A STUDY OF DOS ATTACKS IN MANET

Prof. Ajay Kumar Patel

[1]*Assistant Professor, Computer Engineering Department,*

Institute of Technology, Nirma University, Ahmedabad, Gujarat, (India)

ABSTRACT

A MANET (Mobile Ad-Hoc Network) is a dynamic, self-configurable and independent network without any fixed infrastructure. MANET have different characteristics like limited power, dynamic topology, wireless medium, security , routing and lack of infrastructure unit. Routing is require for communication between nodes. So secure routing is major concern in MANET against various security attacks. In this paper, I introduce various routing protocols and different Denial of Service (DoS) attacks in MANET.

Keywords: Denial of Service (Dos), Mobile Ad-Hoc Network (MANET), Route Reply (RREP), Route Request (RREQ)

I. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is a collection of nodes that communicate with each other via wireless medium. MANET is a type of Ad-Hoc Network. A MANET is a self-configurable and independent network which doesn't requires fixed infrastructure. In MANET communication between nodes is done through shared wireless medium. MANET has dynamic nature means any node can join and leave the network any time. Due to limited communication range each node in the MANET act as a host or router that forward packets to neighbour nodes. Because of dynamic nature of MANETs, it has various applications like military, rescue missions, automated battleships, virtual classrooms, inter vehicular communication and computing, electronic payments, conference meetings and many more. An example of MANET is shown in Fig. 1.

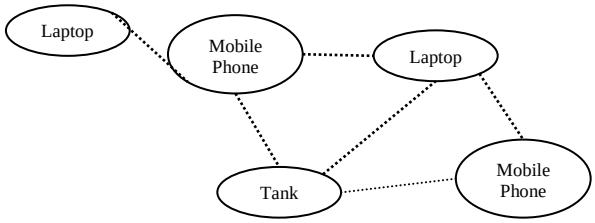

Figure 1. Manet Example

MANET has several issues [1] [2] like security, power constraints, IP addressing, mobility management, bandwidth, Quality of Service (QoS), guarantee of service. In this paper, I surveyed various DoS attacks in MANETs.

II. PROTOCOL STACK SECURITY ATTACKS ON DIFFERENT LAYERS

Security attack can be done on various layers of protocol stack. Routing and its protocols are important consideration for attacks in MANET. Due to dynamic nature and mobility of nodes, nodes do not have any prior

knowledge about topology; because of that nodes have to determine the topology through advertisement. So routing protocol has to identify the optimal path between source and destination that has minimum bandwidth and overhead. Attacks on network are classified as passive or active attacks. In passive attacks, attacker observes the data transmitted between sender and receiver. While in active attacks, attacker modify the data or denial the various resources available at server.

Basically there are three types of routing protocols [1] as mentioned below:

- Proactive protocols:
  - It uses table-driven approach.
  - Route discovery is done prior to requirement.
  - Examples: DSDV, FSR, CGSR, etc.
- Reactive protocols:
  - It uses on-demand approach.
  - Route discovery is done when needed using flooding approach.
  - Examples: DSR, AODV, etc.
- Hybrid:
  - It uses combination of proactive and reactive approach.
  - Route discovery is done prior to requirement.
  - Examples: TORA, HSR, ZRP, etc.

Each layer in protocol has its own functionality. Attacker attacks on layer by its methodology and functionalities. TABLE 1 shows the different attacks on layers of protocol stack [2].

TABLE 1: Security attacks on protocol stack layers

Sr. No.	Protocol Layer	Attack Name
1.	Physical Layer	Jamming, Eavesdropping
2.	Data Link Layer	Traffic monitoring and analysis, WEP weakness, Disrruption MAC (802.11)
3.	Network Layer	*DoS attacks:* Blackhole, Wormhole, Grayhole, Byzantine, Resource Consumption attack, Rushing attack *Information Disclosure* *Routing attacks*: Routing table overflow, Routing table poisoning, Packet replication
4.	Transport Layer	SYN flooding, Session hijacking
5.	Application Layer	Worms, Repudiation, Data corruption, Viruses

In next section I discussed some of the Denial of Service (DoS) attacks in detail.

III. DENIAL OF SERVICE (DOS) ATTACKS IN MANETS

In this section; Blackhole attack, Wormhole attack, Grayhole attack, Rushing attack and Sleep deprivation attack are discussed in following subsections.

3.1 Blackhole Attack

In blackhole attack [2] [3], the malicious node advertises the shorter path to the destination. When malicious node received the packets from the node then malicious node drops the packets. A blackhole attack can be implemented in AODV by sending RREP to received RREQ that says it has shortest path to the destination.

3.2 Wormhole Attack

In wormhole attack [1] [3] [4], malicious nodes (means worms) connected via high-speed tunnel (wormhole link) and they are placed at strongest position in network. Worm encapsulate data packets and falsify the route lengths. One worm records packets at one location and forwards them to another location to peer worm, giving intuition to nodes in both groups that they are immediate neighbours. So many packets in the network are forwarded through these worms. Worm can able to analyze the packet or drop the delivered messages. Wormhole attacks do not alter integrity of received packets.

