COMPARATIVE STUDY OF FLOODING ATTACK IN MOBILE AD-HOC NETWORK

Nupur Agrawal[1], Upendra Dwivedi[2]
Department of CSE, SVITS, Indore, India

ABSTRACT: A Manet is a collection of two or more mobile nodes in a network in which each node can act as a router. Each mobile node in a network can establish the connection with each other. Manets are defenseless to various types of attack because of the features like instant changing topology, resource limitation, and unavailability of any centralized infrastructure. In Manet routing can be caused by the malicious nodes which act as legitimate nodes. The flooding attacks are two types data flooding and RREQ flooding attack. These both flooding attack causes degradation of network performance and also waste the network resources. In this survey paper, various routing attack which is caused in Manet is analyzed. Some routing attack in manet is very difficult to detect because of their nature. The various routing attacks are blackhole attack, wormhole attack, link spoofing attack and much more.

Keywords: MANET, Routing Attacks, Routing Protocols.

I. INTRODUCTION

A Manet is a dynamic wireless network which is a collection of mobile nodes. A Manet is a dynamic wireless network that can be formed without any framework in which each node can proceed as a router. The wireless system gives the versatility based administration use and consequently uproots the area conditions for the clients of cell phones, for example, portable workstations, PDAs, Tablets and PDA's. These systems are classified on the premise of their infrastructural use and scope of transmissions. The primary challenge in building a MANET is equipping each device to continuously maintain the information desire to properly route traffic. Such networks may operate by themselves or may be connected to the better Internet. They may contain one or more transceivers between nodes. This results in a highly dynamic, autonomous topology.

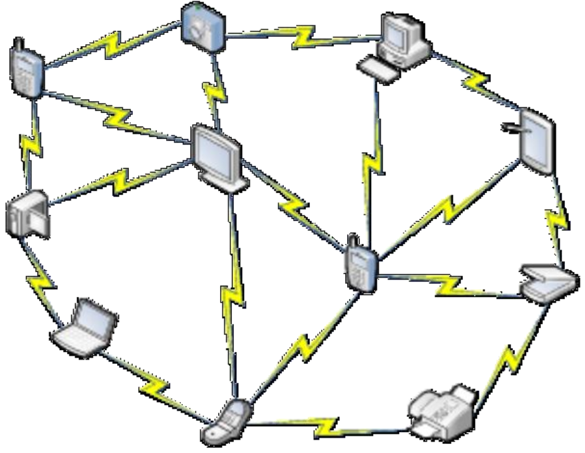

Fig.1. Mobile Ad-hoc Network

This Figure shows the Mobile Ad-Hoc Network. In some ad-hoc networking applications, users may be distributed over a wide area and a given user terminal may be able to reach only a portion of the other users in the network owing to transmitter signal power limitations. In such case, user terminals will have to cooperate in carrying messages across the network between widely separated stations. Networks designed to function this way are known as multi-hop ad-hoc networks. In Manet, routes between the nodes may potentially contain multiple hopes in which nodes act as routers to forward packets for each other and also the nodes mobility may cause the routes changes. The advantages of manet are low cost, flexibility and also the decrease the dependence on infrastructure. The dynamic nature of Manets makes network free for attackers and imprecision. Routing is always the most powerful part of any networks. Each node should not only work for itself but also be cooperative with other nodes. The ad-hoc wireless networks find their applications in many areas due to their quick and economically less demanding deployment. The deployment of a Manet is easy due to the absence of setting up any infrastructure for communication. The application of ad-hoc wireless network is military, emergence operations, collaborative and distributed computing. But slowly Manets have entered in the areas of gaming, sensing and conferencing. This dynamic network is yet to catch most of the commercial applications. The Manet can be extended in many areas where a faster and a cheaper network can be setup instantly for data communication. Mobile ad-hoc networks have many features, which make them quite distinct from wired networks and thus require innovation ways to implement the network.

II. LITERATURE SURVEY

In this paper, author narrates about Manet's various rules because of its routing protocols. The main aim is that rate based control mechanism of forwarding packets has been introduced to mitigate malicious control packets. The advantage of this survey is that the protocol can be made secure against other types of possible DOS attacks. And none of the legal nodes in the network are badly accused as the misbehaving node. The drawback of this method is that it doesn't distinguish between a genuine node and malicious nodes and also which node is flooding the network [7].

In this paper, author represents the technique for the prevention of flooding attack. In this the mobile ad-hoc network is analyzed and the behavior of intruder and also check it by trust function. It provides the prevention from the malicious nodes. It checks if the attacker’s node transmits the packet (i.e. RREQ). In this, the neighbor is categorized into the friend (most trusted), associate (trusted) and foreigner (not trusted). That's why the prevention technique is easily implemented and also identified. The problem in this technique is that it doesn't work properly with higher nodes [8].

In this work, the author presents a distributive approach to detect and prevent the RREQ flooding attack in the mobile ad-hoc network. The selection of threshold values determines the strength of the approach. The main advantage of this approach is the node identification that identifies the senders who are originating data flooding and also cut-off the path and sends the error message to the neighboring nodes in the network. The problem with this approach is it gets delays to detect the malicious node because it allows the node to send the packets until the timeout occurs in the network [9].

