International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

INTRODUCTION TO WORMHOLE ATTACK IN MOBILE AD-HOC NETWORKS (MANET)

- **Sonia Malik, Research Scholar, Department of Computer Science, Himalayan Garhwal University, Uttrakhand**
- **Dr. Syed Mohd. Saqib, Assistant Professor, Department of Computer Science, Himalayan Garhwal University, Uttrakhand**

ABSTRACT

An Ad-hoc network is a self-organized network, without a central coordinator, and which frequently changes its topology. In this paper, we have analyzed the performance of Mobile Ad-hoc Networks (MANET) under wormhole attack. Multiple QoS parameters have been considered here such as throughput, delay, packet delivery ratio, node energy and node density. The NS2 network simulator has been used and the reference point group mobility model is considered to study the effect of node density and the initial energy on the throughput. Security is a very challenging issue in MANET as it is without infrastructure and self-governing. Nodes in MANET used for real time applications also make it difficult to devise the resource demanding security protocols because of their limited battery, power, memory and processing capabilities. One of powerful form of such kind of attacks is wormhole attack that affects on the network layer.

Key words : Mobile Ad-hoc Networks, security

INTRODUCTION

Wormhole attack is mainstream and extreme attack in MANET. In wormhole attack attacker gets the packet at one location in the network and tunnels them to other location in the network.

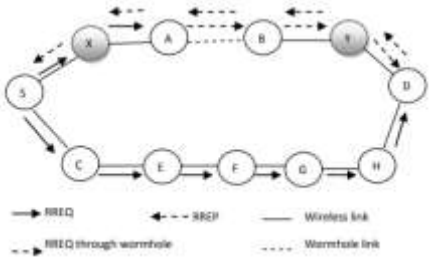

Figure-1: Wormhole attack

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Figure 1 delineates the wormhole attack. At the point when source node S broadcasts RREQ packet to their neighbor nodes X and C. Node X and Node Y expected as malicious nodes. As a result of high speed, tunnel is shaped between node X and node Y, Malicious node X advances the route request packet legitimately to node Y rather than node A. The route request packet from path S-X-Y-D arrives at the goal node first. As indicated by the property of AODV protocol goal node acknowledges the first RREQ packet that arrives at goal node and sends route reply along turn around path. Because of wormhole tunnel between node X and node Y, it builds up the shortest path from source to goal. The route request packet from the path S-C-E-F-G-H-D is disposed of despite the fact that it is a right path.

Wormhole attack using in band channel

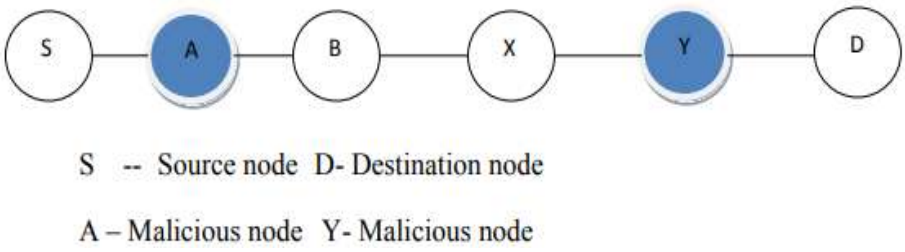

Figure-2: Wormhole attack using in band

Figure 2 illustrates wormhole attack utilizing in band channel. At the point when the source node S needs to send data packet it starts route disclosure process. The source node sends the route request packet to node A. Due to high speed channel between node An and node Y, node A legitimately advances the route request packet to node Y overlooking the node B and X. Rather than unique path S-A-B-X-Y-D, the false path SA-Y-D is picked to send a data packet.

Wormhole attack using out band channel

Figure 3 portrays the wormhole attack utilizing out of band channel. In out of band wormhole attack, the wormhole nodes record the packet they hear and advance the packet inside one another through malicious nodes. In the above figure node An and B are expected as wormhole nodes. Node A advances the packets node B through high speed link

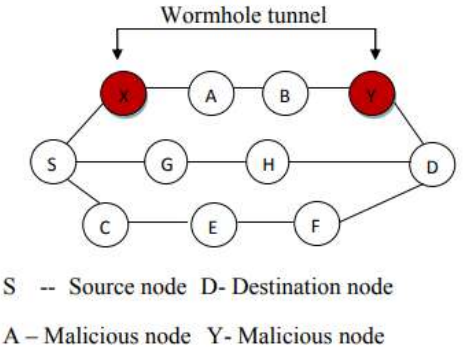

Figure 3: Wormhole using out of band

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

DETECTION FEATURES

In this area, the distinctive element that causes the wormhole is examined. The wormhole attack can be distinguished by utilizing the MANET highlights like location, time, hop count, neighborhood, data packets, route reply, route request and these highlights are talked about quickly in this area.

