ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

BLACK HOLE& FLOODINGAGAINST ROUTING LAYER IN MANET'S

Sunanda Puri
Research Scholar, Department of Computer Engineering
Guru Nanak Institute of Technology, Mullana, Ambala
India
sunandapuri83@gmail.com

Harish Saini
Department of Computer Science Engineering
Guru Nanak Institute of Technology, Mullana, Ambala
India
harishsaini@gni.edu.in

Abstract - Mobile Ad-hoc Network are extensively used in various areas like military, business, commercial sector and other areas. MANET uses dynamic topology which allows any node to enter or leave the network at any point and instant of time. The characteristics like dynamic topology makes it vulnerable to security threats. BLACK HOLE attack is one of the major security threat in mobile ad-hoc network. Here in this paper we are reviewing flooding, black hole security threat sand some provisions to tackle these problem.

Keywords - MANET, black hole, flooding, security ,routing.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is an environment where independent mobile nodes can communicate with each other using radio waves. [4][5]. The mobile nodes which are in radio range can directly communicate with each other, whereas others nodes need the help of intermediate nodes to route data packets in multi-hop fashion. Mobile ad-hoc networks are used in disaster recovery, rescue operations, military communication and many other areas. Designing energy-efficient routing protocols, in multi-hop wireless ad hoc networks is critical since nodes have very limited energy, computing power and communication capabilities. Routing is an important aspect in mobile ad hoc Network. Routing protocol determines the path to be followed by data packets from a source node to a destination node. Resource constraints are a major challenge that a routing protocol designed for ad-hoc network faces. Portability is required in most cases by the devices used in ad-hoc wireless networks and due to this they also have size and weight constraints along with the restrictions on the power source. The nodes may get bulky and less portable when the battery power is increased.[5]

It is a self-configuring network of links connecting mobile nodes in a wireless environment [5][6]. These mobile nodes may be routers and/or hosts depending on the situation.

Without the aid of access points the mobile nodes communicate directly with each other, and therefore their infrastructure is not fixed. An arbitrary topology is formed by them, where the routers are free to move randomly and arrange themselves as demanded.

The current need of wireless world, dominated by Wi-Fi, architectures which mix mesh networking and ad-hoc connections are the beginning of a technology revolution based on their simplicity[5][6]. Ad hoc networks date back to the Seventies. They were developed by the Defense Forces, to comply with a military framework. The aim was to rapidly deploy a robust, mobile and reactive network, under any circumstances. These networks then proved useful in commercial and industrial fields, first aid operations and exploration missions. Ad hoc networks, also called peer-to-peer networks, still have a long way to go in order to be fully functional and commercial, as it has its defects such as security and routing.

II. SECURITY ATTACKS

A. Message bombing:

An attacker can saturate the medium with a havoc of broadcast messages, reducing the desired output and most probably impeding the nodes from communicating and cause Denial of service deploying network layer [1].

B. Shrew Attack

An effective low rate Denial of service attack can be caused by sending slow time scale frequency with short burst repeatedly. TCP operates on timescales of Retransmission Time Out (RTO), in case of severe network congestion. TCP congestion control protocolis triggered by the throughput (composed of legitimate traffic as well as Denial of Service traffic), due to this the TCP flow enters a timeout and awaits a RTO slot before trying to send another packet in the network. The flow repeatedly tries to exit timeout state and fails, producing zero throughput, if the attack period is chosen to approximate the RTO of the TCP flow. The throughput is severely reduced, if the attack period is chosen to be slightly greater than the RTO. The sending rate of Denial of Service traffic is very low to be detected by anti-Denial of Service countermeasures that's why this attack is effective [1].

C. Jellyfish attack

In this type of attack, unwanted delays are introduced in the network by the attacker. The attacker node gets into the network and became a part of the network by getting access to the network. By delaying all the packets that the attacker receives, it introduces delays, once delays are propagated then packets are released in the network. Owing to this the attacker produces high end-to-end delay, high delay jitter and the performance of the network is considerably affected [2].

