ISSN:0975-9646

Impact Analysis and Detection Method of Malicious Node Misbehavior over Mobile Ad Hoc Networks

Priyanka Jain
M.Tech. Research Scholar
SKIT, Jaipur

Mehul Maharshi
Assistant Professor
SKIT, Jaipur

Abstract- At present many researchers working towards the analysis of various attacks that are injected in MANETs and also try to develop solution to either detect or prevent these attacks. The multi-hop communication in MANETs requires intermediate nodes to perform data communication between a source- destination pair. This provides a chance to the attackers to either steel the identity of the legitimate intermediate node or directly become part of the discovered route that will be used for data communication. In this paper, we purposed an attack over MANETs named as Malicious Node Misbehaving Routing Information (MMRI) and analysis its impact on data communication when using a proactive routing protocol. The proactive routing protocol used is well known Optimized link state routing (OLSR) protocol. We use NS-3 simulator to implement the MMRI and simulation results are collected for performance analysis of the underlying network. Various metrics such as packet delivery ratio and network throughput are used to show the effect of the MMRI attack over a wide range of network scenarios.

1. INTRODUCTION: -

Mobile Ad-Hoc network is a system of wireless mobile nodes that self-organizes itself in dynamic and temporary network topologies [1]. MANET's Nodes are connected through wireless links without utilizing the existing network infrastructure or any form of centralized administration. Each node is able to communicate directly with nodes in its transmission range. For nodes outside communication range, intermediate nodes are used to relay the message hop by hop. Hence, such networks are called "multi-hop" networks.

Although MANETs have several advantages over wired networks, on the other side they pose a number of non-trivial challenges to the security design as they are more vulnerable than wired networks [2], [3] due to inherent characteristics and system constraints. The attacks can be launched by nodes within radio range or through compromised nodes. A compromised node may advertise nonexistent or fake links or flood honest nodes with routing traffic causing Denial of Service (DoS) attacks [6] that may severely degrade network performance. A few challenges faced in MANETs are mobility, variable link quality, energy constrained nodes, heterogeneity and flat addressing [4], [5]. To overcome these challenges, there is a need to build a multi fence security solution that achieves both broad protection and desirable network performance.

In this paper, we implemented an attack (MMRI) over MANETs and analyzed its impact on data communication when using a proactive routing protocol (OLSR). In the proposed attack, a malicious node i.e., attacker disseminates wrong network information to its neighbors during the routing table formation and its updation periods. Due to the wrong information spread by the malicious nodes the routing tables of its nearby nodes contains untrue information about routes to various destinations. When this wrong information is used for data communication during the communication process the all the data packets will go to wrong nodes and eventually dropped by some intermediate node.

2. THEORETICAL BACKGROUND OF OLSR: -

The protocol is an optimization of the classical link state algorithm tailored to the requirements of a mobile wireless LAN. Link-state routing algorithms choose best route by determining various characteristics like link load, delay, bandwidth etc. Link-state routes are more reliable, stable and accurate in calculating best route and more complicated than hop count [7]. In OLSR, the problem of duplicate transmissions of a message within a region is addressed through the notion of multipoint relays (MPRs) [8]. MPRs are selected nodes which forward broadcast messages during the flooding process. Route calculations are done by MPR to form the route from a given node to any destination in the network. Each node chooses a subset of nodes in its neighborhood as its MPR and keeps the list of its neighbors which have selected itself as MPR. The shortest path to all shortest destination is then computed from these lists a path between two nodes being a sequence of MPR. MPR node chose to report only links between itself and its MPR selectors. Hence, as contrary to the classic link state algorithm, partial link state information is distributed in the network. . Conceptually, OLSR contain three generic elements: a mechanism for neighbor sensing, a mechanism for efficient flooding of control traffic, and a specification of how to select and diffuse sufficient topological information in the network in order to prove optimal routes [9].

A. Neighbour Sensing: -

Each node must detect the neighbor nodes with which it has a direct link. For this, each node periodically broadcasts Hello messages, containing the list of neighbors known to the node and their link status [9]. The link status can be either symmetric (if communication is possible in both directions), asymmetric (if communication is only

possible in one direction), multipoint relay (if the link is symmetric and the sender of the Hello message has selected this node as a multipoint relay), selected this node as a multipoint relay), or lost (if the link has been lost). The Hello message are received by all 1-hop neighbors, but are not forwarded. They are broadcasted once per refreshing period called the "HELLO_INTERVAL". Thus, Hello messages enable each node to discover its 1-hop neighbors, as well as its 2-hop neighbors. This neighborhood and 2-hop neighborhood information has an associated holding time, the "NEIGH BOR_HOLD_TIME", after which it is no longer valid.

