A Comprehensive Review and Performance Evaluation of Reactive and Proactive Protocols under Routing Attacks in MANET

Sunil Kumar Jangir¹, Naveen Hemrajani²

¹,²Department of Computer Science & Engineering, JECRC University, Jaipur, Rajasthan, India

Abstract — Mobile ad hoc networks although have always proved their efficiency but they are still prone to attacks which are particularly challenging in wireless networks. It can be compromised by various methods. This paper is an attempt to study different types of security attacks and a simulation-based study of the impacts of these different attacks on mobile ad hoc networks (MANETs). Nodes that donot follow the routing protocol specifications may generate incorrect control messages, incorrect traffic relay etc. The objective of the attackers is to exploit the network for creating disorder in the network system and in its topology. We have considered the most common attacks like Wormhole attack, Grayhole attack, Sybil attack and Blackhole attack with respect to AODV and OLSR. Specifically, we have studied how the number of attackers and the number of nodes affect the performance matrices such as Network throughput, packet delivery ratio and Average end-to-end delay. The result helps us to choose the best use of routing protocols with security measurements and how to minimize the effect of the attacks, given above on Reactive and Proactive routing protocols in MANETs.

Keywords — MANET, Blackhole Attack, Wormhole Attack, Grayhole Attack, Sybil Attack

I. INTRODUCTION

The Mobile ad hoc network is one of the wireless network structures in which every node is movable and changes its position dynamically. It represents complex distributed system which consists of the collection of wireless mobile network and its nodes, which are connected through each other by wireless links. MANET isa group of mobile nodes that are decentralized. So, MANET is an ad hoc network which does not have any configuration. It is independent of any fixed infrastructure. In MANET each individual node works as a router for the communication with other nodes in the network. Due to the low cost and mobility, the MANET is best suitable for vehicle network, maritime communications, and emergency operations. The dynamic topology and mobile node routing are error prone in comparison to the conventional routing protocols.

Routing in MANETs has been classified as Proactive Routing protocols (Table driven) and Reactive Routing protocols (On demand). A reactive protocol initiates routes whenever they are needed whereas proactive protocols maintain consistent and keep the table up-to-date which contains routing information of each node from the source to the destination. In this paper we have considered reactive routing protocol like AODV and proactive routing protocol like OLSR. Since no security mechanism has been provided by AODV, attacks can be performed by attackers to any malicious node by violating the protocol specifications. The major AODV weaknesses are Deceptive incrementing of Sequence Numbers and Deceptive decrementing of Hop Count. In OLSR more time is required to rediscover a broken link and more processing power is also required at the time of alternate route discovery. With the security constraint, all the control messages are required to be secured in OLSR. In order to show the routes to the valid addresses the host and gateways are statically configured.

II. ROUTING ATTACKS IN MANETS

As active nodes provide routing among themselves and complete a network so MANET depends only on the active nodes that does so. In the network if the node becomes malicious then the attacker can easily exploit the network and may damage the ad-hoc and routing network which becomes vulnerable to attack due to its dynamic, distributed infrastructure and not having any centralized body.DOS (Denial Of Service)[1] attacks are easily possible for attacker in such cases. Both active and passive attacks are possible here. It’s our assumption in ad-hoc networks that all the nodes are trustworthy but this is not always true.

A. Flooding attack

In Flooding attack the attacker produces excessive route advertisements by flooding false route creation packets to malicious nodes and thus prevents new routes from being created in the network.
B. Wormhole Attack

Wormhole attack includes two malicious nodes [3] in which attacker inject tunnel traffic back to the network by capturing the routing traffic and tunneling it to another point and sharing a high speed communication link between nodes. Thus these two attacks at different points exploit the topology over the wormhole link.[34]

C. Blackhole Attack

This type of attack mainly deals with two major concerns. First, the node attacks on the ad-hoc routing protocol like AODV and falsely advertising itself as if it has some route way to reach the destination even though there is no such route in the network, when the packet flows from that false path the attacker either take that packet and get all the information or modifies the packet and allow it to go to its destination. However, as the neighbouring nodes may monitor and expose the ongoing attacks it leaves other node data intact so that the ongoing node cannot identify the changes in packet by the attacker.[33]

D. Node Isolation Attack

Node Isolation attack is an attack against OLSR protocol. Node isolation attack attempts to isolate a node from the rest of the network. The logic behind node separation is that it prevents the node link information to reach other node and thus other nodes are not able to build and find a route to the affected node and to send data to the attacked node [4].

