Chapter 9
Offline/Online Security in Mobile Ad Hoc Networks

Wen-Jung Hsin
Park University, USA

Lein Harn
University of Missouri – Kansas City, USA

ABSTRACT

Mobile ad hoc network is a network comprised of mobile nodes quickly forming an autonomous network for a particular purpose such as emergency search and rescue. One of the most prominent security challenges for such a network is the limited capacity in the mobile nodes, thereby preventing costly computation operations. However, this limitation on a mobile node manifests itself only when the mobile node is dispatched on an active duty (i.e., online). One can prepare the mobile nodes as much as possible offline in anticipation of an upcoming deployment. In this chapter, the authors present three offline/online authentication and key agreement schemes and one offline/online non-repudiation scheme, all aiming at fast online computation for mobile nodes in mobile ad hoc networks.

INTRODUCTION

A Mobile Ad hoc NETwork (MANET) is a set of mobile nodes rapidly and dynamically forming an autonomous network. A mobile node is a generic term for a mobile communication device such as a router, a laptop, a Personal Digital Assistant (PDA) and a smartphone in which the device can freely move around. The main attraction of a MANET is its self-organizing, roaming, and swiftly deployable features among the mobile nodes. Initially, a MANET was for use in military (Taneja & Patel, 2007). Over the years, it has also been applied to the communication among entities in many other settings, e.g., emergency rescuers, conference and meeting attendees, sensors for collecting environmental and ecological data, devices for monitoring human physiological data (Saha, Bhattacharyya,

DOI: 10.4018/978-1-4666-4030-6.ch009

& Banerjee, 2012), learners in an instantaneous classroom (Luo, Zerfos, Kong, Lu, & Zhang, 2002), taxicabs dispatching and booking services (Boukerche, Camara, Loureiro, & Figueiredo, 2009; Huang, Hu, Crowcroft, & Wassell, 2005), and vehicle-to-vehicle and vehicle-to-roadside in vehicular MANETs (Raya & Hubaux, 2007).

A MANET has been studied extensively due to its distinct challenges. These challenges include energy and memory limitation in the mobile nodes, low bandwidth, limited transmission ranges, unreliable transmission links, changing topology due to the roaming feature of the mobile nodes, and network forming without requiring fixed network infrastructure (Taneja & Patel, 2007). As routing is essential to the feasibility of a MANET, the study in routing was one of the focal points in the early stage of a MANET. Many routing protocols (such as ARAN – Authenticated Routing for Ad Hoc Networks, SAODV – Secure Ad Hoc On-Demand Distance Vector Routing, and SEAD – Secure Efficient Ad Hoc Distance Vector Routing) have been proposed for a MANET since then (Karlsson, Dooley, & Pulkkis, 2012; Kaur & Rai, 2012; Lee, 2011; Singh, Yadav, & Ranvijay, 2007).

Outside of feasibility study, security is very important for a MANET especially when one of the first applications of a MANET is to be used in battlefields where a secure MANET is important in the midst of attacks by the enemies. Considering the distinct challenges mentioned above, it is difficult to directly use the traditional cryptography techniques in a MANET. For example, when using public-key cryptography within an autonomous MANET, public-key infrastructure such as a Certificate Authority (CA) may not exist (Chlamtac, Conti, & Liu, 2003). Additionally, public-key cryptography usually incurs high computational overhead (Kumar, Munjal, & Sharma, 2011; Liang & Wang, 2005). Thus, it is not feasible for energy and memory limited mobile nodes. Consequently, it may not be practical to directly apply some of the current public-key cryptosystems in a MANET. In spite of the challenging considerations mentioned above, as MANETs become increasingly popular for the applications that they can support, it is imperative to strengthen the security of MANETs.

For the literature up to date, one can broadly categorize the schemes that deal with the secure association in MANETs into three categories:

1. A MANET with a centralized server (also referred to as an organized MANET by Lin and Slay [2005]; as an authority-based MANET by Van der Merwe, Dawoud, and McDonald [2007]).
2. A MANET with a distributed server (Di Crescenzo, Ge & Arce, 2007; Murugan & Shanmugam, 2012).
3. A MANET self-organized by the mobile nodes themselves (also referred to as an open MANET by Capkun, Buttyan, and Hubaux [2003]; as a pure MANET by Lin and Slay [2005]; as a public MANET by Van der Merwe, Dawoud, and McDonald [2007]).

A MANET with a centralized server is frequently used for applications such as military or emergency relief where the mobile nodes are to follow certain authority so that they can access the network services robustly (Van der Merwe, Dawoud, & McDonald, 2007). For a MANET with a distributed server, a collective service is distributed among a set of mobile nodes. In a MANET self-organized by the mobile nodes themselves, there is no centralized or distributed server as such this kind of MANET tends to be open (i.e., the mobile nodes can come in and out of a MANET at ease [Van der Merwe, Dawoud, & McDonald, 2007]).

Depending on the duration of the MANET applications, Saxena, Tsudik, and Yi (2009) distinguished MANETs into long-lived MANETs and short-lived MANETs. Saxena, Tsudik, and Yi gave an example of a long-lived MANET in which military ships travel overseas in a group. Examples of a short-lived MANET are for sensors gathering environmental data for an afternoon,