Chapter 4
Security Aspect in Multipath Routing Protocols

Prasanta K. Manohari
Silicon Institute of Technology, India

Niranjan K. Ray
Silicon Institute of Technology, India

ABSTRACT

In the absence of central authority, dynamic topology, limited bandwidth and the different types of vulnerabilities secured data transmission is more challenging in Mobile Ad hoc Network (MANET). A node in MANET acts as a host as well as a router. Routing is problematic due to node mobility and limited battery power of node. Security mechanisms are required to support secured data communication. It also requires mechanism to protect against malicious attacks. In recent times multipath routing mechanisms are preferred to overcome the limitation of the single path routing. Security in routing dealt with authentication, availability, secure linking, secure data transmission, and secure packet forwarding. In this chapter, we discuss different security requirements, challenges, and attacks in MANETs. We also discuss a few secured single path and multipath routing schemes.

1. INTRODUCTION

Mobile ad hoc network (MANET) is a self-configuring, infrastructure-less network. The nodes in this network are mobile in nature and they do not depend on any fixed

DOI: 10.4018/978-1-4666-8687-8.ch004

infrastructure to support communication among themselves (Mohapatra, & Krishnamurthy, 2005). Network topology changes rapidly due to the node characteristics. The network is easy to deploy in any environments. MANETs lead themselves to countless applications such as battlefield communication, disaster recovery management, environmental monitoring, etc. In the same time, it suffers with different challenges due to its physical constraints.

MANET performs many tasks and routing is major among them. The path between a source and destination is established through many intermediate nodes. The packet is forwarded by many nodes and passes through multi-hops to reach at destination. Nodes can move, leave and join the network at any point of times. As a results, path between source-destination changes rapidly. It causes link-failure, frequent modification at routing table, increased delay and congestion in the network. Subsequently it is very easy for hackers to eavesdrop and gain access to confidential information. Attacker inserts erroneous routing information, changes routing updates and transmits incorrect routing information.

The security objectives in the mobile ad hoc networks are also affected by different attacks. Such objectives are: *authentication, confidentiality, integrity, availability, and non-repudiation* (Yang, Haiyun, Fan, Songwu, & Zhang, 2004). Excluding these parameters security of MANETs cannot be complete. In literature, numerous security mechanisms are discussed. But, they do not give any concrete solutions to protect against the different attacks. In this chapter, we focus on different security aspects in single and multipath routing (Tarique, Tepee, Adibi, & Erfani, 2009). Single-path routings are not enough to provide higher data rate transmission. However, that can be achieved by establishing multiple paths between a source-destination pair. Therefore in many applications multipath routing are preferred. Multipath routing provides many benefits and at the same time, security in multipath is also more challenging. Several attacks or vulnerabilities may affect the route discovery of multipath routing protocols. Any malicious node or misbehaving node can create unfriendly attack or remove all other nodes from providing any service. Attacks or vulnerabilities are allowing a small set, or even a single node, to control the routing paths of critical nodes. The use of multiple paths in MANETs could diminish the effect of unreliable wireless links and the frequent topological changes. Nodes in an ad hoc network are usually powered by carefully distributing traffic load into multiple paths.

The remaining of this chapter is coordinated as follows: In Section 2, different security challenges and requirements are discussed. In Section 3, different secured routing mechanisms are discussed. Conclusions are given in Section 4.