B. Multi Point Relay (MPR):-

The idea of MPR is to minimize the overhead of flooding message in the network by reducing redundant retransmission in the same region. In MPR a node which is selected by its one hop neighbor to "retransmit" all the broadcast messages that it receive from other nodes, provided that the message is not a duplicate, and that the time to live field of the message is greater than one [9]. In OLSR protocol, MPR use of "HELLO" message to find its one hop neighbor and its two hop neighbors through their response. Each node has a MPR selection set, which indicates, which node acts as a MPR. Message is forward after the node gets new broadcast message and message sender's interface address in the MPR Selector Set [12]. MPR Selector Set is update continuously using "HELLO" message which are periodic because neighbor nodes is called of dynamic nature of MANET.

C. Topology Control Information:-

Topology Control messages are diffused with the purpose of providing each node in the network with sufficient link state information to allow route calculation [7]. TC messages are broadcast periodically by a node. Like "HELLO" messages with these TC messages the topological information are diffused over the entire network. A minimum criterion for the node is to send at least the link of its MPR Selector Set [7], [11].

3. MALICIOUS NODE MISBEHAVING ROUTING INFORMATION (MMRI) ATTACK:-

This attack exploits the working of a proactive routing protocol known as optimized link state routing (OLSR) protocol. Due to the dependency on the intermediate nodes during the communication process these networks are open to various forms of attacks. In our proposed attack an attacker node which is an intermediate node on the selected route or a normal node in the network will perform an attack by broadcasting false information in the network through the broadcast control messages. This attack will eventually decreases the network performance in terms of packet delivery ratio, end-to-end delay and network throughput which is undesirable in these kind of networks as these networks are already considered as un-reliable for data communication due to their wireless communication channel and environment conditions.

4. PROPOSED ATTACK WORKING DETAILS:-

In our proposed Malicious node Misbehaving Routing Information (MMRI) Attack an attacker node first obtain the network topology information using the OLSR protocols HELLO and TOPOLOGY control messages that are exchanged by all the nodes in the network to create or update their view to the current network topology. The attacker node exchange HELLO packets with its neighbor node to get the information about its one hop and two hop neighbors. Once this information is collected the node can calculate its multipoint relay set (MPR) which is the set consisting of minimum number of neighbor nodes that together can reach to the entire node's two-hop neighbor.

During the TOPOLOGY control messages which are only forwarded by the MPR nodes the node will sent the information about its MPR set which when received by other nodes in the network they all update or create an entry for the destination nodes. In OLSR protocol the data is forwarded by MPR nodes only therefore, a destination node can receive traffic from one of its MPR node only. The attacker node exploits this functionality of OLSR protocol and put the wrong information in its TOPOLOGY control messages about its MPR set.

The research shows that when a source node receives a data packet from application layer for transmission to a specific destination node it searches its routing table for routes for the destination. The routes in the routing table of a node are created and updated using periodic HELLO control messages and the topology changes are disseminated using the topology control messages.

When an attacker node receives a topology control message it update its routing table with false information i.e., it changes the next hop address for various destinations and also add that he is the next hop address for various destinations in the network. Once this information is stored in its routing table next time when attacker node broadcast the HELLO or topology messages the false routing information in its routing tables are disseminated to its neighbor nodes and then further that information is re-broadcasted in their neighbor nodes. After a while this false information is disseminated in the whole network and each node has false information for the destinations in their routing tables. When this information is used for data packet transmission or forwarding by source or intermediate nodes the data packets reaches to the wrong nodes and those nodes has no way to send them to their destinations. Therefore the nodes start dropping the data packets which decreases the network performance and increases the network overhead and effect of attacks on the underlying network.

5. SIMULATION PARAMETER:-

The attack is simulated on NS-3 simulator. In order to simulate the mentioned attack some significant changes were made to OLSR protocol. Initially the attack was implemented with only one attacker, and later on with multiple attackers. Some basic assumptions were made such as all nodes are placed in a grid and attacker gains complete information about the network topology after a certain period of time known as convergence time. Convergence time is the time taken by OLSR to know about all the network topology. The details about simulation parameters are given in table 5.1.

