Chapter 10
DoS Attacks in MANETs:
Detection and Countermeasures

Rajbir Kaur
Malaviya National Institute of Technology, India

M. S. Gaur
Malaviya National Institute of Technology, India

Lalith Suresh
Malaviya National Institute of Technology, India

V. Laxmi
Malaviya National Institute of Technology, India

ABSTRACT

A mobile ad hoc network (MANET) is a collection of mobile devices that communicate with each other without any fixed infrastructure or centralized administration. The characteristics specific to MANET (1) dynamic network topology, (2) limited bandwidth, (3) limited computational resources, and (4) limited battery power pose challenges in achieving goals of security and availability. MANETs are vulnerable to Denial of Service (DoS) attacks that can adversely affect performance of MANET. In this chapter the authors present a survey of DoS attacks at various layers, their detection and respective countermeasure.

INTRODUCTION

With the widespread use of lightweight devices like laptops, PDAs, wireless telephones and sensors, the importance of wireless computing and particularly mobile ad hoc networking have come to the fore. Continued reduction in cost has resulted in diverse fields where deployment of such networks is being conceived. In mobile networks, there are some applications, which cannot rely on the presence of any fixed infrastructure. Examples of such applications are: emergency disaster relief in a damaged area after a storm or an earthquake; a set of digital sensors positioned to take measurements in a region unreachable by humans; military tanks and planes in a battlefield; and finally, students (or researchers) sharing

DOI: 10.4018/978-1-60960-123-2.ch010

information during a lecture. This infrastructure independence leads to the concept of mobile networks namely, ad hoc networks.

A mobile ad hoc network (MANET) is a collection of mobile devices that communicate with each other without any fixed infrastructure or centralized administration. The mobile hosts in MANET establish their own network as and when required. It is for this reason that MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes.

In MANET the nodes can communicate directly if they are within each other's transmission range. If the source node is outside the destination node's wireless range, it needs to rely on intermediate hosts to relay its packets. This is referred to as a multi hop scenario. Each node in MANET functions as a source, destination or an intermediate router. Another characteristic of MANET is that mobile hosts have limited resources (CPU, storage, energy, etc.), the wireless channels are unreliable and have limited bandwidth.

These very characteristics of MANET make it vulnerable to a wide variety of attacks. Like any other network, ad hoc networks must also provide some security services to protect resources and information from attack. An effective security architecture must ensure (1) Availability, (2) Authentication, (3) Data confidentiality, (4) Integrity and (5) Non-repudiation. With all other security services in place, MANET is not achieving its objective if the services provided by it are not **available** to authorized users when they need it. This non-availability of resources to authorized users is known as Denial of Service (DoS).

This chapter surveys DoS attacks and it's countermeasures based on protocol stack, in MANETS. The rest of the chapter is organized as follows: In Section 1, an overview of DoS is presented followed by taxonomy of DoS attacks in MANET. In section 2 we discuss DoS attacks and its countermeasures in the physical layer, followed by attacks and countermeasures at MAC layer in section 3. A general description of two protocols - DSR and AODV - largely adopted by (IETF's MANET working group, n.d.) can be found in Section 4. This is subsequently followed by a discussion on attacks and detection schemes in the network layer in section 5. Section 6 concludes the chapter.

1. DENIAL OF SERVICE (DOS)

A DoS can be characterized as an attack with the purpose of preventing the legitimate users from using a victim computing system or a network resource. A DoS attack usually has the following properties:

(a) **Malicious:** Intentional act of harming a node so as to cause a failure.
(b) **Disruptive:** Degradation or disruption of some capability or service.
(c) **Asymmetric:** The property of prevention/detection measure effort of an attack being greater that the effort required mounting it. For example, buffer overflow attacks are easy to execute but the effect may crash the server.
(d) **Remote:** Attacks are usually carried out over the network using a spoofed IP to escape traceback.

DoS attacks are thus proving to be a serious and permanent threat to users, organizations and network resources.

Figure 1 outlines the taxonomy of DoS attacks at the lower three layers of the wireless protocol stack. In this chapter, we analyze attacks in terms of IEEE 802.11 standard, which covers physical and MAC layer. The standard currently defines a single MAC that interacts with three PHYs (running at 1 or 2 Mbit/s). We also survey attacks and defense mechanisms in the routing layer. In the remaining sections we discuss these attacks.