ISSN:0975-9646

Study of Various Attacks in MANET and Elaborative Discussion of RREQ Flooding Attack and Its Solutions.

[1] Neha Kamdar, [2] Vinita Sharma, [3] Poorva Kakani

Department of Computer Science & Engineering

***Abstract*: One of the majority up-and- imminent fields for research is mobile ad hoc network. Mobile means moving and ad hoc means temporary devoid of every fixed infrastructure. Security is high main concern obligation in wireless ad-hoc network. In ad hoc network the communicating nodes sets novel challenges for the security style because it doesn't unavoidably supply on fixed infrastructure. In the ad-hoc network denial of service attacks (DOS) convincingly start through malicious nodes or attacker which is more vulnerable. Black whole, Gray hole, Worm hole, Flooding is such type of security threats that affects the network. This paper presents a review on MANET, types of attacks .Here we are clarify the event of flooding attack and their exposed to the possibility of being attacked or harmed effects which give chance to a genuine node for doing dissimilar attacks also. So we get going towards is to recognize the presence or existence of RREQ flooding attack using secure routing protocols and Technique which can easily find the attacker node and protects the network from RREQ Flooding attack.**

Keywords: **Wireless network, MANET (Mobile Ad-Hoc Network), Flooding Attack, , Routing Protocols, Security**

I. INTRODUCTION

In Mobile ad-hoc network (MANET), every mobile terminal is an autonomous node. Hence, hence, it worked as each host and router. Networks are self-organizing network of mobile nodes that use wireless links to form a network [1].MANET acts as light weighted terminal with less CPU processing capability, small memory size and less power Storage. MANET does not provide centralized Control. MANET distributes the control and management of the network among the nodes. Since the nodes are mobile, the network topology may change quickly and MANET acts as a dynamic network topology.

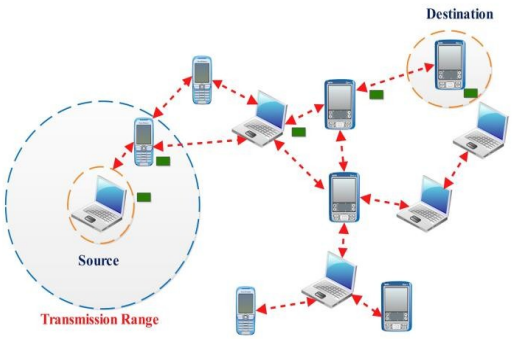

Fig 1: MANET Network

Since MANET allows the devices to maintain connection and also to add or remove the node from the network, it can easily used in the military battlefield to maintain the information network between the solider and vehicle as well as in commercial sector such as disaster relief effort for eg. Fire, flood or earthquake, etc. MANET is also used in personal area networking. MANET has some limitations like limited resources and physical security. It is also hard to detect the malicious node because of its volatile network topology. There are some major issues involving in MANET such as broadcasting, clustering, mobility management, bandwidth management and power management.

This network is a momentarily network that can be destroyed anytime. This network formed dynamically and share common wireless link. As in tradition networks there is not basic fixed structure. Nodes are free to move randomly and can leave or join the network on the fly. In MANET each node works as both host and route. A mobile ad hoc network (MANET) is a group of mobile devise connected by wireless link without the requirement of fixed common infrastructure in place like wireless access point or base station point.

Wireless link in MANET make them more likely to attack. It is easier for hacker to attack this network easily and gain access to private information. They can directly attack the network to delete message, add malicious messages, or masquerade as a node. These violate the network goals of availability, authenticity, authorization, integrity and confidentiality [2].

The mobile ad-hoc networks diverge from already present networks by the fact that they don't depend on fixed infrastructure [3]. As in ritual networks there is no basic fixed structure but in MANETs nodes are free to move randomly and can leave or join the network on the fly. In MANET every single node works as host and route. A mobile ad hoc network is an assembly of mobile nodes attached by wireless link without the necessity of stationary infrastructure in place like wireless access point or base station point.