In this paper,the author has proposed a technique to prevent and detect the distributed denial of service (DDoS) attack. The wireless networks are extremely vulnerable to DDoS attack because it is an open area network and also a wireless medium. The DDoS attack is an attempt to make a resource inaccessible to its genuine users. In this paper the author has taken the benefit of the weakness of the routing protocol and it has also evaluated various detection methods of the routing protocol. For that, an algorithm is suggested that is capable of detecting the attacker node which is misbehaving in the network [10].

III. ROUTING ATTACK IN MANET

Flooding Attack

The flooding attack is that in which it try to cause a failure in the network by providing more input than it can access properly. The purpose of the flooding attack is to exhaust the network resources like bandwidth, battery power and computational or to disorder the routing operation to cause the severe reduction in the network. Flooding attacks occur when a network or service becomes heavily weighed down with packets which result in incomplete connection requests because of which no genuine connection request can be served. There are two types of flooding attack i.e. RREQ flooding attack and data flooding attack. In RREQ flooding attack the attacker nodes declare many RREQ packets in the network so that the bandwidth of the network gets waste. And in the data flooding attack, the attacker flood the network with unnecessary packets so that the resource of the network is wasted. This can be explained by example, in which a malicious node can send a huge number of RREQ request packets to route nodes of the network so that the network gets flooded and all the power of battery and bandwidth gets consumed.

Black hole Attack

The attack in which the attacker that is supposed to communicate packets in the network rather discards them. This usually occurs when a node of the network becomes compromised from a number of different causes. The packets are commonly dropped from a loss network, this type of attack is very hard to detect and prevent. The malicious node can also attain this attack by dropping packets for a particular destination of a network or can delay the packet for the certain time or a randomly chosen part of the packets. If the malicious node tries to drop all the packets that are received by it then attack can be quickly discovered through the detection tools called race route. Also, when other nodes notice that the malicious node is dropping all the packets which are received by it then they will begin to remove that node from the routing tables and no packet will be transferred from that node and attack is prevented. However, if the malicious node drops the packets at a particular time or after every n packets, it is much harder to detect the node because some traffic will flow from the node and so it is not discarded form the routing table and from the network. This attack can be explained by using an example in this attack, the attacker node will send a fake RREP response packet to the source node with the fake sequence number in it saying that it has the new route to the destination node. Because of this, the source node selects this route which contains the attacker node and then this attacker node will discard or modify the packet.

Link Spoofing Attack

The link spoofing attack is the type of routing attack in which the malicious node display the fake link with non-neighbors in the network to its neighboring nodes to disrupt routing operations of the neighboring nodes. A malicious node can also manipulate data of the nodes and can also dropping the packets. This can be explained by example like in OLSR protocol the malicious node broadcast a fake link in the network including two hops of neighbor because of which the source node select the route which is provided by the malicious nodes. And in this way, the spoofing attack can be possible in the network.

Routing Attacks	Connectivity Problem	Message Loss
Flooding Attack	The connection problem takes place because network gets flooded	Their is no loss of message
Black hole Attack	Their is no connectivity problem in the attack.	Their is no loss of message
Link Spoofing Attack	Their is no connectivity problem in the attack.	Message is lost in the network
Wormhole Attack	Their is no connectivity problem in the attack.	Message is lost in the network
Gray hole Attack	Their is no connectivity problem in the attack.	Message is lost in the network
Sinkhole Attack	The connection problem takes place because network gets flooded	Their is no loss of message

Tab.1. Comparative Table of Routing Attacks

Wormhole Attack

In this attack, the attacker node records the entire data packet at any location in the network and then mine them to the somewhere else location using the private network. By this, the routing gets disrupted because the message that controls the routing is tunneled in the network. This tunneling of the location between the two conspiring attacker is called as wormhole attack. This type of attack is very difficult to detect in the network and also it's cannot be prevented for all routing protocol. This type of attack is used against the communication which provides confidentiality and authentication in the network.

Selfish Node Attack

The selfish node attack is the type of routing attack in which the selfish node acts as a normal node in the network. The selfish node doesn't forward the data packet in the network or simply delay the time of forwarding so that the connection gets a delay. This type of node cannot be detected easily because they act as a normal node.

Gray Hole Attack

The grayhole attack is the modification of blackhole attack where an illegal node first behaves as a legal or normal node when the route in the network is discovered. After the route discovery process, the node which is illegal drops the packet (some or all packets) which is forwarded to it for further forwarding in the network. This attack is a more difficult attack because it is not detected easily like black hole attack. In gray hole, the attacker drops the packet with certainty.

Sink Hole Attack

In sink hole attack, the attacker broadcast the incorrect routing information in the network to its neighbor node and symbolize that it has low cost and have an approving route to the destination. Because of this manipulation of the information of routing most of the traffic is drawn towards this node in the network. After all this manipulation all the neighboring nodes send the packet to this node to forward further but this node drops all the packet or some packet it totally depends on the node.

