Chapter 7

A Secure Gateway Discovery Protocol Using Elliptic Curve Cryptography for Internet-Integrated MANET

Pooja Verma
Madan Mohan Malaviya University of Technology, India

ABSTRACT

Integration procedures are employed to increase and enhance computing networks and their application domain. Extensive studies towards the integration of MANET with the internet have been studied and worked towards addressing various challenges for such integration. Some idyllic mechanisms always fail due to the presence of some nasty node or other problems such as face alteration and eavesdropping. The focus of this chapter is on the design and discovery of secure gateway scheme in MANET employing trust-based security factors such as route trust and load ability. Over these, the elliptic curve cryptography is applied to achieve confidentiality, integrity, and authentication while selecting optimum gateway node that has less bandwidth, key storage space, and faster computational time. Simulation results of the security protocol through SPAN for AVISPA tool have shown encouraging results over two model checkers namely OFMC and CL-AtSe.

DOI: 10.4018/978-1-5225-5742-5.ch007

INTRODUCTION

Mobile Ad hoc network is an autonomous stand-alone structureless network without any need of centralized authority. MANET is a galaxy of mobile nodes which can communicate via wireless links. These nodes are free to move and change their location anytime, and anywhere. A type of an interface called a gateway is required to connect a MANET architecture with the Internet. This integrated architecture results in a kind of wireless access network wherein gateway advertises its information regarding its availability along with consumption of resources of the network, however, various challenges arise during this process. Due to mobility of end nodes, they receive several advertisement messages from different gateways. Consequently, the decision-making process regarding the selection of the most efficient gateway out of various available gateways becomes challenging. Being a key towards successful integration of MANET with the Internet, several gateway discovery procedures have been developed, however, a procedure which is both efficient as well as able to transmit and receive packets securely is highly desired. Design of such a gateway discovery procedure requires a clear understanding of the security concept of MANET, various security algorithms and security parameters to have a safer data delivery and a highly efficient integration of MANET with the Internet.

Figure 1, illustrates the integration of MANET with the Internet, where mobile nodes MN1, MN2, MN3, MN4, and MN5 belong to proactive zone and all other mobile nodes belong to the reactive zone. This architecture comprises of two gateway nodes GW1 and GW2 which are used for its integration with Internet. It has three fixed node points to which MN intends to communicate (Gupta, Kumar and Gupta, 2014).

Several strategies for selection of optimum gateway based on ‘route trust’, ‘load capacity of a node’, ‘path’ and ‘node trust values’, have been proposed. However, these have found to be inadequate to prevent the malicious node activities.

In this chapter, a *gateway discovery scheme* which is efficient, trustworthy and secure is presented. The security is achieved by the use of secure parameters as ‘route trust level’, ‘node trust’, ‘hop count’ and ‘residual path load capacity’. To prevent possible malicious activity by some node, an authentication scheme based on elliptic curve cryptographic scheme is used in the proposed method. The proposed scheme also improves the delivery ratio, decreases the packet drop rate with cost lower in comparison to other gateway selection mechanisms. It also requires less bandwidth and storage space, thereby resulting in the fastest computation. The use of elliptic curve cryptography ensures secure integration with the Internet.