Chapter 11
A Novel Secure Routing Protocol in MANET

Ditipriya Sinha
CIEM, India

Uma Bhattacharya
Bengal Engineering and Science University, India

Rituparna Chaki
University of Calcutta, India

ABSTRACT

This chapter gives an overview of research works on secure routing protocol and also describes a Novel Secure Routing Protocol RSRP proposed by the authors. The routes, which are free from any malicious node and which belong to the set of disjoint routes between a source destination pair, are considered as probable routes. Shamir’s secret sharing principle is applied on those probable routes to obtain secure routes. Finally, the most trustworthy and stable route is selected among those secure routes using some criteria of the nodes present in a route (e.g., battery power, mobility, and trust value). In addition, complexity of key generation is reduced to a large extent by using RSA-CRT instead of RSA. In turn, the routing becomes less expensive and highly secure and robust. Performance of this routing protocol is then compared with non-secure routing protocols (AODV and DSR), secure routing scheme using secret sharing, security routing protocol using ZRP and SEAD, depending on basic characteristics of these protocols. All such comparisons show that RSRP shows better performance in terms of computational cost, end-to-end delay, and packet dropping in presence of malicious nodes in the MANET.

1. INTRODUCTION

This chapter gives an overview of secure routing protocols in MANET and describes a robust secure routing protocol (RSRP) proposed in (Sinha et al., 2012). A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETs are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected...
A Novel Secure Routing Protocol in MANET to the Internet. Security service requirements of MANET are similar to wired or any infrastructure wireless network. Here, every routing protocol needs secure transmission of data. Authentication, availability, confidentiality, integrity and non-repudiation are five inevitable concepts to provide secure environment in MANETs. Authentication ensures that the communication or transmission of data is done only by the authorized nodes. Without authentication any malicious node can pretend to be a trusted node in the network and can adversely affect the data transfer between the nodes. Availability ensures the survivability of the services even in the presence of the attacks of malicious nodes. Confidentiality ensures that information should be accessible only to the intended party. No other node except sender and receiver node can read the information. This can be possible through data encryption techniques. Encryption and decryption are two important techniques for secure routing in MANETs. Encryption is a technique which converts plain text message in ciphertext. Decryption is the reverse of encryption. Integrity ensures that the transmitted data is not being modified by any other malicious node. Non-repudiation ensures that neither a sender nor a receiver can deny a transmitted message. Non-repudiation helps in detection and isolation of compromised node.

Key generation, encryption and decryption play an important role for providing secure routing in MANETs. However these schemes increase computational overheads for all nodes in the network. The RSA algorithm involves three steps: key generation, encryption and decryption. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. Chinese remainder theorem (CRT) uses the result about congruence in number theory and its generalizations in abstract algebra. In RSA-CRT, it is a common practice to employ the Chinese Remainder Theorem during decryption which results in a decryption much faster than modular exponentiation used in RSA.

Secret sharing in MANETs is a challenging issue due to its dynamic nature. Many researchers are involved in solving the secret sharing problem. Shamir’s proposal is one of the eminent secret sharing schemes. This scheme uses the concept of Lagrange’s Interpolation method, a popular technique for polynomial evaluation. Shamir’s scheme divides the data packet into n pieces such that it can be easily reconstructed from any $k = \frac{n}{2}$ number of pieces.

Main objective for secure routing is that data should be transmitted in secure and confidential way from source to destination. Trust value, battery power and stability of the nodes are the factors or attributes for determining a reliable, stable and trustworthy path in between a source-destination pair. Absence of any attributes of them may make the path unreliable.

A new security scheme has been proposed in this chapter for MANETs. This paper uses RSA-CRT scheme for its high efficiency in key generation, encryption and decryption of data. For secure route detection a safety key is generated. This safety key is divided into n pieces and propagated through n different available routes in between a source-destination pair. Safety key can easily be reconstructed from any $k = \frac{n}{2}$ pieces.

Shamir’s secret sharing has been extended to the application of finding secure routes between a source destination pair using Lagrange’s Interpolation scheme in the proposed work. Final route amongst those is chosen by using the criteria of a stable and trustworthy path i.e. trust value, battery power and stability of the nodes.

Section 2 contains background of past works related to the area, Section 3 contains scope of the work, Section 4 describes some basic schemes used in secure routing, proposed secure routing protocol is elaborated in section 5, performance
Related Content

Chipless RFID Sensor for High Voltage Condition Monitoring
[www.igi-global.com/chapter/chipless-rfid-sensor-high-voltage/69712?camid=4v1a](www.igi-global.com/chapter/chipless-rfid-sensor-high-voltage/69712?camid=4v1a)

Distributed Computation in Wireless Sensor Networks: Efficient Network Architectures and Applications in WSNs
[www.igi-global.com/article/distributed-computation-in-wireless-sensor-networks/154479?camid=4v1a](www.igi-global.com/article/distributed-computation-in-wireless-sensor-networks/154479?camid=4v1a)

Extended Cell Planning for Capacity Expansion and Power Optimization by Using MEMETIC Algorithm
[www.igi-global.com/article/extended-cell-planning-for-capacity-expansion-and-power-optimization-by-using-memetic-algorithm/85004?camid=4v1a](www.igi-global.com/article/extended-cell-planning-for-capacity-expansion-and-power-optimization-by-using-memetic-algorithm/85004?camid=4v1a)

Spectrum Handoff Management in Cognitive Radio Networks: Solutions, Modeling, and Future Directions
[www.igi-global.com/chapter/spectrum-handoff-management-cognitive-radio/78233?camid=4v1a](www.igi-global.com/chapter/spectrum-handoff-management-cognitive-radio/78233?camid=4v1a)