Distance : If there should arise an occurrence of attacks the location of the interloper node assumes an indispensable job. The careful situation of the attacker node can be related to the assistance of that diagram can be plotted. So it will be anything but difficult to discover the location of the node. Joining every node with the worldwide situating framework expands the expense of the framework. To conquer this, recipient node is appended with the worldwide situating framework to know the situation of the neighbor node. The unique recieving wire is utilized to gather the information about the relative nodes and with the assistance of the relative node we can discover from where the data has been sent. The fundamental burden of utilizing the extraordinary recieving wire or worldwide situating framework is the expanded expense of the framework. The use of worldwide situating framework or exceptional radio wire will decrease the battery life of the framework. Detection component by utilizing the location may expand the false positive rate in light of the fact that the location of the node isn't static in mobile impromptu networks.

Time : The wormhole attack can likewise be detected utilizing the time highlight. The route where the attacker node is available will take additional time per hop when contrasted with the ordinary route. The distinction between the times when the node is sent from source to goal can be firmly monitored by utilizing a synchronized check in the network. There is another method to calculate the time contrast without utilizing the synchronized clock and that is the primary node sends greetings message to the last node when the node arrives at the goal it answers with reply hey message to the source, the time spent to send hello message from source to goal is monitored. The time contrasts between the sender and collector are calculated by excluding the time taken by the source node, goal node and intermediate node and in this manner partitioned by 2. By utilizing this method, average time taken in each hop is calculated and actualizing synchronized clock is tough and costly.

Hop count : The hop count mechanism is utilized in detecting the wormhole attack on the grounds that the wormhole node straightforwardly attacks the network traffic by demonstrating an inappropriate route that is it shows the route of the shortest path. The path where the attacker node travels will have the less number of hops when contrasted with the typical path on the grounds that the hop count won't increment when the node travels in the attacked private path. By utilizing a few techniques or mechanism the worm whole attacker node can be recognized utilizing hop count with location or tie technique. The average time of each hop can be calculated utilizing a total number of hops by total distance or total time. In the event that any hop has a higher average time of hop, at that point the hop contains malicious node. The model that works based on the planning mechanism or distance mechanism will require synchronized check or extraordinary receiving wire in the network.

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Neighborhood : The principle capacity of the attacker node is to show non-neighbor node as a neighbor node. From this announcement, the attacker node can be related to the neighbor node information too. The area is utilized to gather and keep up the information about the prompt neighborhood node; some different techniques discover the worm whole attack by examining the 2 neighbor node by sending the hello message. This technique can't be utilized in the dense network in light of the fact that every node contains numerous neighbors. To investigate up to two neighbor node requires more space, time and storage and furthermore the hello message will build the traffic in the network and the general productivity of the network will diminish and the false positive rate additionally increments on the grounds that the nodes are dynamic and they will change their position.

Data packets : The wormhole attack can be detected utilizing data packets by finding the contrast between the total quantities of nodes sent and got in the network. In this model the nodes are set in a mode with the goal that they listen to the capacity of the neighbor node. Those nodes keep up a record of various nodes sent by the neighbor node. Table-1 outlines the correlation of wormhole attack detection highlights.

Table 1 Comparison of wormhole attack detection features

Detection time	**Congestion**	**Routing Delay**	**Resources Overuse**	**Special Hardware**	**Mobility**
Location	----	----	Yes	Yes	----
Time	-----	-----	Yes	Yes	----
Hop Count	----	Yes	Yes	----	----
Neighborhood	Yes	----	Yes	----	Yes
Data Packets	Yes	----	Yes	Yes	----
Route Reply	----	----	Yes	Yes	Yes
Route Request	----	----	Yes	----	----

With the assistance of this they can see the status of the node whether the nodes have been dropped or changed or arrived at goal or sent to some different nodes other than the goal. With the assistance of this information, they can calculate the trust value of every node in the network and the attacker node can be distinguished and it very well may be utilized in the dense network.

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Route reply : By utilizing the RREP message appeared in Figure 4 the wormhole attack can be distinguished, on accepting the request of the crisp route, the node present in the network sends the RREP message to a neighbor node or goal node. The attacker node won't utilize this method for attacking. Since route request sent in the unicast route, on the off chance that they need to dissect and keep up the record of the node, at that point it must be set in the valuable node. In the event that the node is set in valuable node, at that point it will diminish the network productivity.

