Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Flooding Attack on MANET – A Survey

[1]C.M. Nalayini, [2]Dr. Jeevaa Katiravan and [3]Arvind Prasad. V
[1,2]Assistant Professor-IT, [3]UG Scholar
[1,2,3]VEC-Chennai, TamilNadu, India

***Abstract*--** A Mobile Adhoc Network is a infrastructure-less network of mobile devices that is self-configuring and is connected wirelessly. The communication in MANET functions properly only if the participating nodes cooperate in routing without any malicious intention. Since a MANET does not have any infrastructure sudden flooding would result in performance degradation and would result in the termination of the communication taking place. This research paper analyses the impact of flooding on MANET.

***Keywords*--** *MANET, RREQ, Hello, SYN, Data, ICMP, UDP flood.*

I. INTRODUCTION

A Mobile Adhoc Network (MANET) is a network of mobile devices connected through a wireless link as shown in Fig1. Each node works as a router and a host for forwarding and receiving packets. A MANET may be suitable for networks within an Airport, meeting rooms, military arenas etc. The nodes have a dynamic topology and hence are free to join or leave the network and so the links change frequently.

Due to its dynamic nature a MANET is vulnerable to different attacks and mainly it gets affected by DDOS attacks.

The advantages include low cost, small size, high level of convenience, and support for different devices and so on. Lack of security, link failure and power constraints are the major disadvantages. Other major issues include broadcasting, clustering, mobility management, power management and bandwidth management. There are various types of attacks that try to degrade the network performance. In a flooding attack a network is overloaded with unnecessary packets initiating a request for a link that it can no longer process authentic requests. Flooding results in traffic and network congestion and result is Denial of Service (DOS).

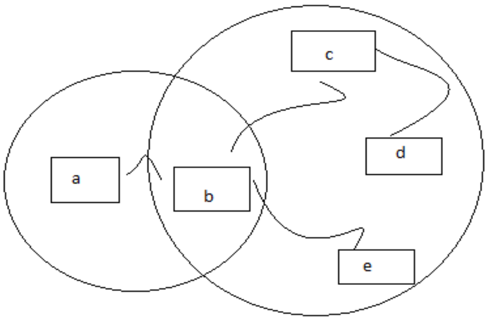


Figure 1: Mobile Adhoc Network

II. PROPERTIES

MANET has several significant properties, a few of them are listed below:

Mobility: Nodes can travel freely and hence the topology should accommodate all types of links.

Self-Configuration: Nodes have the ability to reconfigure the network topology i.e. they can discover new paths when links break or when nodes move due to mobility.

Energy Constrained Operation: Each node in a MANET relies on an exhaustible source of energy such as batteries for power.

Absence of Centralized Router: In Mobile Adhoc network each node acts as routers because every node moves independently from one location to the other pertaining to dynamic topology

III. ATTACKS

Adhoc networks are vulnerable to two different levels of attack. The first level attack is on basic mechanisms like routing and the second level attack is for damaging the security mechanisms. The attacks in MANET are broadly classified into:

1. Active Attacks
2. Passive Attacks

A. Active attacks

Here the attacker degrades the performance of the network and also modified the data stream. Active attacks are further classified into internal attacks and external attacks.

As the name suggest internal attack is carried out by the nodes that are a part of the network and external attacks are carried out by nodes that are not a part of the network.

B. Passive attacks

In a passive attack the attacker listens to the communication between the nodes. The attacker does not break into the system nor meddle with the data.

IV. PROBLEM STATEMENT

Flooding is an active attack wherein the main aim of the attacker is to disrupt the performance of the network by sending fake packets. As a result of this legitimate requests are not handled by the server since it is bombarded with both genuine and fake requests. Therefore it is necessary to have efficient prevention and detection mechanism to overcome flooding attacks in order to improve network performance.

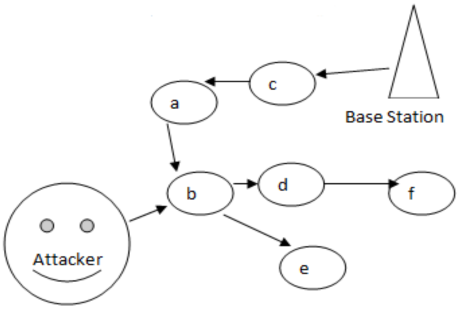
V. FLOODING ATTACK

Flooding attack is a type of active attack in which attacker exhausts the network resources, such as bandwidth, consumption of node resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance

A flood attack occurs when a network is unable to process genuine requests since it is weighed down by invalid requests. This eventually fills a host’s memory buffer. Once this buffer is full, connections can no longer be made and this results in DOS. A Flooding attack is broadly classified into the following types:

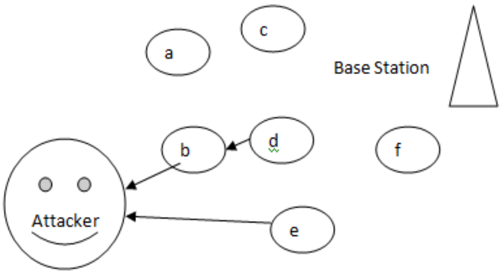
A. Hello flooding

The attacker node broadcasts a hello packet with very high power (powerful transmitter). Therefore the other nodes in the network assume that this attacker node is the parent node and starts forwarding packets towards this node hoping it to be the best route to the destination. This will lead to increase in delay in the network and also convince the other nodes that this attacker node is their neighbour, so that all the other nodes will respond to the HELLO message and waste their energy as shown Fig 2a and ab. The attacker node performs a selective replay attack as its power overwhelms other transceivers



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

Figure 2: Hello Flooding broadcast mechanism



Here the legitimate nodes consider attacker as the parent as well as neighbor node and start forwarding the packets

Figure 3: Hello flooding packet transmission

B. RREQ flooding

The attacker selects IP addresses that are not a part of the network and broadcasts several RREQ packets as shown in Fig 3. The attacker deactivates the RREQ rate so this consumes more bandwidth.

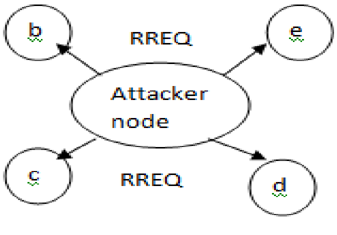


Figure 4: RREQ mechanism

C. Data flooding

In this attack, malicious node first construct path to all the nodes and then starts sending useless data packets to exhaust the network bandwidth as shown in Fig 4. It is hard to detect the data packet.

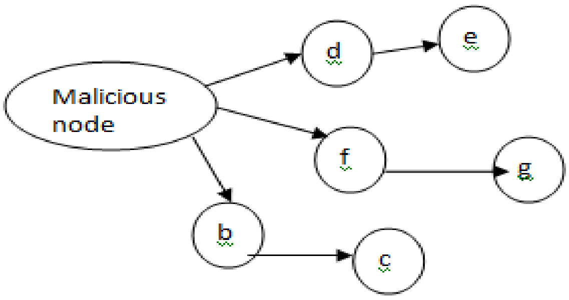
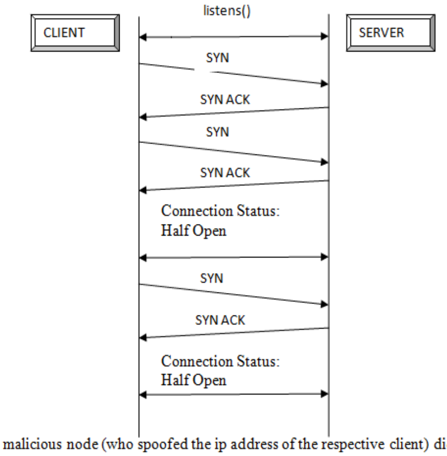


Figure 5: Data flooding mechanism

D. SYN flooding

The attacker sends a large amount of synchronization packets to the destination node and this result in a large amount of memory being consumed. After the IP address of the respective client is spoofed, the attacker or malicious node treat itself as the original client node and starts sending the SYN msg to the server, then the server will reply the malicious node by SYN ACK. Without the knowledge of the original client node, again and again the malicious node will keep on send the SYN msg instead of final ACK to the server and makes the connection half open as shown in Fig 5, thereby the server will also do continuous reply by sending SYN ACK to the malicious client and update the repeated information in its buffer. At one point of time the buffer becomes full and the server couldn't reply for other client's request. Therefore the entire session gets denied.



malicious node (who spoofed the ip address of the respective client) didn't send final ACK to the server, therefore the server not only wastes its energy by sending continuous SYN ACK to the request but also denies the request of other clients.

Figure 6: SYN Flood mechanism

E. ICMP (Internet Control Message Protocol) flooding

An attacker generates a stream of ICMP ECHO packet [12] to target the victim node. Thereby the victim wastes its power and network resources by sending replies to all the ICMP requests.

F. UDP flooding

In this attack, the attacker sends n number of UDP packets to the victim in order to overwhelm the victim's network bandwidth [12]

VI. RELATED WORK

[1]In this paper the author suggests a packet filtering firewall to provide a defence against flooding. A firewall is used to monitor incoming and outgoing traffic and acts as a barrier between an internal and external network. Even though this method protects the network from unauthorized access, sometimes the traffic can't be denied.

[2]The author specifies an incentive mechanism based on reputation and trust to detect and prevent flooding. Initially the trust value is 1 and is increased/decreased based on the node's behaviour. This results in improved packet delivery ratio, throughput and reduced routing overhead. But network overhead is high.

[3]Here the author uses a filtering technique with a threshold value of 10.As a result of this there is increased throughput and effective packet delivery fraction. But the timeout is increased if the blacklisted node misbehaves again.

[4]Here the author(s) uses prediction and pre-processing method to detect errors. The node collects information and monitors the traffic and takes a decision when there is an abnormal increase. Traffic analysis is very effective, but periodic traffic monitoring should be done, if not a malicious node may surface again.

[5]In this paper a node to node verification is performed using a Malicious Node Table and challenge response protocol. Security will be maintained with the help of MNT. It does not provide better packet delivery ratio, throughput and also fails to control overhead.

