as a base station. This base station brings the whole village connected [2].

However, traditional security mechanisms cannot be applied to MANET, because of the wireless nature of communication. The lack of any security infrastructures raises several security problems. The mobility nature of MANET also leads to frequent topology change. Security schemes for MANET generally cannot use symmetric mechanisms. The reason is that in ad hoc network, two parties cannot trust each other and