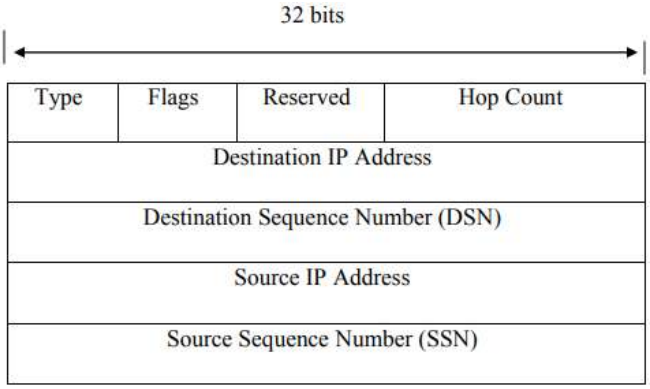

Figure 4: RREP message format

Route request

The route request message appeared in the Figure 5 assumes an important job in the on-request routing network and it can likewise be utilized to discover the wormhole attack with blend of some other element. The route request message is sent from the source node and it arrives at the whole node present in the network.

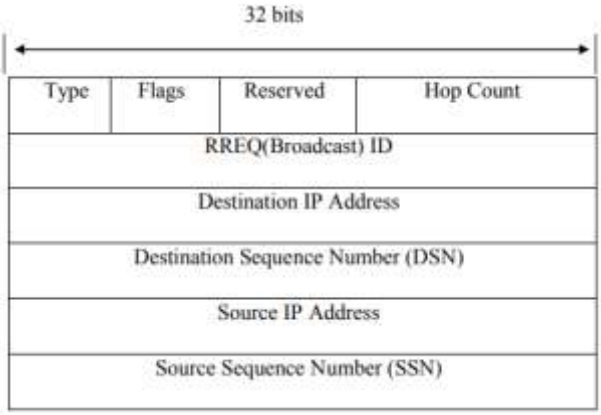

Figure 5: RREQ message format

AODV ROUTING ATTACKS

AODV gives bunches of opportunities to attackers. There are various misuse destinations that an inside attacker may want to achieve.

Misuse Goals : The misuse goals can be one or more of the following:

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

Route Disruption: In this, attacker includes in attempting to separate a current link or stopping another path from being set up. The point is to target just route between two endpoints.

Route Invasion: In this, an insider attack incorporates himself as a piece of a route among source and destination points of communication channel.

Node Isolation: In this, an attacker separates a specific node from network and forestall node to participate in communication process with different nodes in the network. The point is to focus on every single imaginable route.

Resource Consumption: In this, an attacker attempts to consume accessible bandwidth in the network and storage space accessible at each node to disturb transmission process. For instance, an inside attacker may consume the network bandwidth by flooding fake messages in the network.

Denial of Service: In this, an attacker attempts to stop legitimate nodes to use some portion of network or whole network connection. Denial of service can be broadened itself to all layers of protocol stack. They can attack on legitimate users' access to a service supplier or service accessibility.

Attacks : To accomplish these objectives that are depicted in past segment, the accompanying misuse activities or attacks might be performed:

Packet Dropping Attack

In a packet dropping attack, they got routing messages are essentially dropped by the attacker. This can be detected by monitoring whether a neighbor node is broadcasting packets towards definite destination or not. To empower the monitoring of neighbor nodes, it is required to keep neighbor table. This attack is accessible in various structures. Different subcategories are as per the following:

In the event that an attacker needs to apply packet dropping attack on the RREQ messages it gets, RREQ messages can likewise be specifically dropped by an inside attacker. Such sorts of misuses by attackers are comparative in nature to the childish nodes. On the off chance that an attacker worries on applying this attack on RREP messages, it very well may be the situation of route interruption. This attack can likewise apply on other data packet and will keep influenced node from taking data packets from neighboring nodes for a little timeframe. After accepting RREQ message, an attacker can make adjustments like to expand RREQ ID, to change the destination IP address with other IP address, to include the source grouping number by one, to set up non-existent IP address of source IP address. After doing this, fake message can be sent by an attacker.

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

At the point when all neighbors of an attacker get the fake RREQ message, they change the next hop of the source node to the non-existent node in light of the fact that faked RREQ message have a larger source grouping number. Due to non-existent destination IP address, the fake message will travel to the extraordinary nodes in the impromptu network. At whatever point any node requires sending data packets towards the source node, they will follow route made utilizing the fake RREQ message. Due to non-existent node, data packets might be dropped. With the assistance of local fix mechanisms in the AODV protocol, this attack can't totally separate the injured individual node. At whatever point a node watches fruitless delivery of data packets, nodes will again begin route revelation process.

