Chapter 47
Investigating the Performance of the TSS Scheme in Noisy MANETs

Hussein Al-Bahadili
Petra University, Jordan

Ghassan F. Issa
Petra University, Jordan

Shakir M. Hussain
Petra University, Jordan

Khaled El-Zayyat
Al-Ahliyya Amman University, Jordan

ABSTRACT

A Mobile Ad Hoc Network (MANET) suffers from high packet-loss due to various transmission impairments, such as: wireless signal attenuation, free space loss, thermal noise, atmospheric absorption, multipath effect, and refraction. All of these impairments are represented by a generic name, noise, and therefore such a network is referred to as a noisy network. For modeling and simulation purposes, the noisy environment is described by introducing a probability function, namely, the probability of reception (p_c), which is defined as the probability that transmitted data is successfully delivered to its destination despite the presence of noise. This chapter describes the implementation and investigates the performance of the Threshold Secret Sharing (TSS) node authentication scheme in noisy MANETs. A number of simulations are performed using the MANET Simulator (MANSim) to estimate the authentication success ratio for various threshold secret shares, number of nodes, node speeds, and noise-levels. Simulation results demonstrate that, for a certain threshold secret share, the presence of noise inflicts a significant reduction in the authentication success ratio, while node mobility inflicts no or an insignificant effect. The outcomes of these simulations are important to facilitate efficient network management.

INTRODUCTION

A mobile ad hoc network (MANET) is defined as a collection of low-power, wireless, mobile nodes forming a temporary network without the aid of any established infrastructure or centralized administration (Murthy & Manoj, 2004; Agrawal & Zeng, 2003; Toh, 2002). Despite the fact that MANETs offer a number of benefits over wired and other infrastructure wireless networks, still there are many challenges that need to be addressed for fully harvesting MANETs' benefits. These include: limited communication bandwidth, limited battery power and lifetime, size of the mo-

DOI: 10.4018/978-1-4666-2919-6.ch047

bile devices, security, communication overhead, induced transmission errors, distributed control problem, nodes mobility and dynamic variation of network topology, scalability, meeting certain Quality-of-Service (QoS), etc (Stallings, 2003).

MANETs security is challenging for several reasons, such as (Huang & Medhi, 2008): security breach, node mobility, service ubiquity, network dynamics, network scale, etc. Furthermore, MANETs are very vulnerable to a number of security attacks, such as: passive eavesdropping over the wireless channel, Denial-of-Service (DoS) attacks by malicious nodes, and attacks from compromised entities or stolen devices (Kong, et al., 2001). As for any information exchange system, the main requirements that need to be carefully considered to ensure high-level of MANET security are: confidentiality, authentication, integrity, availability, and non-repudiation.

This paper is concerned with one of the main security requirements for MANETs, namely authentication. Authentication is the verification of the identity of a party who generated some messages, and of the integrity of the messages. In computer networks, two types of authentication can be identified, namely, message authentication and node authentication. Message authentication is a technique for verifying the integrity of a transmitted message. While node authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to system resources and sensitive information and interfering with the operation of other nodes. There are two differences between message and node authentications, these are (Forouzan, 2008):

1. Message authentication may not happen in real time; node authentication does. In message authentication, when a sender sends a message to a receiver, while the receiver authenticates the message; the sender may or may not be present in the communication process. On the other hand, when the sender requests node authentication, there is no real message communication involved until the sender is authenticated by the receiver. The sender needs to be online and takes part in the authentication process. Only after the sender is authenticated can message communicated between the two parties.
2. Message authentication simply authenticates one message; the process needs to be repeated for each new message. Node authentication authenticates the sender for the entire duration of a session.

The most popular network authentication architectures are Kerberos (Kohl, et al., 1994), the X.509 standard (Aresenault & Turner, 2001), and Public-Key Infrastructure (PKI) trust model (Perlman, 1999), which are based on using a globally trusted Certificate Authority (CA) model (Balfanz, et al., 2002). Using a globally trusted CA model may work well in wired or infrastructure (access point) wireless networks, but not MANETs because: MANETs provide no infrastructure support (infrastructureless), each of the CA servers is exposed to a single point of compromises and failures, multihop communications over the error-prone wireless channel expose data transmissions to high packet-loss rate and large latency, and frequent route changes induced by node mobility, which makes locating and contacting CA servers in a timely fashion non-trivial (Yi & Kravets, 2003). Variations of the CA model, such as hierarchical CAs and CA delegations, can ameliorate but cannot addresses issues such as service availability and robustness (Perlman, 1999). Therefore, more efficient and reliable solutions are required to address the above issues. One alternative solution to address the problem of authentication in MANETs is to use the concept of secret share proposed by Adi Shamir in 1978 (Shamir, 1979).

The Shmir's concept of secret share was used in (Luo, et al., 2002) for developing an efficient scheme for self-securing wireless ad hoc networks, which we shall refer to as Threshold Secret Shar-