A Survey on DoS Flooding Attack in MANET

Vibha Tripathi[1], Mayuresh Kanher[2]
[1, 2] Department of CSE
[1, 2] GITS, Gwalior, India

Abstract- *An Adhoc network is a network in which nodes communicate without using any network infrastructure and move in random order. MANET (Mobile Adhoc Network) is an attractive technology for many applications, such as rescue and tactical operations, due to the flexibility provided by their dynamic infrastructure. MANET is an autonomous system of wireless mobile hosts without fixed network infrastructure and centralized access point such as a base station. The different routing attacks in MANET are flooding, black hole, link spoofing attack. In this present a survey on Flooding attack in MANET their security issues, attacks, characteristics and present the previous work in Dos flooding attack.*

Keywords- MANET, Dos, Flooding attack, Aodv.

I. INTRODUCTION

Mobile Ad hoc Network (MANET) [1] is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed.

Fig. 1 Example of a typical Manet

II. MANET CHARACTERISTICS

There are various characteristics of MANET includes:

1) Cooperation:

Manets rely on the cooperation of the nodes for routing and packet transmission. If the source and destination node are not in the range of each other then the communication between them takes place with the cooperation of other nodes. All the nodes between them form a optimum chain of mutually connected nodes. In this each node is to act as a host as well as a router simultaneously so this is also known as multi hop communication[2].

2) Dynamism of Topology:

The Manet nodes are random and unpredictable and so is the topology. The nodes may leave or join the network at any point of time also the topology is vulnerable to link failure, all these affect the status of trust among nodes and the complexity of routing.

3) Lack of fixed infrastructure:

The absence of a fixed or central infrastructure is a key feature of MANETs. There is no centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

4) Resource constraints:

MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring[2].

III. ROUTING PROTOCOLS IN MANET

Since MANETs has been in an active research area and in recent years many routing protocols have been introduced. A routing protocol specifies the communication which is carried out between the routers. The choice of that

route selection is done by the routing algorithm. These main routing protocols are divided into 3 categories-

- Proactive protocols/Table driven
- Reactive protocols/On-demand
- Hybrid protocols

1) Proactive routing protocol:

In proactive routing scheme every node continuously maintains complete routing information of the network. This information is stored in tables. Each node maintains a routing table which contains the list of destinations and routes.

2) Reactive routing protocol:

The reactive routing protocols are based on some sort of query-reply dialog. In this the nodes do not need periodic transmission of topological information of the network. When there is a need for a route to a destination, route request messages are flooded periodically with new networks status information. Every node in this routing protocol maintains information of only active paths to the destination nodes.

3) Hybrid Routing Protocols:

Often reactive or proactive feature of a particular routing protocol might not be enough. These protocols combined the features of both reactive and proactive routing protocols[2].

IV. SECURITY ISSUES

A crucial barrier with wireless network is its security. When data is transmitted there is always the probability that attacker nodes hacking the data and gain access to the network and misuse the data. For observing the certainty of ad hoc networks we required certain parameters. The basic parameters are:-

Availability: Availability means the information should be available when ever required.

Confidentiality: Confidentiality ensures that information must be confidential from unauthorized user.

Integrity: Integrity assures that a message is not modified by intruder.

Authentication: both the parties must be authenticating each other at the time of communication.

Non repudiation: Non repudiation ensures that sender and receiver of a message cannot deny that they have ever sent or received such a message.

Anonymity: Anonymity means all information about identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

Authorization: This property allocates different access goodness to many types of users[3].

V. ATTACKS IN MANET

Attack in MANET can be classified as

A. Active Attacks

Active attacks are the attacks in which attacker tries to disturb the performance of the network and also involves by modifying the data stream or creation of fake stream .Active attacks can be internal or external Internal Attack: Internal attack is from cooperate nodes which are actually part of the network. External Attack: External attack carried out by node that does not belong to the domain of the network.

1. Black hole attack:

The black hole attack is an active attack. It has two properties First is attacker sends fake routing information, declaring that it has the valid route from source to the destination, due to which other nodes in the network route the data packets through the malicious node. Second, malicious node targets the routing packets, drops them instead of normally forwarding them. The Figure is an example of black hole attack in the mobile ad hoc networks was source node A and F represents the destination node. Node B is a misbehaviour node who replies the RREQ packet which is sent from source node, and makes a fake response that it has the shortest route to the destination node. Therefore source node incorrectly looks towards the route discovery process with completion, and starts to send data packets to node B. In the mobile ad hoc networks, a malicious node i,e node B probably drops the packets which is send by source node. So this misguiding node can be regarded as a black hole problem in MANETs.