E. Routing Table Poisoning Attack

Routing table poisoning attack is possible in the routing protocols that maintain tables that hold the network information. This attack aims to put false entries in the table that result in non-optimal route less selection, bottlenecks, routing loops creation and even the network partitioning. Here the attacked nodes change the valid messages from other nodes. Another way is to insert a RREQ packet that replaces RREQ having the low sequence number with high sequence number [5].

Various routing protocols maintain routing tables that hold the information regarding routes of the nodes in network topology. The attacker node generates and sends dummy packets, or shift legal messages from one node to another node which helps them to create fake entries in the tables of the participating nodes.

F. Rushing Attack

In this attack, the attacker node initializes the route discovery process to the destination or node. If all its ROUTE REQUESTS are the first to reach the neighbours of the target node then the route discovered by this Route Discovery includes a hop through the attacker and the neighbouring nodes discard any legitimate requests and it doesnot forward any further REQUESTS from this Route Discovery. Thus the initiator does not find any route that does not include any attacker node or victim node. [6]

G. Blackmail

This is a relevant attack for those routing protocols that use a mechanism to identify malicious nodes present in the network. This attack is basically due to lack of authentication. This allows any node to corrupt other node’s useful information by forging reporting message. These reporting messages are used by routing protocols and tells other nodes to add any node in their network which may also be an attacker node. Thus legitimate node gets isolated from the network [7].

H. The Invisible Node attack

This attack is different from other existing attacks as in this case the attacking node or the victim node is invisible to other nodes. It is relevant for those protocols that are dependent on the identification of the functionality of the nodes. If any node is participating in this protocol without sharing its identity then it becomes invisible to other nodes and termed as INA. This type of attack has not been solved yet. [8].

I. Snare Attack

This attack has been proposed by Lin et. al which is related to military specific applications. In this attack, a node could physically compromise in the same way when a soldier is caught by enemy soldier in the battlefield. Later on, the attacker can easily prevent any transmission and changes in the network with the help of the compromised node, trace the location of VIN and analyze routes. Thus the attacker can easily win the battle by launching a Decapitation Strike on VINs. [9].

J. Byzantine Attack

In this attack, compromised nodes or a set of such compromised nodes work secretly and carry out various attacks such as forwarding packets to non-optimal paths, creation of routing loops and selectively dropping the packets [10]. As a result, the routing service degrades.
It is hard to detect byzantine attack as operation of the network with respect to the nodes seems to be normal but actually it may show byzantine node behavior.

Byzantine attack and “selfish” node problem have some features in common [11] but aim of the nodes in these two models are in contrast. The selfish node aims to gather the advantages of participant nodes in ad hoc network without using their resources whereas in case of Byzantine node, it aims to interrupt the communication of other node regardless of their own resource.

Once the active set of node in the same network gets targeted by the attackers then the whole network will be in the control of attacker and further secure transmission of data in network is not possible. This is an important issue in case of networking devices that are used by military and medical fields for transferring patient reports and advices. This attack drops the route request of node and thus prevents the route discovery process by modifying the route selection metrics such as packet ids, hop counts, randomly packet dropping, creating routing loops, forwarding the packets through the non-optimal paths with the purpose of time and bandwidth consumption.[12]

K. Sleep Deprivation Attack: (AODV-OLSR)

In this attack, the attacker starts a conversation with the target node in a way that seems to be justified but the resources of the nodes are constantly consumed by keeping them busy in routing decisions. The malicious node requests for either existing or non-existing destination nodes continuously, thus forcing the intermediate nodes to forward these packets and as a result uses its batteries and network bandwidth obstructing the normal operation of the network.

It is a kind of flooding attack in which a particular node or a group of nodes are chosen in order to use their resources. This attack can come into effect by forcing the target node to use its resources like battery life, network bandwidth or computing power by continuously sending incorrect RREQ requests for either existent or non-existent destination nodes. In the meantime it will not be able to process the requests coming from correct nodes. It is difficult to prevent and identify this attack. The main aim of the malicious node is to reduce the real nodes lifetime by wasting its valuable resources and thus cannot be distinguished from original request.

K. Colluding Misrelay attack:

In this attack, multiple attackers work secretly with an aim to either modify or drop the routing packets to disrupt the routing operations in MANET.

