Chapter 6
Prevention of Blackhole Attack using Certificateless Signature (CLS) Scheme in MANET

Vimal Kumar
M. M. M. University of Technology, India

Rakesh Kumar
M. M. M. University of Technology, India

ABSTRACT

One of the generally used routing protocols for MANET is AODV (Ad hoc on demand Distance Vector), which is vulnerable to one of the particular type of security attack called blackhole attack. The characteristics of blackhole attack, a malicious node sends a false route reply without having any fresh route to a destination and is also drop all receiving packets and replay packet in the entire network. A certificateless based signature scheme enables users to generate their public key and private key without using any certificate. Due to this reason, we do not need any certificate authority (CA). In this paper, we propose a novel CLS scheme for prevention of a blackhole attack and also provide secure communication based on CLS scheme. Simulation results show that CLS scheme prevents blackhole attack successfully and is provide better performance to other existing schemes in the presence of blackhole node and also ensuring authentication, integrity and non-repudiation.

DOI: 10.4018/978-1-5225-0741-3.ch006

INTRODUCTION

A wireless mobile ad hoc network (MANET) (Abel, 2011) is a collection of self-configuring nodes deployed in an ad hoc manner. These self-moveable nodes communicate with each other in single hop as well as multi-hop manner without the aid of any centralized administrator or established infrastructure. Because of unrestricted mobility and connectivity to the users, the liability of network management entirely depends on the mobile nodes which form ad hoc network. Multi-hop communication is needed due to a limited transmission range of wireless ad hoc network (Saha, Chaki, & Chaki, 2008). The success of communication highly depends on the cooperation of intermediate nodes. In such networks, each mobile node works as host as well as a router to find an optimal path in different routing approaches of MANETs. MANET is an infrastructure less network. The structure or topology of a MANET changes with time due to nodes mobility. Thus, the vulnerability of a MANET is greater than wired networks due to these salient characteristics such as dynamic topologies, limited physical security, compromised nodes in networks, no centralized management and no infrastructure (Nadeem & Howarth, 2013). Routing (Perkins, Park, & Royer, 1999) in MANET is a challenging task. Two main routing algorithms category are proactive viz., table driven and reactive viz., on-demand routing algorithms. Routes are created on-demand in reactive routing protocols. There are several reactive routing protocols (Abhay et al., 2010) such as Ad-hoc On-demand Distance Vector (AODV), Associativity Based Routing (ABR), Location-Aided Routing (LAR), Dynamic Source Routing (DSR) protocol and Temporally Ordered Routing Algorithm (TORA). Routes are always available in proactive routing. In such protocols, routing tables are updated through periodical message exchange. Examples of such protocols (Djenouri & Khelladi, 2005) are Wireless Routing Protocol (WRP), Destination Sequence Distance Vector (DSDV), Distance Routing Effect Algorithm for Mobility (DREAM) and Fisheye State Routing (FSR).

Security Goals

There are some basic security requirements (Goyal, Batra, & Singh, 2010) for secure message communication as given below:

- **Confidentiality:** It ensures that message content is never seen by unauthorized mobile nodes (Kannhavong et al., 2007).
- **Authentication:** It ensures that data is coming and going to or from a trusted and authorized source and a claimed destination.