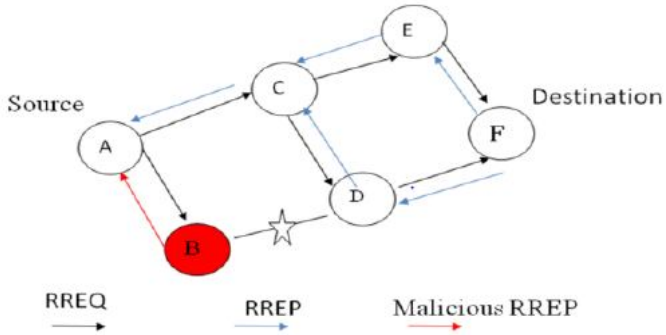

Fig 2 Black hole Attack

2. Flooding attack:

Flooding Attack can be begin by flooding the network with fake RREQ or data packet leading to the blocking of the network and reduces the probability of data transmission of the real node .Depending upon which type of packet used to flood in the network .it is classified into three categories are HELLO FLOODING,RREQ FLOODING And DATA FLOODING. HELLO FLOODING: Some routing protocols in wireless network require nodes to broadcast hello messages to announce themselves to their neighbours. A node which receives such a message may assume that it is within a range of the sender. Some misbehaving nodes in the network flood the Hello packet continuously. Without maintaining the hello interval. It creates the disturbances in the network operation. This activity diverts the legitimate node's action in the network. Figure 3 shows the hello flooding in the network.

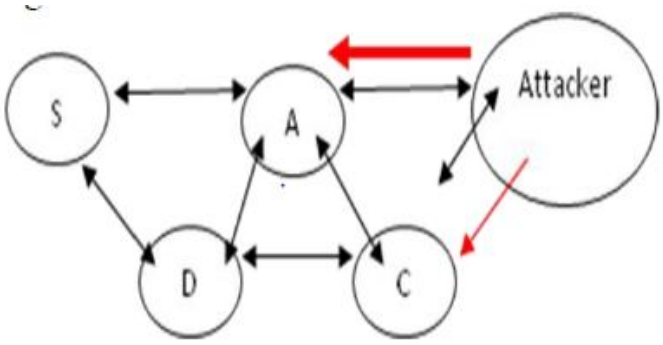

Fig 3 Hello Flooding attack

RREQ FLOODING: In this type of flooding attack, the attacker broadcast many RREQ packets for the node which exist or not exist in the network. TO perform RREQ flooding the intruder disable the RREQ rate so it will effect on to consumes network Bandwidth.

DATA FLOODING: In Data flooding data packet are used to flood the network. In this flooding malicious node builds a path to all the nodes then send the large amount of fake data packet and this fake data packet fail the network resources so it will very hard to detect.

3) Denial of service attack:

The goal of a denial of service attack is to reject valid user's access to a particular resource. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

4) Distributed Denial of Service

Distributed Denial of service has the cohesive strength of many compromised systems working towards a single cause. The first stage of this attack is to build its platform with many host systems that can work under remote commands. The attacker group would first scan networks to hunt for vulnerable systems that are weak in security features. According to researchers there are millions of host machines that are vulnerable without secure patches and proper updates that often fall victims to these attackers. Once the scanning procedure is completed, attackers would bring these hosts into control using software exploitations like buffer overflow, dangling pointers, code injection etc. Special root kits are also used in many cases that are installed in a host system to incur these software exploitations. After having sufficient hosts under control, attackers also create backdoors that allows special access that is used for future entry. The attackers also update the hosts and tighten its security so that another attacker does not use the same host. Any future entry would be done using the back entry that has been specially crafted.

5) Gray-hole attack:

This attack is also known as routing misbehaviour attack which show the way to dropping of messages. Gray hole attack has two phases .In the first phase the node itself advertise having a valid route to destination while in second phase, nodes drops interrupt packets within a certain probability As soon as it receive the packet from neighbor the attacker drop the packet.

6. Byzantine Attack:

In this attack an intermediate node or a set of intermediate nodes work in collusion and carry out attacks such as creating routing loops, forwarding packets on non – optimal path which results in degradation of the routing system.

7. Selfish Nodes:

In this selfish node is not helping to communicate with other nodes which are taking part in the network. But malicious node which is not taking part in network operations, use the network for its advantage to save its own resources.

B. PASSIVE ATTACKS

A passive attack is an attack categorized by the attacker listening in on communication. In such an attack, attacker does not try to break into the system or otherwise change data.

1. Traffic Monitoring: Traffic monitoring specifies for MANET and also other wireless network such as cellular, satellite and WLAN to developed or identify the communication and functional information for the launching of attacks.

2. Eavesdropping: The main goal of eavesdropping is to obtain some confidential information that should be secret during communication. This confidential information may include the location of public key or private key and also the password of the nodes

3. Traffic Analysis: Traffic analysis is a passive attack used to increase the information from which node can communicate with each other and also how data should process.

VI. AODV

AODV (Adhoc On-demand Distance Vector) is a reactive routing protocol, but it is basically an improvement of DSDV routing protocol which is proactive protocol. It initiates route discovery process routes only when there is any need to find node. AODV can handle low, moderate, and relatively high mobile rates, together with a variety of data traffic loadings. However, it makes no provisions for security. In Route Discovery Process of AODV there are types of messages: Route Request (RREQ), Route Reply (RREP), and Route Error (RERR) messages. A source node broadcasts a RREQ message by route discovery process whenever it wants to communicate to destination node but does not have a fresh route to the. All the intermediate nodes that receive this RREQ message either send a RREP to the source node or forward the RREQ message to the other nodes. RREP message is send only when the intermediate nodes have a fresh route to the destination node and the "destination only" flag is not set. If the request packet has been forwarded by this intermediate node before, it is silently dropped. When the destination node receives a RREQ for itself, it sends back a RREP message on the reverse route. The requesting node and the nodes receiving RREP messages on the route update their routing tables with the new route. A route generates a RERR message either a route breaks or it does not have a route to the destination to which the packet is to be send.