This attack is hard to detect by using the traditional methods such as watchdog and pathrater. In [13] the authors discuss Colluding misrelay attack in OLSR routing protocol and show that a pair of attacker nodes can interrupt up to one hundred percent of data packets in the OLSR MANET.

M. Sybil Attack:-

In this attack a malicious node contains multiple addresses and behaves as a group of nodes. Sybil node can get an identity in two ways; stealing other node’s identity or obtaining fake identities. By pretending that a large number of nodes is present in the network, the malicious node prevents other nodes from using those addresses. As a result, it can escape from detection systems, and can “out vote” the well-behaved nodes. This attack can severely damage geographic routing protocols, and can harms multiple path routing protocols and node localization. [14][32]

Sybil attack demonstrate itself by allowing the malicious nodes to weaken the network by generating and controlling a large number of duplicate nodes. Each radio represents a single individual and the broadcast nature of radio allows a single node to take identities of many nodes simultaneously while transmitting. The side-effect of this Sybil attack is analyzed using Packet Delivery Ratio (PDR) in the form of performance metric. Theoretical based graphs are simulated to study the effect of Sybil attack in PDR.[15]

N. Jellyfish(JF) attacks.

JellyFish attacks are passive attacks and very hard to detect until after the “sting.” JellyFish attack targets closed-loop flows which are responsive for the network conditions such as loss and delay. For example- TCP flows and congestion-controlled, UDP flows employing a TFRC-like algorithm .[16]The aim of JF nodes is to reduce the output of all traversing flows near to zero but dropping only a small fraction of packets. In particular, JF nodes uses one out of three mechanisms. The first mechanism is a packet reordering attack. TCP has a vulnerability to re-ordered packets due to certain factors. These factors may include route changes or the use of multi-path routing. A number of TCP modifications have been suggested to improve quality in order to prevent incorrect ordering [17, 18, 19, 20].

O. Grey Hole Attack (GH):-

It is a special case of the black hole attack, in which an attacker initially captures the routes, i.e., becomes intermediate node to the routes in the network (as with the BH attack), and then starts dropping packets randomly.
For example, the attacker may drop packets from specific source nodes, or it may drop packets in some other specific pattern. Black hole and Grey hole attacks are very different in nature from packet dropping attacks. In those attacks the attacker simply fails to forward packets for some reason. On the other hand, BH and GH executes in two different ways: Firstly, the attacker captures routes and then either drops all packets (BH attack) or some packets (GH attack) randomly. [21]

Greyhole attack is a refined form of the blackhole attack. In this attack a corrupted node drops only selected packets and forwards the rest of the packets. It can drop the packets depending on the source or the destination of the packets. Another kind of gray hole may behave suspiciously for a specific period by dropping all the packets then switching back to normal behavior later. This attack beats trust-based mechanisms and makes the detection of malicious node more difficult. [22][31]

**P. Replay Attack :-**

In a MANET, node mobility brings frequent change in topology. This concludes that current topology will not be present in the future. In a replay attack, an attacking node records some valid control messages and then resends them later. [23]

This results in recording of routing table of other nodes. Replay attack can be misused to disguise as a specific node or simply to damage the current routing operation in a MANET.

In replay attack, an attacker can retransmit the valid data continuously to push the network routing traffic that has been caught previously. This attack usually targets the freshness of routes, but can also be used to disable incorrectly designed security solutions. [24]

In Replay attack, old control messages are send repeatedly by malicious node that have been transmitted earlier. When other nodes receive these messages, they update their routing tables according to this incorrect information. This results in a view of the network topology that contains errors. Moreover, it also useful to obtain data which was requested by replayed packet in order to damage the usual operation of routing protocol. [25][30]

**Q. Link Spoofing :-**

In link spoofing, a malicious node announces fake links with nodes which are not neighbour to disrupt routing operation.

The Optimized Link State Routing protocol OLSR [26] consists an example for this attack, where malicious node can convince a target node to choose it as an MPR by advertising non-existing links with the target’s neighbors which are two hops away. [25]

A malicious node can then manipulate data or routing traffic, for example, modifying or dropping the control packets or performing various DoS attacks.

**R. Detour**

This attack is also known as gratuitous detour, occurs at the initial phase where the malicious node deflects traffic through congested route, by altering a route request such that it becomes more costly beside another route to which the attacker attempts to transmit traffic. Different ways can be used for this, like increasing the hop count or delaying multiple broadcasting of route requests. [27]

**S. Link Withholding Attack :-**

In this attack, an attacking node does not give any attention to the need to advertise the link of specific nodes or even a group of nodes. This may result in serious loss of links to these nodes. This type of attack is particularly present in the OLSR routing protocol.