II. VARIOUS ATTACKS IN MANET

Attack in MANET can be classified as-

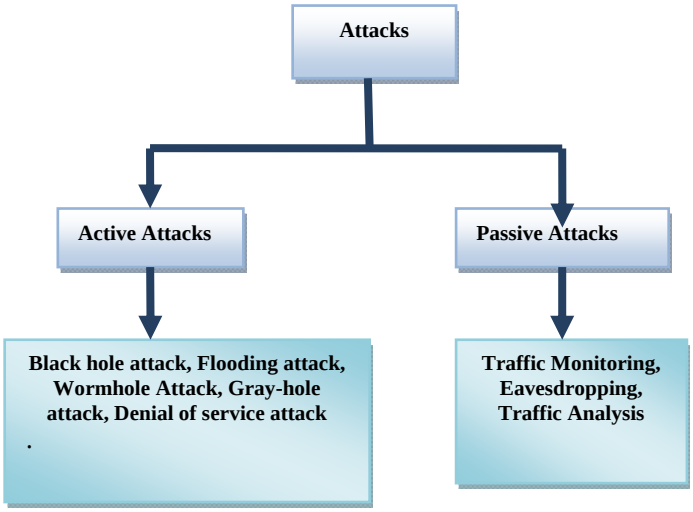

Fig 2. Classification of MANET Attacks

A. Active Attacks

Active attacks are the attacks within which attacker tries to disturb the performance of the network and involves by modifying the data stream or creation of bogus 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.

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 two categories are RREQ FLOODING and DATA FLOODING.

- **RREQ FLOODING**

In this type of attack, the flooder node broadcast several RREQ packets for the node which exist or not exist in the network. To complete RREQ flooding the attacker deactivate the RREQ rate so it will consumes network bandwidth. 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.

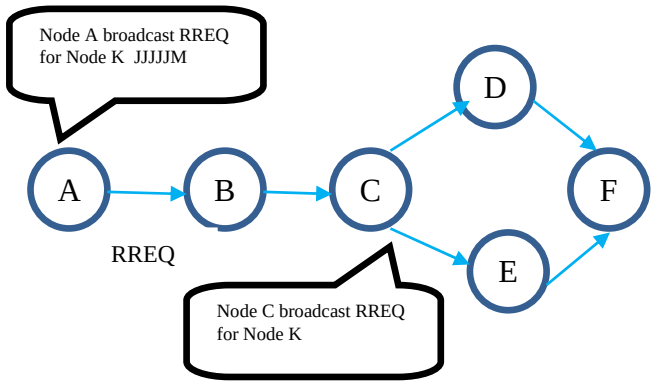

Fig 3. RREQ Flooding Attack

- **DATA FLOODING.**

In this type of attack, data packets are used to flood the whole network. The attacker or flooder node, construct a route towards all the node then send the huge quantity of fake data packet and this bogus data packet fail the network resources so it will be hard to detect the flooder node. 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.

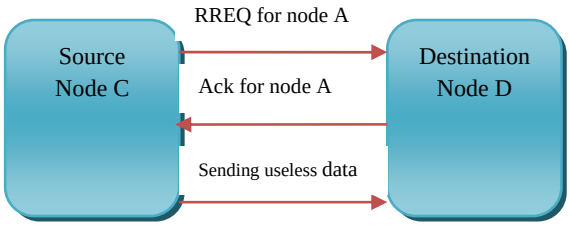

Fig 4. DATA Flooding Attack

3. Wormhole Attack: In a wormhole attack, an attacker receives packets from one location in the network, tunnel" them to another location in the network, and then repeat them into the network from that location.. This tunnel between two colluding attacks is known as a wormhole In DSR, AODV this attack could prevent discovery of any routes and may create a wormhole even for packet not address to itself because of broadcasting. Wormholes are hard to detect because the path that is used is not part of the actual network.

4. 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.

5. Gray-hole attack: This attack is also known as routing misbehavior 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.

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. [9].

III. CLASSIFICATIONOF MANET PROTOCOL

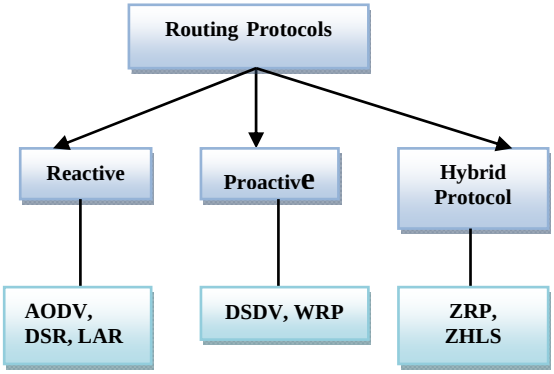

Fig 4. Classification of MANET routing protocol

A. Reactive protocols

Reactive protocols additionally referred to as on demand driven protocols as a result of they discover route only if it's on demand. It solely establishes the route once supply node within the network desires to send a message or a packet to destination node. the most factor of this protocol is that it reduces routing table once it's overflow however the unhealthy factor is that longer delay has been seen because it is on demand the instance of this kind of protocol are DSR (dynamic supply routing), AODV (ad hoc on demand distance vector routing), LAR (location Aided Routing), TORA (temporally ordered routing algorithm).