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

D. Modification Attack

Any node can freely join the network and can leave it in case of ad-hoc network. Mobile nodes intending of attack, join the network. The irregularities in the network amongst the nodes are then exploited by the attacker nodes. The malicious node participates in the transmission process and later on some stage the message modification attack is launched by it. The two types of modification attack are misrouting and impersonation [1].

E. Replay attack

Old control messages, though valid in the past, describe a topology configuration that no longer exists as the topology changes. A replay attack can be implemented by the attacker by recording old valid control messages and re-sending them, to make other nodes use stale routes in updating their routing tables. If control messages bear a digest or a digital signature that does not include a timestamp, this attack is successful [1].

F. Gray Hole Attack

In this kind of attack the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receive the packets from the neighboring node, the attacker drop the packets. This is a type of active attack. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack [2].

G. Rushing attack

A violation that can be carried out against on-demand routing protocols is the rushing attack. On-demand routing protocols state that nodes must forward only the first received Route Request from each route discovery; all further received Route requests are ignored. This is done in order to reduce cluttering. The attack consists, for the adversary, in quickly forwarding its Route Request messages when a route discovery is initiated. If the Route Requests that first reach the target's neighbors are those of the attacker, then any discovered route includes the attacker[2].

H. Wormhole Attack

It is a severe attack situation where two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. In wormhole attack, the attacker gets themselves in strong strategic location in the network. They make the use of their location i.e. they have shortest path between the nodes. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data. The wormhole attacker creates a tunnel in order to records the ongoing communication and traffic at one network position and channels them to another position in the network. When the attacker nodes create a direct link between each other in the network. The wormhole attacker then receives packets at one end and transmits the packets to the other end of the network[3].

I. Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

The method how malicious node fits in the data routes varies. Fig. 1.1[2] shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

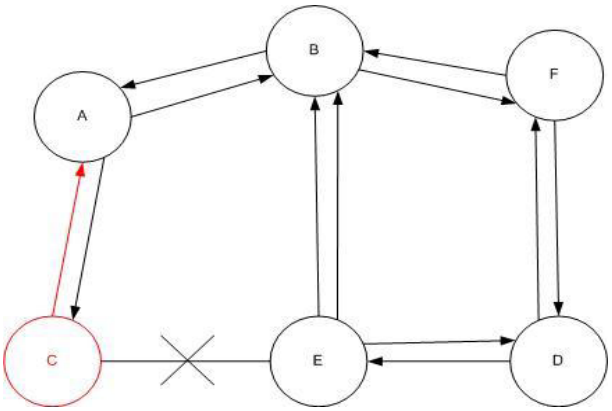

Figure 1.1 Black Hole Problem

J. Flooding Attack

Flooding is an easy to implement attack but it can cause severe damages. Such attack can be caused either by using Data flooding or RREQ. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. In this approach the attacker node selects such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker set up paths between all the nodes in the network by getting in to the network. The attacker injects an immense amount of useless data packets into the network once the paths are established, which is

ISSN 2348 - 2249
Volume-2, Issue-2, June-2014
International Journal for Multi Disciplinary Engineering and Business Management
(IJMDEBM)

directed to all the other nodes in the network as shown in fig 1.2. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time [2].

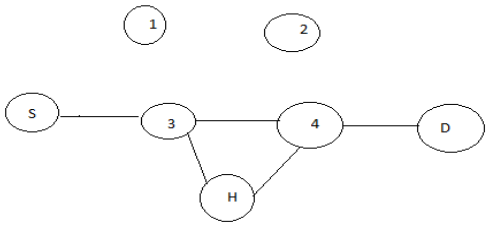

Fig.1.2 Flooding attack model with attacker node H

III. METHODS

A. *Black Hole attack*

It is a serious security threat, as whole or some of the data packets can be misrouted or lost. Some methods are proposed here to deal with this problem.