**T. State Pollution Attack :-**

In ad hoc network, each mobile node must have a free IP address before its participation in unicast communications. Malicious node can affect the uniqueness of address assigned to node by providing fake responses related to the requested parameters, for example, in best effort allocation; a malicious allocator can always assign the new node an existing node address in topology, leading to multiple broadcast of duplication address detection messages in the network which leads to rejection of new node. [28]

**U. Power Drain Attacks:-**

In this attack [29] the limited resources like battery powers are drained in mobile ad hoc nodes. Once the attacker node becomes intermediate node into the route, it can further flood any node by sending a large number of control packets (route request (RREQ), route replies (RREP) or route error (RRER) packets in AODV routing protocol) to the target node. As a result, the target is always busy processing the incorrect or unwanted packets. This drains the resources of the target node and is considered unreachable by other nodes in the network topology.
III. SIMULATION AND RESULT ANALYSIS

Table 1: Simulation Parameter

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulator</td>
<td>NS-3</td>
</tr>
<tr>
<td>Protocol Studied</td>
<td>AODV, OLSR</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>100 sec</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>700 x 700</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>250</td>
</tr>
<tr>
<td>Node Movement Model</td>
<td>Random waypoint</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR</td>
</tr>
<tr>
<td>Data payload</td>
<td>Bytes/packet</td>
</tr>
</tbody>
</table>

Table 1 Consisting Simulation Parameter from which we can simulate and produce results for performance matrices like PDR, ANT, AEED etc.

Figure 1: Packet delivery ratio for Black hole Attack in AODV and OLSR

From Fig 1-3, the performance analysis it has been successfully analyzed the Black hole attack on AODV and OLSR with respect to different performance parameters such as network throughput, Average end-to-end delay, and packet delivery ratio. Here we conclude that the black hole attack affects AODV protocol highly as compared to the OLSR protocol.
In Fig 4-6, wormhole attack with three different scenarios with respect to the performance parameters of throughput, end to end delay, packet delivery ratio. In a network a protocol should be efficient and effective in terms of security. The research shows that AODV and OLSR are more affected by the wormhole attack when the number of the nodes and the number of route requests is high. Based on the analysis of the traffic via simulation and mathematical results, we have shown that AODV is weaker against wormhole attack as compared to OLSR. Therefore, when more than one attacker exists in the network, the application of MANET that uses proactive routing protocol is preferred as compared to the reactive one.
In Fig 7-9, the impact of gray hole attack on the AODV and OLSR routing protocol has been analyzed. Results clarify the impact of that the gray hole attack is doing much perturbation to the routing mechanism of AODV protocol as compared to OLSR. A number of simulation experiments show the impact of the gray hole attack in MANET. During the simulation of this attack on AODV protocol, the AODV framework limitations and weaknesses were realized. The simulation observation also clarifies the same.
From the fig.10-12, the performance analysis it has been analyzed that when Sybil attack is present the throughput of OLSR gets more reduced in comparison to AODV, though this effect is more pronounced when the number of the nodes is higher in the network. Similarly in the presence of Sybil attack and at a higher network size, the End-To-End packet delay of the OLSR (proactive routing protocol) increases. Network load which is a reflection of total traffic (including overhead and payload) get gradually increased for OLSR as compared to AODV. So it has been concluded that under Sybil attack, reactive routing protocols are less affected than proactive routing protocols.

IV. CONCLUSIONS

In this paper we successfully studied the different types of security attacks and a simulation-based study of the impacts on MANETs by different types of attacks. Here we have considered the attacks like wormhole attack, blackhole attack, Sybil attack and Gray hole attack with respect to AODV and OLSR. We have studied the effect of number of attackers and no. of Nodes on the performance metrics like Network throughput, packet delivery ratio and Average end-to-end delay. Here we have made a conclusion that the effect of the black hole attack, wormhole attack and gray hole attack on AODV protocol is high as compared to OLSR protocol. We have also analyzed that when Sybil attack is present the throughput of OLSR protocol gets more reduced in comparison to AODV protocol. So for using efficient routing we have to consider all the security parameter for applying routing in MANET.

REFERENCES


[34] sunil k.j., Naveen H., “A comprehensive review on detection of wormhole attack in MANET”International Conference on ICT in Business Industry & Government (ICTBIG), indore ,India,2016