Sequence Number Attack

The freshness of route combined with a node will be shown by utilizing arrangement number. In the event that an attacker transmits an AODV control packet with a large arrangement number of the undermined node, the route will be coordinated towards traded off node. The grouping number might be diminished to control refreshing in the table or expanded to restore other nodes' switch route tables. This attack can likewise be apply on both either Source Sequence Number or the Destination Sequence Number. A RREQ message can be extraordinarily recognized by RREQ ID alongside the source IP address. The blend of this shows the freshness of a RREQ message. Whenever, a node just considers the primary duplicate of a RREQ message. In the event that another node acknowledges the expanded RREQ ID alongside source IP address, that implies node will acknowledge faked RREQ message. Grouping number attack can just consider arrangement number field, accessible in RREQ message.

Field Modification Attack

As it is realized that data packet will be sent with the header. In layering process, data packets experience various layers and include headers appropriately. The field alteration attack is answerable for changing the field values in header at network layer. As above, grouping number attack is altering arrangement number field in this manner it tends to be said that succession number attack is a piece of field adjustment attack. Different fields that an attacker can adjust are highlighted beneath. The table given underneath will show effect of changed field during ordinary routing process.

Table-2: Field Modification Attack on RREQ Message Field

RREQ Message Field	Modifications
RREQ ID	To make faked RREQ message acceptable or unacceptable, attacker increases or decrease RREQ ID.
Type	Message type will be changed.
Hop Count	To invalidate the update, hop count will be decreased or increased to update other nodes' reverse routing tables.
Destination IP Address	Replace with another IP address
Source IP Address	Replace with another IP address to change the reverse route

International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 11 Issue 05, May- 2021
ISSN: 2249-7382 | Impact Factor: 8.018|
(An open access scholarly, peer-reviewed, interdisciplinary, monthly, and fully refereed journal.)

At the point when a few fields have been adjusted by attacker, it shows prompt security repercussions in the network. For guaranteeing circle opportunity in AODV, a node after accepting RREQ message alters its turnaround routing table. This change happens just if source grouping number is more noteworthy than the value in its routing table or source arrangement number is equivalent yet hop count value is littler than that in the routing table for RREQ message. To influence other node's routing table, an inside attacker can likewise include in changing these fields. Same technique will be utilized for a RREP message. In this, if the destination arrangement number in RREP message is more prominent than the value one in its routing table or destination succession number is the equivalent however the hop count in addition to one is littler than the value in routing table, a source node or an intermediate node alters its forward routing table. Presently take attacker point of view, if the destination succession number in the RREP message is more noteworthy than the one in its routing table, or the destination arrangement numbers are the equivalent, yet the hop count in the RREP message in addition to one is littler than the one in its routing table, the attacker can contain the legitimate RREP message by expanding the destination grouping number.

Field Addition Attack In this attack, an attacker can fabricate a RREQ message without accepting a RREQ message. For propelling this attack, there is a need to gather some essential information to assemble faked RREQ messages (e.g., by listening to the traffic). In principle, to cause disturbance in routing process, the attacker may include any field in a RREQ message.

CONCLUSION

In this paper we introduced the wormhole attack, presented its different modes in details together with an attack graph that we constructed to illustrate the sequence of events in each mode. We also discussed the threats that this attack presents briefly, and overviewed the effort done in the literature to combat this attack. While wearing an attacker's hat, we analyzed each mode and identified its advantages, disadvantages, challenges, possible solutions to these challenges, minimum number of nodes to launch each attack mode, suitable network topology, and countermeasures that could be used and have to be considered while launching each wormhole attack mode. To illustrate this attack's effect we presented the simulation results of two modes of this attack. T

REFERENCES

- K. Lee, H. Jeon, and D. Kim, "Wormhole Detection Method based on Location in Wireless Ad-Hoc Networks," in New Technologies, Mobility and Security: Springer Netherlands, 2018, pp. 361-372.
- S. Ning, Q. Lijun, and L. Xiangfang, "Wormhole Attacks Detection in Wireless Ad Hoc Networks: A Statistical Analysis Approach," in Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05) - Workshop 17 - Volume 18: IEEE Computer Society, 2015 .
- S. Khurana and N. Gupta, "FEEPVR: First End-to-End Protocol to Secure Ad Hoc Networks with Variable Ranges against Wormhole Attacks," in Second International

Conference on Emerging Security Information, Systems and Technologies, secureware, 2018, pp. 74-79.

- L. Gunhee, S. Jungtaek, and K. Dong-kyoo , "An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks," in Proceedings of the 2018 International Conference on Information Security and Assurance, 2008, pp. 220-225