First Method - The first approach to tackle black hole attack is to transmit redundant data packets or in other words multiple routes should be selected to transmit the same data packets instead of only shortest path [3]. In this method the sender node will wait until RREP is received from more than two nodes. During this waiting time the sender node will buffer its data packets. After the RREP is received the sender node will analyze the whole path to the destination node. When a safe route is discovered it will transfer the packets in buffer.

The two or more redundant nodes must have shared some hops, from these shared nodes safe route can be examined. If none of the two nodes have shared hops it will wait for another RREP. The major drawback of this approach is that it consumes a lot of time. The efficiency of transmission is reduced due to time delays.

Second Method - One another approach to tackle the black hole can be synthesized using two separate tables. One table will maintain the record of sequence number of last data packet sent to every node and one for the sequence number of data packet received from every node [3]. The entries in these tables will get updated whenever any data packet is sent or received. The sender will broad cast the RREQ packet to its neighboring nodes and when the receiving node receives the RREQ packet, a RREP packet will get generated having the sequence number of last packet received and the sequence number of last packet sent, and reaches the source node. The sender node can easily examine the trusted node and destination.

This method is fast and reliable approach to handle black hole problem.

B. *Flooding attack*

It causes severe damages to network deteriorating the efficiency and overall services. Some methods are proposed here to deal with the problem of flooding

RREQ Flooding - To handle RREQ flooding a simple approach is adopted, the threshold level for the maximum number of packets, a node can receive from the nodes in its neighborhood is set. A node having reached this threshold level can no more flood the network with useless packets [8].

Data Flooding - To prevent data flooding the intermediate node assigns a threshold value of number of packets it can receive from its neighboring nodes, when this value is achieved it drops all the RREQ packets of that particular node whose threshold value is reached, are ignored and dropped.

IV. CONCLUSIONS

Here we studied various security threats on mobile ad-hoc network. Black hole attacks as well as flooding attacks both are serious security threats in MANET. In this paper we studied about the impact of black hole attacks and the flooding attacks on mobile ad hoc network . We also discuss about various methods and comparative study about both black hole as well as flooding attacks on MANET.

REFERENCES

[1] Ankita Gupta, Sanjay Prakash Ranga, “Various Routing Attacks in Mobile Ad-hoc Networks” published in International Journal of Computing and cooperate Research, volume 2 Issue 4 July 2012.

[2] Gagandeep, Aashima, Pawan Kumar,“Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review,”International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012

[3] Malcolm Parsons,Peter Ebinger,“Performance Evaluation of the Impact of Attacks on Mobile Ad hoc Networks”

[4] http://ijircce.com/upload/2014/acce14/17_P150Mobile.pdf

[5] Kuldeep Sharma, Neha Khandelwal, Prabhakar.M, “An Overview Of security Problems in MANET”

[6] http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group11/

[7] http://www.ijstr.org/finalprint/july2013/ “Simulation-And-Analysis-Of-Performance-Parameters-For-Black-Hole-And-Flooding-Attack-In-Manet-Using-Aodv-Protocol-.pdf“

[8] Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava, “Simulation And Analysis Of Performance Parameters For Black Hole And Flooding Attack In MANET Using AODV Protocol”,INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 2, ISSUE 7, JULY 2013 ISSN 2277-8616

[9]Bhuvaneshwari. K, Dr.A.Francis Saviour Deva raj, “Examination of Impact of Flooding attack on MANET and to accentuate on Performance Degradation”Int. J. Advanced Networking and Applications Volume: 04 Issue: 04 Pages:1695-1699 (2013) ISSN : 0975-0290

[10]S. A. Razak, S. M. Funnel, P. J. Brooke,”“Attacks against Mobile Ad Hoc Networks Routing Protocols”,Network Research Group, University of Plymouth

[11]Malcolm Parsons,Peter Ebinger “Performance Evaluation of the Impact of Attacks on Mobile Ad hoc Networks”

[13]Gagandeep, Aashima, Pawan Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.

