Chapter 13

Security Issues and Models in Mobile ad hoc Networks

Revathi Venkataraman
SRM University, India

T. Rama Rao
SRM University, India

ABSTRACT

This chapter covers issues related to security in mobile ad hoc networks. It acts as a comprehensive survey material covering the cryptographic schemes and trust modeling techniques traditionally found in mobile ad hoc network (MANET) survey articles. The need for hybrid security techniques, involving both cryptographic approach and trust based model, in a resource constrained ad hoc network, is also emphasized in this work. Additionally, the lack of realism in the research works related to ad hoc network security is also pointed out. The state of the art in ad hoc security should employ hybrid techniques that can be easily implemented in an ad hoc network. This will lead to the large scale deployment of mobile ad hoc networks in various context-aware applications.

INTRODUCTION

A revolution in ubiquitous computing has arrived due to the technological advances made in the development of wireless computer networks. Wireless networks in which computing nodes are capable of self-organization have become a reality thus enabling deployment of ad hoc networks. The ad hoc capability can potentially lead to the extension of Internet services to places with geographically rough terrain where a communication infrastructure is nonexistent. This capability, however, does not come without a price. Due to unpredictable availability and performance of communication links and dynamically changing topologies of nodes, a lot more design constraints and complexities are to be taken care of.

MANETS are characterized by peer-to-peer communicating nodes on ad hoc basis over an infrastructure-less network. The memory and
computational power of these mobile ad hoc devices are limited. Due to this reason, it is not possible to employ any central monitoring audit software over these networks. The communication in a mobile ad hoc network is over a wireless link and a number of security attacks are possible. Some of these links may be lossy and dynamic due to environmental factors and hence, they are unreliable.

MANETs have significant applications in the defence arena. With the move towards the Network Centric Warfare and Global Information Grid (GIG), a variety of services on demand to the various echelons of the defence forces can be easily provided. With these advancements in the MANET field, the security has become a raising concern in MANET deployment in field areas. They are also used for a wide variety of applications like battlefield surveillance, industrial process, machine monitoring, control, medical, healthcare and traffic control systems (Glisic, 2006). The wireless channel of communication is an open channel where any adversary node can easily overhear the transmission between the communicating parties. Since, these networks are infrastructure-less, many of the security approaches suitable for web services cannot be directly applied to these ad hoc devices. This is also due to fact that their resources are limited in terms of energy, bandwidth, computation and memory.

The MANET security issues and challenges are addresses in two broad ways, namely cryptographic approaches and trust-based approaches. The cryptographic approaches extensively used in ad hoc security (Buttayan & Hubaux, 2007) use one or more symmetric and asymmetric encryption algorithms and hashing techniques to achieve confidentiality, authentication and access control. These techniques are considered as hard security approaches. While these techniques are time-tested approaches, they cannot identify ‘soft security threats’. Here, the user may be an authenticated and authorized user in the network. But, due to compromise or sabotage, they may behave maliciously thereby causing maximum damage to the network resources. Trust based security approaches act as an extended arm by addressing these challenges. But, they cannot stand independent and provide complete security to a system. The five security requirements are to be satisfied by any security framework

A comprehensive survey on the traditional cryptographic and trust based approaches is made in this work. The issues that are not addressed by each of these approaches are pointed out and the need for hybrid security schemes employing both cryptographic and trust-based approaches is emphasized. Additionally, this article also addresses the voids in MANET security research where more realistic approaches are required, other than simulation models, for the deployment of these devices in practical applications.

**BACKGROUND**

**Security Issues and Threats**

Security attacks in MANETs are classified into two broad categories: passive and active attacks.

- In a passive attack, the attacker *eavesdrops* the channel used by the victim node. By promiscuously listening to the victim node, an attacking node can gather the unencrypted data that is actually being transmitted. Even otherwise, if the data is encrypted, the attacker analyses the traffic patterns and the frequency of transmissions between the communicating victims. This information can be later used for causing further damage to the system.
- In an active attack, the attacker may *not cooperate* in the network. In a non-cooperating state, the attacker may not involve in the routing process and drop the data packets meant for other nodes in the network. This behavior is *selfish* as these attacking