Types of Flooding Attacks in MANET

Miss. Vrushali B. Mankar, Dr. Makarand R. Shahade , Mr. Swapnil V. Bamb, Mr. Chetan J. Ghyar
[1]IT department, J.D.I.E.T , Yavatmal, Maharashtra, India
mankarvrushalib@gmail.com
[2]IT department, J.D.I.E.T , Yavatmal, Maharashtra, India
makarandshahade@rediffmail.com
[3]IT department, J.D.I.E.T , Yavatmal, Maharashtra, India
swapnilbamb4444@gmail.com
[4]IT department, J.D.I.E.T , Yavatmal, Maharashtra, India
chetanjghyer @gmail.com

ABSTRACT

The Mobile Ad-Hoc Network (MANET) is open, infrastructure-less wireless network which composes a set of mobile, decentralize and self organized nodes. In MANET each node has the freedom to connect with other nodes, to leave that node and to move freely in the network. As the mobile ad-hoc network has no fixed infrastructure or it is a central administration, the relative communication issues arrived in network are more complex as compared to cellular network. In that case as the nodes in the mobile ad hoc network any type of secure protection, it has no physical protection for unaware attacks. Hence the node of the mobile ad-hoc network is easily influenced by any type of networking attacks. The nodes are particularly to be exposed by denial of service (DOS) attacks which are launched through unauthorized disclosure. The new DOS attack, called Ad-Hoc Flooding Attack (AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV, DSR. The intruder transmits all data packets to drain the communication bandwidth and node information, so that valid communication cannot establish over the network.

In this paper we are discussing about flooding attacks and other attacks which may harm the network by their presence in the network. So we continue to detect such types of flooding attacks in MANET.

Keywords: Mobile Ad-Hoc Network (MANET), Ad-Hoc Flooding Attack (AHFA), Denial of Services (DOS).

I. INTRODUCTION

Mobile ad-hoc network is the autonomous infrastructure system mobile nodes in which nodes are connected in wireless network. Each node in the network act as an a router in the MANET. Mobile ad-hoc network (MANET) gives the flexibility of using network to transmit or receive the data in the large network without the use of fixed infrastructure such as base stations. Each node having the ability to reconfigure the network topology means that they can discover new path when link breaks or node can move due to mobility. In this way the networks can work in standalone fashion and number of nodes or users can connected freely in large internet network. The mobile ad hoc networks have several salient characteristics, such as Dynamic topologies, Bandwidth-constrained, variable capacity links, Energy-constrained operation, limited physical security. Due to such features mobile ad-hoc network is most likely to be exposed to the chance of being attacked.

In this paper we are discussing about new type of attack that is Ad-Hoc Flooding Attack (AHFA), which results in Denial of Service (DOS) attack used against previously version of all ad hoc network protocol. In this attack, the attacker either broadcast number of route request packets for node IP who is not in the network so as to block that path. To defend routing protocol against the Ad-Hoc Flooding attack, we provide solution called Flooding Attack Prevention (FAP), which can be applied to the AODV protocol to allow that protocol to resist from blockage of route.

The flooding attack is also found in the wired networking, which is popularly known as SYN Flooding Attack. In this attack the attacker sends many TCP connection requests with malicious source address to the victim's machine. Each request causes the targeted host to exemplify data structure out of pool resources. The goal of SYN flooding attack is to consume more resources at the receiving side of data. The SYN flooding attacks on transport layer and ad hoc flooding attack's on network layer.

In this paper we find out the information about such ad hoc flooding attack and other types of attacks which is harmful to the network.

II. TYPES OF SECURITY ATTACKS

The mobile ad-hoc network is most commonly to be exposed to the chance of being attack by two different level of attack. The first level of attack is simple mechanism of routing and second level of attack is for damaging the security of the network. The attacks in MANET are mainly classified as follows:

A) Internal Attack:

In internal type of attack, the attack is initiated by trusted node present in that network and it might come from unauthorized disclosure and improper node.

Internal nodes are identified by unauthorized disclosure if the external attackers influenced the trusted node present in the network. The security necessity of the network like authentication, confidentiality and integrity on server side are more likely to be exposed

1) Active Attack
2) Passive Attack

1) Active Attacks

In this type of attack, the attacker reduces the level of performance of the network and also modified the actual data transmitted by sender node to the receiver node. The active attack further classified into two types as internal active attack and external active attack.