B. Proactive Protocol

Proactive protocols are known as table driven routing protocol as a result of they maintain the routing table of the complete network. In proactive every node needs to maintain its tables for storing routing info and additionally update the table i,e changes is completed whenever the network changes. If any changes in topology as every node can send a broadcast message to entire network therefore it'll have an effect on the routing table for maintaining the routing entries. for giant network proactive routing protocol not be instructed as a result of for every node maintaining the table causes a lot of information measure consumption and overload to routing table .the samples of proactive routing protocol area unit DSDV (destination sequence distance vector) and OLSR (optimised link state routing)

C. Hybrid protocols

It is a mix of each reactive and proactive routing protocol. To beat the weakness of reactive and proactive routing protocol the hybrid is generally used. In hybrid routing protocol network is split into zones. It's the foremost appropriate routing protocol amongst all. The examples of hybrid protocols are ZRP (zone routing protocol), ZHLS (zone based hierarchical state). [9]

IV. RELATED WORK

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, rate limit and blacklist limit. If no. of RREQ is less than rate limit 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 rreq limit and less than blacklist limit 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, white listing 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 introduces 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. The RFAP technique cannot stop the illegal data packets.

V. DETECTION AND PREVENTION TECHNIQUES OF FLOODING ATTACK

1) Node to Node Authentication using Challenge Response Protocol Technique [7]

In this paper introduce a node-to-node verification technique using challenge-response protocol and MNT (Malicious Node Table). Challenge- response protocol 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.

2) Trust Estimation Technique [6]

A trust estimator is used in every node to estimate the trust level of its neighboring nodes. The trust level is a function of various factors like, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor average time taken to respond to a route request etc. This technique proposed a distributive approach to identified and prevent the flooding attack. The efficiency of the proposed technique depends on the range of threshold value.

3) RREQ Flooding Attack Prevention (RFAP) Technique [8]

This technique, RFAP for mitigating the RREQ flooding attack in MANET by utilizing AODV protocol. The result shown that the RFAP technique can easily find the attacker node and protect the network from RREQ flooding attack. The RFAP technique cannot stop the illegal data packets.

4) Effective Filtering Technique [4]

The author proposed the distributive approach to resist the flooding attack. In this method they have used the two threshold value; RATE_LIMIT and BLACKLIST_LIMIT. If RREQ count of any node is less then RATE_LIMIT then the request is processed otherwise check whether it is less then BLACKLIST_LIMIT, if yes then black list the node but if the count is greater than RREQ_LIMIT and less than BLACKLIST_LIMIT then put the RREQ in the delay queue and process after queue time out occurs. These methods can Handel the network with high mobility.

VI. CONCLUSION

Security attacks like black hole, gray hole, wormhole and flooding attacks are analyzed. Flooding attack in MANET results in exhaustion of Battery power, degradation of throughput and wastage of bandwidth. In this paper, we have analyzed Different types of attacks and routing protocols, here briefly discussed on one of the crucial security attack in MANET i.e. RREQ Flooding Attack and Different techniques to detect and prevent flooding attack. Discussion of techniques presented in this paper is helpful to design secure techniques for flooding attack.

REFERENCES

[1]. Pradip M. Jawandhiya and Mangesh M. Ghonge, “A Survey of Mobile Adhoc Network Attacks”, International Journal of Engineering Science and Technology, Vol. 2(9), pp. - 4063-4071, 2010.

[2]. A. Mishra and K...M.Nadkarni, Security in Wireless Ad –hoc Network, in Book. “The Hand Book of Ad Hoc Wireless Networks” (chapter 30) , 2003.

[3]. Pradip M. Jawandhiya and Mangesh M. Ghonge, “A Survey of Mobile Adhoc Network Attacks”, International Journal of Engineering Science and Technology, Vol. 2(9), pp.-4063-4071, 2010.

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

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

[6]. 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.

[7]. Komal Joshi Veena Lomte, “Preventing Flooding Attack in MANET Using Node-to-Node Authentication”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, pp. 136-140, November 2013.

[8]. Kashif Laeeq,"RFAP, A Preventive Measure against Route Request Flooding Attack in MANETS", IEEE, 2012.

[9]. Shruti Bhalodiya, Krunal Vaghela, “Study of Detection and Prevention Techniques for Flooding attack on AODV in MANET”, International Journal of Science and Research (IJSR) Volume 4 Issue 1, January2015.