Chapter 2
Network Security:
Attacks and Control in MANET

Mamata Rath
C.V.Raman College of Engineering, India

Jhum Swain
Siksha 'O' Anusandhan University, India

Bibudhendu Pati
C.V.Raman College of Engineering, India

Binod Kumar Pattanayak
Siksha 'O' Anusandhan University, India

ABSTRACT

This chapter describes how with the rapid increase of internet users, more people have access to global information and communication technology. As a result of which, the issues of using the internet as a global platform for the enabling of smart objects and machines to coordinate, communicate, compute and calculate, gradually emerge. In Mobile Ad-hoc Networks (MANETs) the individual nodes are self-reconfigurable according to the changes of the network topology. Joint effort between portable hubs is more critical because they face major challenges such as powerlessness to work safely while protecting its assets and performing secure steering among hubs. With the existence of malicious nodes, one of the principal challenges in MANETs is to outline powerful security arrangement that can shield MANETs from various routing attacks. This chapter highlights major attacks and control mechanism in MANETs with an intention that it will open directions for researchers to explore more in the field of network security. At the end of this chapter, basic security mechanisms and issues related to emergence of IoT from Mobile networks has been highlighted.

DOI: 10.4018/978-1-5225-4100-4.ch002

INTRODUCTION

As MANET is a core technology emerged in the new generation, the basic security challenges include seamless communication with reliability in the network. In a wireless network without any infrastructure where there is no base station and access point, the chance of vulnerability is more. The mobile devices are free to move in any direction still maintaining connectivity with other mobile nodes. Due to this special quality of MANET, the design of MANET protocol with high-security features in very much essential. Again, due to dynamic change in topology, the network change takes place dynamically and so the network is decentralized and more vulnerable than the wired based network in many aspects.

In a special network called MANET, electronic devices and gadgets such as tablets, PCs, mobile phones, machines with specially appointed correspondence capacity are connected together to make a system. MANET is a self-organizing structure of flexible switches related hosts associated with secluded connections. The routers move randomly and compose themselves accordingly; along these lines, the systems remote topology may change quickly and capriciously (Huang et al., 2014). In MANETs (Madan Mohan et al., 2013), each node acts as the router and because of dynamic changing topology the accessibility of hubs is not generally ensured (Ling et al., 2012). It likewise does not ensure that the way between any two hubs would be free of pernicious hubs. The remote connection between hubs is exceptionally vulnerable to connection assaults such as passive eavesdropping, active interfering, etc. (Sridhar et al., 2013). Due to inflexibility in the infrastructure of MANET, it affects the security feature whenever any kind of extreme computation is done to perform encryption. So due to this problem, it is important to build a secured connection which can provide the high-security solution to provide secured services like authentication, confidentiality, integrity, non-repudiation, and availability. So here security is provided in each and every layer (Madan Mohan et al., 2013).

SECURITY MECHANISM IN MOBILE AD-HOC NETWORKS

Mobile Ad-hoc Networks have been well appreciated in recent years due to its fantastic features such as self-configurable workstations called nodes and they themselves can do their own maintenance (Jain et al., 2014). There are many open security issues in this special network such as its open architecture of network, its shared medium, the problem of resource constraints, and changeable network topology. In the network layer of the network model various attacks takes place during routing of the packets from one mobile device to other. There are some forwarding attacks, which leave the routing tables alone, but change the delivery of packets. Due to any weakness of the design of the underlying protocol, many attacks happen because of which there is denial of service to authenticated devices and many other type of problems take place (Choudhury et al., 2015). In the data link layer, various attacks take place due to any lacuna in Wireless Encryption Protocol. Similarly, another type of attack called Denial of Service (DoS) takes place (Dolk et al., 2017) in which the attacker prevents the communication between the network and a particular node member by isolating it from the group (Mejri et al., 2017). There are many novel contributions to develop secured protocols to prevent such attack in the network (Rath et al., 2016). The basic objective of security implementation in Mobile Ad-hoc networks is to keep sustainable connectivity over multi-hop wireless channels (Umamaheswari et al., 2015) to provide link-level security solutions and security mechanism provision at the network level (Paramasivan et al., 2015).