[6]The broadcast of IP address is disabled. This improves the performance affected by flooding attack. Packet delivery ratio doubles and number of collisions is reduced by half using this method. But Computational complexity is more.

[7] Here the author(s) uses PDS(Profile based Detection Scheme) approach where dynamic profile based traffic analysis is done to detect misbehaving nodes and isolate them at a faster rate. Detection phase detects the malicious node which sends the bogus RREQ packets, with the help of threshold value, rate limit parameter is stored in profile table of each node and updated dynamically through hello message. . Every receiving node should check with its profile table before forwarding the RREQ to its neighbour node so that the malicious node would easily been identified at a faster rate and isolate it from participation in the network. If the profile table is not protected with strong password then attackers will easily access the information. The threshold values should be dynamic enough to detect the attacker as the earliest stage otherwise there is a chance of depleting the resources and degrades the network performance.

[8]RFAP(RREQ Flooding Attack Prevention (RFAP)) technique is used to identify the malicious flooder node. Compared to AODV, RFAP detects the false node at a faster rate. But this cannot be used to stop illegal data packets.

[9]Detection of flooding is improved by using the amount of legitimate packets processed at each node. A buffer called receive buffer is used to measure the total available packets. This scheme improves the end-to-end packet delivery ratio.

[10] In this paper a distributive approach is used to detect the RREQ flooding attack. Choice of best threshold value is applied in the delay queue method which uses timer concept to reduce the probability of accidental blacklisting of the node. If the threshold value is not efficient then there is a chance to allow false nodes blindly.

[11] In this paper a novel period-based defence mechanism (PDM) against data flooding attacks is proposed to enhance the throughput of burst traffic. PDM scheme is based on periods, sets up w periods for the data transmission, uses a blacklist which considers the data type, and processes packets according to the priority so as to defend against data flooding attacks and checks data packet floods at the end of each period in order to enhance the throughput of burst traffic in the network.

VII. LIMITATIONS

Performance degradation leads to unavailability of network nodes. If one popular and successful website such as Amazon is affected by such an attack even for an hour, the financial losses can be huge. Power and Resource constraints on nodes limit cryptographic measures which are used to apply a secure connection

Dynamic topologies may lead to compromise and allow any node can pretend to be a legitimate node and provide incorrect information. Eavesdropping and traffic monitoring are also other serious issues to be considered.

CONCLUSION

This study aims to understand the MANET structure, its properties, routing knowledge and the necessity to develop an efficient algotithm or technique to prevent, detect and control different types of flooding attack in MANET. Since wireless networks are used for almost all kinds of data transmission security of the data that is being transmitted has a very important role. Therefore future work on flooding control mechanism will be more efficient than the existing system.

References

[1] Harikrishnan Nair, Sreeja Nair,"Firewall based Signature Enhancement for flooding attack in MANET", International journal of advanced Research in computer and communication Eng., March 2016.

[2] VibhaTripathi, MayureshKanher "Detection and prevention of DDOs flooding attack in MANET", International journal of Advanced research in Computer Science and Software Engineering, Jan 2016.

[3] ShrutiBhalodiya, KrunalVaghela "Enhanced Detection and recovery from flooding attack in MANET using AODV ROUTING PROTOCOL", International journal of computer applications, Sep 2015.

[4] Neethu Raj P, Dr.S.Suresh Babu, Prof. Nishanth N"A Novel SYN Flood detection mechanism for wireless network", International Journal of Advanced Trends in Computer Science and Engineering, Aug 2015.

[5] KomalJoshi, VeenaLomte "Preventing Flooding attack in MANET using node to node authentication," International journal of advanced research in computer science and software engineering, Nov 2013.

[6] MukeshKumar & Naresh Kumar"Detection and Prevention of DDOS Attack in MANET Using Disable IP Broadcast Technique." InternationalJournal of Application or Innovation in Engineering & Management, July 2013.

[7] Bhuvaneshwari K, Dr. A. Francis Saviour Devaraj, "A Profile based Detection Scheme for flooding attack in AODV based MANET", International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 3, June 2013,DOI : 10.5121/ijsptm.2013.2302

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

[9] HyoJin Kim, Ramachandra Bhargav Chitti and Jose Song, "HandlingMalicious Flooding Attacks through Enhancement of PacketProcessing Technique in Mobile Ad Hoc Networks", in Journal of Information Processing Systems, DOI : 10.3745/JIPS.2011.7.1.137,Vol.7, No.1, March 2011.

[10] Shishir K. Shandilya, SunitaSahu, "A trust based security scheme for RREQ flooding attack in MANET"

International Journal of Computer Applications (0975–8887), Volume 5-No.12, August2010.

[11] Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, Member,2010 IEEE "Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks".

[12] Schuba, C.L., I. V.,Kuhn, M.G., Spafford, E.H., Sundaram, A., and Zamboni, D.(1997). Analysis of a denial of service attack on TCP. In Proceeding of 1997 IEEE Symposium on Security and Privacy, pages 208-223, Oakland, CA.