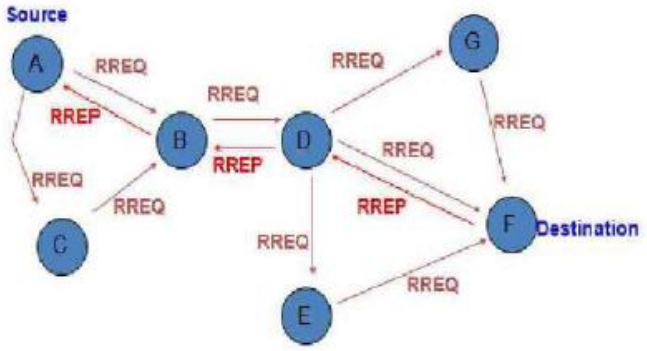

Fig. 4 Example of a AODV Routing Protocol

VII. LITERATURE REVIEW

In Fan Hong, Yu Zhang and Jian-Hua Song [4], the author planned the new methodology to conflict the flooding attack. In this technique they implementing two thresholds value namely, ratelimit and blacklist limit. If no. of RREQ is less than ratelimit then the request succeeded else check it is less than blacklist limit or not. If yes then make node black listed but if the no. of nodes greater than rreqlimit and less than blacklistlimit then place the RREQ in the delay queue. Then process after time out occurs. These techniques can handle the network with high mobility.

In Venkat Balakrishnan, Vijay Varadharajan and Uday Tupakula [5], they analyzed the flooding attack in unidentified communication. In this technique mainly three components are used: blacklist threshold, whitelisting threshold and transmission threshold. Efficiently recognize & reject the nodes which flood the network. In this unidentified network it's impossible to track back destination and source nodes.

In M. Pushpalatha, T. Rama Rao and Revathi Venkataraman, [6], they presented the extended AODV protocol based on the trust factor. In this technique, authors

have categorized the nodes in three categories based on the trust value: Friends, acquaintance and stranger. Friends are trusted nodes, Stranger are non trusted nodes, and which has the trust factor less than the friends and greater than the stranger its called acquaintance. This technique does not work with higher node mobility.

In Komal Joshi and Veena Lomte [7], the author introduce a node-to-node verification technique using challenge-response protocol and MNT (Malicious Node Table). Challenge- response protocol(CRP) checks genuine node flooding from malicious node and MNT (Malicious Node Table) used for storage information about malicious node noticed by CRP. AODV routing protocol is used for packet forwarding and security will be maintained by MNT. The aim of this technique is to provide node accessibility and better security for packet transfer in MANET. It does not provide better packet delivery ratio, throughput and control overhead.

In Kashif Laeeq [8], author introduces RFAP technique for transforming the RREQ (route request) flooding attack on AODV protocol in MANET. The result analysis shows that, the RFAP technique can identify the malicious flooder node and protects the network properties from flooder or attacker node (flooding attack). At the time of flooding attack, original AODV protocol can create defective result compare to RFAP technique. RFAP technique can easily find the flooder or attacker node and defend the network from RREQ flooding attack.

VIII. CONCLUSION

Due to the absence of any centralized authority the mobile ad hoc network suffers from many security attacks as the wireless link is accessible to all. Flooding attack in MANET results in degradation of throughput, exhaustion of battery power, and wastage of bandwidth. In this present a survey on Flooding attack in MANET their security issues, attacks, characteristics and present the previous work in Dos flooding attack.

REFERENCES

[1] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.

[2] Supriya Tayal 1, Vinti Gupta 2 “A Survey of Attacks on Manet Routing Protocols” International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 6, June 2013

[3] Khushboo Sawant, Dr. M.K Rawat “ Survey of DOS Flooding Attacks over MANET Environment” Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 5(Version 6), May 2014, pp.110-115

[4] Jian-Hua Song, Fan Hong and Yu Zhang, “Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks”, IEEE, 2006.

[5] Monu Singh,Ajay Singh,Rajesh Tanwar and Ritu Chauhan, "Security Attacks in Mobile Adhoc Networks",International Journal of Computer Applications(IJCA), 2011.

[6] Venkat Balakrishnan, Vijay Varadharajan ,and Uday Tupakula” Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications”, IEEE, 2007.

[7] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, “Performance Analysis of Flooding Attack Prevention Algorithm in MANETs”, International Scholarly and Scientific Research and Innovation, pp. 421-424, 2009.

[8] Ms. Neetu Singh Chouhan and Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", in International Journal of Computer Technology and Electronics Engineering (IJCTEE), pp. 68-72, November 2011.