Colluding Misrelay Attack

In this attack, the multiple attackers modifies or drop the packet so that routing operation gets disrupted. This type of attack is not detected by using the watchdog and path-rater methods of convention system. suppose there is a network in which various nodes are connected in a network. Then a source node is forwarding the packet to node 1 (attacker node). Then node 1 will forward the packet to node 2(second attacker node) so that it does not get detected by the source node. Then this node 2 will drop or modify the packet and routing operation gets disrupted. In this way, the attack is been conducted by the multiple attackers.

Rushing Attack

This attack mainly works on the On-demand routing protocol. This type of attack will modify the process of discovery. This sort of attack significantly affect network connectivity and weakness network functionality and also capabilities such as control and message delivery. In this attack, various senders and receiver participate together where duplication of packets are done at the branch point. Where an attacker node sends the packet to the other neighboring node but the attacker nodes send that packet again and again to flood the network. This can be prevented by the technique in which the nodes must only forward the first packet request which is received by it and then all the other packets are discarded at that time only. This is done to reduce the cluttering in the network.

IV. PROBLEM STATEMENT

A router is a tool that performs in layer 3 of OSI model whose main function is to select the path for the packet and forwarding the packet. This is the key part of the network and because of which its security is the major issue in the system. The attacker node can attack the Manet in many different ways like again-and-again sending the fake message, fake information of route, and broadcasting fake links in the network so that the operation of routing gets disrupted. The routing attacks in the network cause various network degradation like network halt, the decrease in performance and also the battery of the network is reduced. These all problems are caused because the introduces the heavy traffic in the network while exchanging the packets. The network is the combination of both the legal node and the malicious node because it doesn't contain any centralized hub. There is various routing attack present in the network which degrades the performance of the network. In flooding attack, its purpose is to flood the network with the packets so that the legal connection between the nodes doesn't take place and the network gets halt. The second attack is blackhole attack whose purpose is that it drops the data packet or modifies the packet which is to be forwarded to the destination node. In wormhole attack it records the packet at one location and the tunnel them to some other location in the network and packet gets lost. In link spoofing attack the attacker node broadcast the fake link to the neighbor node so that the legal connection is not established. Selfish node is the node which acts as a normal node in the network to harm the data packets in the network. All these attacks have some or other problem which case network partition or network halt and the data packets are not properly transmitted in the network.

V. CONCLUSION

A mobile ad-hoc network is a combination of two or more nodes equipped with wireless communications and networking capability. Such nodes can communicate with another node that is immediately within their radio range or one that is outside their radio range. In this paper, we are evaluating about the routing attack which is caused by the excess amount of packets in the network. This attack consumes the bandwidth, resources of the node and battery of the network. So, all the routing attack is evaluated and their solution has been drawn from that analyses. During the analyses, it is taken out that by using the prevention technique attacks can be prevented to increase the efficiency of the network and also to improve the network performance.

REFERENCES

[1] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei kato “Asurvey of routing attacks inmobile ad hoc networks”,ieee wireless communications • october 2007 85 1536-1284/07/$20.00 © 2007 ieee.

[2] Rashid Hafeez khokhar, MD Asri ngadi, Satria mandala “A review of current routing attacks in mobile ad hoc networks”, international journal of computer science and security, volume (z) issue (3)

[3] Yi-an huang and wenke “ Attack analysis and detection for adhoc routing protocols” e. jonsson et al. (eds.): raid 2004, lncs 3224, pp. 125–145, 2004.springer-verlag berlin heidelberg 2004

[4] Venkatesan Balakrishnan, Vijay Varadharajan, Udaya Kiran Tupakula “Defense against Flooding and Packet Drop Attacks in MANET” INSS Research Group, Department of Computing, Macquarie University,North Ryde, Sydney, NSW Australia 2109.

[5] Krishan kumar1, Yogesh kumar2, Gaurav Pruthi “A review of manet security protocols” ijcsms international journal of computer science and management studies, vol. 11, issue 03, oct 2011

[6] Abhay Kumar, Rai Rajiv Ranjan Tewari, Saurabh Kant Upadhyay “Different types of attacks on integrated manet”-internet communication international journal of computer science and security (ijcss) volume (4): issue (3) 265

[7] Jian-Hua song1, 2, Fan Hong1, Yu Zhang1 “Effective filtering scheme against rreq flooding attack in mobile ad hoc networks “ proceedings of the seventh international conference on parallel and distributed computing, applications and technologies (pdcat'06)0- 7695-2736-1/06 $20.00 © 2006.

[8] MS Neetu Singh Chouhan, MS Shweta Yadav “Flooding attack prevention in manet” international journal of computer technology and electronics engineering (ijctee) volume 1, issue 3.

[9] Shishir k. Shandilya, Sunita sahu “A trust based security scheme for rreq flooding attackin manet”,international journal of computer applications (0975 – 8887)volume 5– no.12, august 2010.

[10] Neha Singh , Sumit chaudhary Kapil kumar verma “ Explicit query based detection and preventiontechniques for ddos in manet”, international journal of computer applications (0975 – 8887)volume 53– no.2, september 2012.