3.3 Grayhole Attack

It is also known as selective blackhole attack. In this attack [2] [3] [5], malicious node becomes the part of the network and drops the selective packets rather than dropping all the packets. It is done by various ways. First way, it drops the packets comes from a particular sender or intended for a particular receiver. Second way, it drops the certain type of packets while forwards all other packets. Third way, it drops the packets at specific time. Four way, it drops the certain type of packets at specific time.

3.4 Rushing Attack

It uses duplicate suppression mechanism [3]. In which attacker forwards route discovery route request packet that it receives more quickly than the legitimate nodes without considering the processing delay and changing hop count of request packet received to 1.

3.5 Sleep Deprivation attack

Sending and receiving messages depends on battery power of node. In this attack [3], it is launched by flooding the specific node with garbage routing packets. Here attacker broadcasts large number of RREQ packets in the starting of route discovery phase so that all legitimate nodes receives them and process them. So it utilizes the battery power to serve unnecessary RREQ packets. It is also named as resource consumption attack.

3. 6 Forwarding Disruption Attacks

Malicious node can launch forwarding rejection attacks [6] [7]. Jelly fish attacks are type of forwarding disruption attack.

Due to TCP congestion control mechanism, TCP flows are closed-loop flows. TCP is vulnerable to drop, delay and mis-order the packets. Wormhole, flooding and other attacks disobeys the protocol rules. While in jelly fish attack, malicious node obeys all the rules of protocol. It is passive type attack and difficult to detect also. The goal of jellyfish node is to weaken the goodput, which can be done by dropping some of packets. There are three types of jelly fish attacks as explained in TABLE 2.

TABLE 2: Types of Jelly Fish Attacks

Sr. No.	Jelly fish attack name	Short Description
1.	Jellyfish Reorder Attack	It uses TCP reorder packets vulnerability. It is possible due to factors like multipath routing, route changes, etc.
2.	Jellyfish Periodic Dropping Attack	It is possible due to sarcastically chosen period by the mischievous node. It is possible at relay nodes. Here suppose node drops some percentage packets periodically then TCPs throughput may be reduced to near zero for small values of percentage [6].
3.	Jellyfish Delay Variance Attack	In this attack, malicious node delays the packet without changing packets order. Here delay is selected randomly.

3.7 Sybil Attack

In this attack [2], a malicious node uses more than one identities in network by assuming new IDs. There is no centralize entity in MANET, it means no true correspondence between entity and identity. A malicious node has many identities in which only one identity is true. When malicious node receives a packet for the false identity, it can cause packet forwarding misbehaviour or send a fake acknowledgement or send the packet as a genuine forward.

3.8 Sinkhole Attack

A malicious node places itself at very good position in the network and broadcasts the high quality route or shortest route to destination or spoofs the neighbouring nodes that are neighbours of receiver. Then performs one of the various tasks like drop the packets, selective forwarding or data manipulation [2].

IV. CONCLUSION

Secure and trusted routing is a prime concern for researchers in MANET. In this paper, I covered the routing protocol overview and attacks on different layers of protocol stack in MANET. I discussed various DoS attacks like Wormhole, Blackhole, Grayhole, Jelly fish, etc. So exhaustive research must carried out to develop secure, trust-based and efficient mechanism for DoS attacks.

REFERENCES

[1] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, DoS Attacks in Mobile Ad-hoc Networks: A Survey, Second International Conference on Advanced Computing & Communication Technologies, 2012, 535 – 541

[2] Rutvij H. Jhaveri, Ashish D. Patel and Kruti J. Dangarwala, Comprehensive Study of Various DoS Attacks and Defense Approaches in MANETs, International Conference on Emerging Trends in Science, Engineering and Technology, 2012, 25-31

[3] Kasturiniva Das and Amar Taggu, A Comprehensive Analysis of DoS Attacks in Mobile Adhoc Networks, International Conference on Advances in Computing,Communications and Informatics (ICACCI), 2014, 2273-2278

[4] Kitisak Osathanunkul and Ning Zhang, A Countermeasure to Black Hole Attacks in Mobile Ad hoc Networks, International Conference on Networking, Sensing and Control Delft, the Netherlands, 11-13 April, 2011, 508-513

[5] Veronika Durcekova, Ladislav Schwartz and Nahid Shahmehri, Sophisticated Denial of Service Attacks aimed at Application Layer, IEEE, 2012, 55-60

[6] Ashish Kumar Jain and Vrinda Tokekar, Classification of Denial of Service Attacks in Mobile Ad Hoc Networks, International Conference on Computational Intelligence and Communication Systems, 2011, 256-261

[7] Ashok M.Kanthe, Dina Simunic and Marijan Djurek, Denial of Service (DoS) Attacks in Green Mobile Ad–hoc Networks, MIPRO 2012, Opatija, Croatia, May 21-25, 2012, 675-680