Chapter XXVIII
Secure Routing with Reputation in MANET

Tomasz Ciszkowski
Warsaw University, Poland

Zbigniew Kotulski
Warsaw University, Poland

ABSTRACT

The pervasiveness of wireless communication recently gave mobile ad hoc networks (MANET) significant researchers' attention, due to its innate capabilities of instant communication in many time and mission critical applications. However, its natural advantages of networking in civilian and military environments make it vulnerable to security threats. Support for anonymity in MANET is orthogonal to a critical security challenge we faced in this chapter. We propose a new anonymous authentication protocol for mobile ad hoc networks enhanced with a distributed reputation system. The main objective is to provide mechanisms concealing a real identity of communicating nodes with an ability of resistance to known attacks. The distributed reputation system is incorporated for a trust management and malicious behaviour detection in the network.

INTRODUCTION

The contemporary information society extensively takes advantage of wireless communication using several specific network technologies. This continuously evolving area provides a flexible and convenient way for improving work standards in business, home, education, or rescue applications. Thanks to the pervasiveness of private unlicensed spectrum technologies such as Bluetooth and IEEE 802.11 family protocols, the communication between personal and handheld electronic devices is easier, comfortable, and mobile. Through the years, a lot of researches' efforts were devoted to the functional and network performance improvements, covering existing standards designed for fully cooperative environments. However, many first pioneering deployments of wireless networks quickly turned out its several vulnerabilities they suffer from. Since that time substantially more

attention has been paid to the security as a supplementary service protecting and supporting performance in wireless communication. The specific and unique characteristics of mobile ad hoc networks (MANET) such as a multihop routing and highly dynamic topology impose a new type of security concerns that we present in this chapter.

In response to the vulnerabilities being identified in several MANET protocols a set of security considerations have taken place in a number of extensions to existing nonsecure approaches. Even though, the strong security requirements are met in many MANET protocol designs, only few of them address anonymity and privacy guaranties (Boukerche, 2004; Ciszkowski & Kotulski, 2006; Kong & Hong, 2003; Zhang, Liu, & Lou, 2005), which are treated as an orthogonal to security critical challenge we discuss in this chapter. On the example of a novel anonymous authentication protocol (ANAP) for mobile ad hoc networks (Ciszkowski & Kotulski, 2006) we present an enhanced distributed reputation system designed for efficient and secure routing in MANET. The main objective of this work is to provide protocol with mechanisms concealing the real identity of the communicating nodes maintaining the resistance to known attacks (Chaum, 1981; Pfitzmann & Hansen, 2005). The distributed reputation system is incorporated in order to build and manage mutual trust of the communicating nodes. The trust knowledge reflects a trustworthy and malicious activity in the network, effectively improving secure routing in MANET by means of anonymous authentication and path discovery phases. ANAP delivers links for secure exchange of data, taking advantage of an on-demand routing approach (Hu et al., 2002; Perkins & Royer, 1999; Royer & Toh, 1999).

The following sections present related work and protocol designs focusing on the distributed reputation system improving secure and anonymous routing in MANET. Two last sections cover some concluding remarks and further research directions.

BACKGROUND

MANET is a set of mobile nodes which operates wirelessly in an environment with a devoid of fixed network structure enforced by self-configuring and self-organizing mechanisms. All its nodes are free to move, join, or leave the network in ad hoc manner, while the end-to-end communication between nodes being beyond its radio range is performed in a multihop fashion. This specific feature demands for additional requirements to every node that, apart from sending and receiving data, must act as an interconnecting router. Since every node may be obliged to perform data forwarding, appropriate routing algorithms were developed to meet such a requirement. The main objective of routing protocols for ad hoc network is creating an up-to-date multihop communication path in a dynamically changing network topology. The appropriate and specific path discovery and path maintenance algorithms have already been developed which characterizes particular routing protocols. One can distinguish two groups of protocols designed for MANET: reactive (on-demand) and proactive (table-driven). The first type tries to resolve a path to a destination node on the source node demand, whereas the second approach is more preventive and continuously keeps routing tables up to date by monitoring the nearest neighbourhood. The detailed description and comparison of both classes of routing protocols for ad hoc networks may be found in works by Hu et al. (2002), Johnson (1994), and Royer et al. (1999).

At the moment several applications apart from strict MANET paradigm take advantage of the dynamic ad hoc routing phenomenon and make use of it in an akin to MANET wireless environments such as wireless mesh networks or vehicular ad hoc networks (VANET). This increasing application potential gives the MANET's security a primary concern for researching communities.

For MANETs there are several solutions considering multilayer defence against known attacks, mainly focusing on provided services such as authentication, anonymity, confidentiality, and integrity based on the network layer security. Most of them extend existing protocols for which the