The name implies that the internal attack obtained by the node that are part of the network and external attack carried out by the node which are not part of the network.

2) Passive Attack

In this type of attack the attacker present like a malicious user which only listen the communication between the nodes and not do any type of modification in the data.

Denial of Service Attack

The main objective of denial of service attack is to refuse to accept the request of valid client to access the network resources. In DOS attack, the attacker usually send the deficient massages asking the network or valid server to accepting the requests that have invalid return addresses. The server or network then will not be able to find to the chance of being harmed in ad hoc networks with unauthorized disclosure because communication keys used by these nodes might be stolen and forwarded to the other attackers. In this way the attack by internal node is difficult to prevent.

B) External Attack:

The external attacks are the type of attack which is launched by opponent who are not authorized user to participate in the network operations. These types of attacks have aim to create network blockage, not allowing to access to specific function or to disturb the whole network system. The fake packets injection, Denial of Services are some types of attack initiated by the external attackers. The external attack further classified into two types as follows:

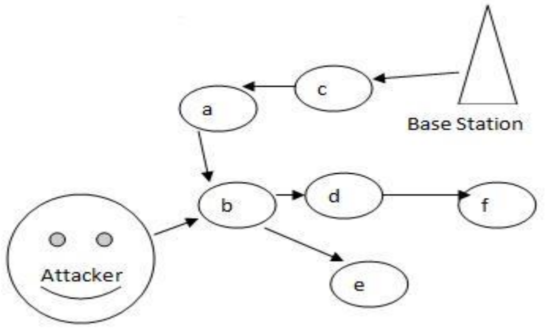
Out the return address of the attacker when sending the authenticated massage approval, reason for the server to wait before closing the connection. Even the server closes the connection, attacker till sends the authenticated massage with invalid return address. In this way the process of sending authenticated massage and waiting of server will begin again, by keeping network or sever continuously busy.

FLOODING ATTACK

Flooding is a active type of attack in which attacker uses all the resources of the network, broadcast the false packets to all over the network to drained the available resources and reduce the throughput of the network so that the valid user cannot able to use the network resources for better communication. Flood attack possibly found in most secure on demand routing like AODV, SRP, ARAN etc. Flood attacks occur when a network or service become so weight down with packets providing incomplete connection requests that it can no longer to be established proper connection requests. By flooding server or user with connections that cannot be completed, the flood attack eventually fill the user buffer. Once the buffer become full no further connections can be made and that the result is Denial of Service. The flooding attack broadly classified into following types as follows:

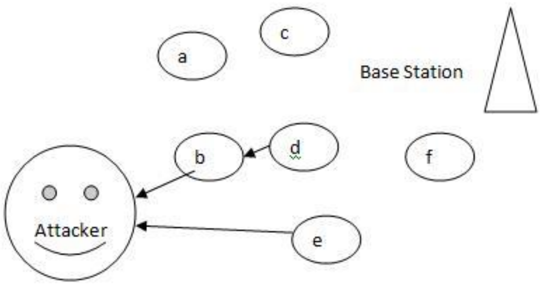
A. Hello Flooding

The attacker node broadcast hello packets with high transmission power. Therefore all the other nodes present in the network assume that the attacker node is trusted parent node and start forwarding packets towards this node hoping that it is the valid root reach to the destination. This will lead to increase in delay in the network and convinced other node that this attacker node is trusted neighbor node, so that all the other nodes respond to the HELLO massage and waste their energy shown in the Fig1. Here the attacker node then further play an attack as its power overpowers other transceivers.



Here the attacker broadcasts HELLO packet with very high transmission power than the base station

Fig.1 HELLO Flooding broadcast mechanism



Here the authentic node consider the attacker parent as well as trusted neighbor and starts forwording packets.

Fig.2 HELLO Flooding packet transmission

B. RREQ Flooding

In this type of attack, the attacker selects IP addresses which are not part of the network and transmit number of RREQ packets towards that IP address as shown in the fig.3. In the route discovery process client node transmit RRQE packets over the network. The priority of the RRQE packet is much more than data packets so at high load also RREQ packets are broadcasted. In Fig3.the attacker deactivates the RREQ rate so that it consumes more bandwidth.

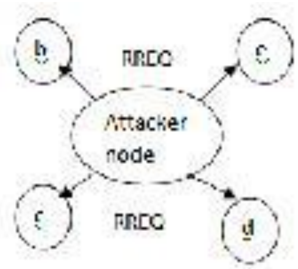


Fig. 3 RREQ mechanism

C. Data Flooding

In this attack, malicious node first constructs a path belonging to all nodes and starts sending useless data packets to consume the network bandwidth as shown in fig. 4.In this case these useless data packets consumes the network resources and hence the trusted user cannot be able to use network resources to establish valid communication. It large network is hard to detect the data packets present in that network.

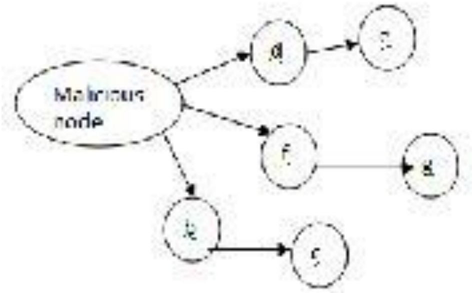


Fig. 4 Data Flooding mechanism

D. SYN Flooding

The attacker sends large number of synchronized packets to the destination node and this result in large amount of memory being consumed. After the IP address of respective client is spoofed, the attacker or malicious node treat itself as the original or trusted client node and starts sending the SYN massage to the server, then the server replied to that malicious node by sending SYN ACK massage. Without knowing about original client node, malicious node again and again will keep on send the SYN massage instead of final ACK to the server and makes the connection half open as shown in the Fig. 5, where the server will also continuously reply by sending SYN ACK to the malicious client and store the repeated information in its buffer. At one point of time the buffer becomes full and server couldn't reply to other client's request. Therefore the entire session gets refuse to give result.

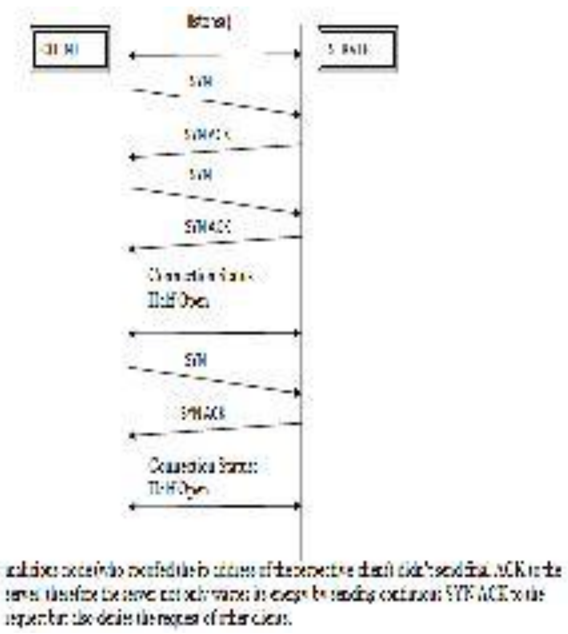


Fig.5 SYN Flood mechanism

III. CONCLUSION

In this paper, we in short discuss about some important security attacks in MANET i.e. DOS Flooding and some other types of flooding attacks and also the characteristics of such attacks. As we seen in the paper that all the attacks impact on network are different according to their characteristics. In our future work, we will develop and work on Flooding Attack Prevention (FAP) scheme to improve its attack prevention rate against larger number of collaborate flooded packets and also enhance the security features of FAP, so that we protect network from any types of attacks and enhanced communication standard.

REFERENCES

[1] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, A New Routing Attack in Mobile Ad Hoc Networks, published in International Journal of Information Technology Vol. 11 No.2,,pp.83−94.

[2] Abhay Kumar Rai ,Rajiv Ranjan Tewari and Saurabh Kant Upadhyay, Different Types of Attacks on Integrated MANET-Internet, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3), pp 265-274

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, And Nei Kato, IEEE Wireless Communication October 2007,,pp.85−91.

[4] Yi-an Huang and Wenke LeeE. Jonsson et al. (Eds.): Springer-Verlag Berlin Heidelberg 2004RAID 2004, LNCS 3224,pp.125–145,2014.

[5] Kavuri Roshan1 , K.Reddi Prasad2 , Niraj Upadhayaya3 & A.Govardhan4, International Journal of Computer Science & Information Technology (IJCSIT) Vol4, No 3, June 2012, pp. 25-34.

[6] YihChun Hu , Adrian Perrig, David B. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network routing Protocols; September 19, 2003, San Diego, California, USA.