Channel Capacity	1 Mbps
Convergence Time	25 seconds
MAC Protocol	Wireless(802.11)
Number of nodes	25 to 64 Nodes
Packet generation rate	1 Packet per second
Protocol used	OLSE
Simulation Time	200 Seconds
Simulator	NS 3
Size of Data Packet	512 bytes
Topology	Grid (N X N by default)
Transmission Rate	500 Meter

Table 5.1: Topology Detail

6. Simulation Analysis and Results:-

6.1. 2-Attacker Node: -

For every topology (25, 36, 49 and 64 nodes) packets were sent from source node to all other nodes. A node was chosen as source node while 2 attacker nodes were chosen. From source node 100 packets were sent to each remaining node present in the network in normal condition as well as under attack condition. The attack was simulated in 2 conditions with 2 attackers. In first condition both the attackers are taken at a minimum distance of 4 hopes from each other. Their positions are chosen in such a manner that one attacker is close to the source and other is far from the source.

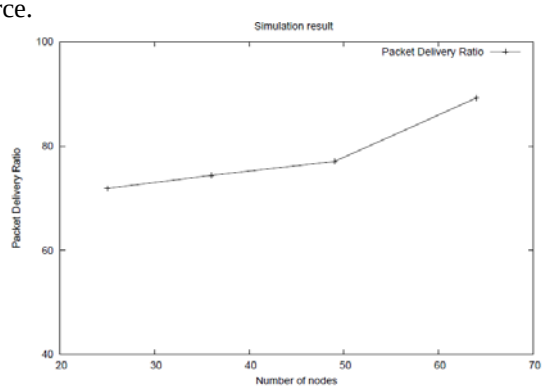

Figure 6.1: Packet Delivery Ratio with different topologies.

Figure 6.2 shows that in presence of 2 attackers distant to each other, more number of packets get dropped. The Packet Delivery Ratio significantly drops by almost 30 percent for smaller topology with 25 and 36 nodes, whereas as it drops by around 40 percent for larger topologies with 49 and 64 nodes than in case of 1 attacker.

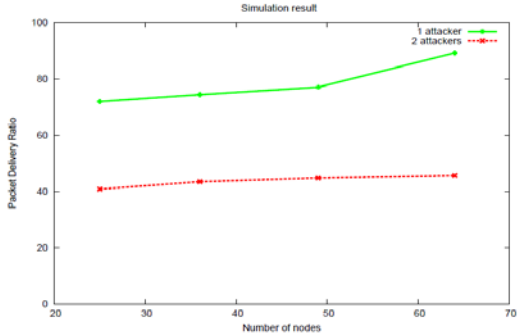

Figure 6.2: PDR comparison in presence of 1 & 2 attackers.

In the Fig. 6.3 we can see that when 2 attackers are taken at a distance of just 2 hops from each other, the attack is much effective only in case of smaller topologies having 25 and 36 nodes. Whereas in larger topologies the effect of attack is less and its almost same as in case of 1 attacker. This behavior is due the fact that the impact of attack is much severe in proximity i.e. Till 3 hops and in larger topologies due to availability of additional routes packets do not get dropped.

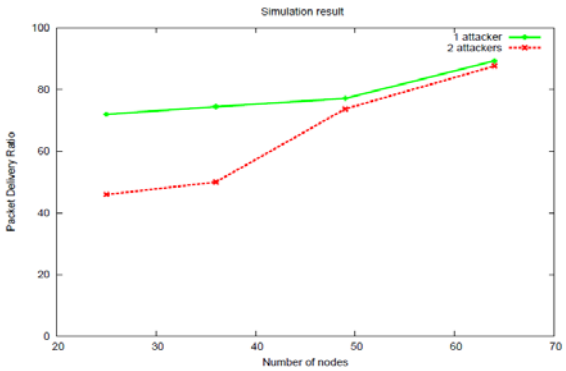

Figure 6.3: PDR comparison with 1 attacker and 2 attackers (Close to each other).

The graph in Figure 6.4 shows the impact of attack in presence of 2 attacker nodes, in both the cases, when attacker nodes are close to each other and when they are distant to each other. Its understood from graph that for 25 and 36 nodes topology, both the attack simulations produce somehow similar impact. In case of 49 nodes and 64 nodes, as seen previously, close attacking positions of attackers makes the attack as if only 1 attacker was present, while in case of distant attackers there a large drop in PDR as shown in graph.

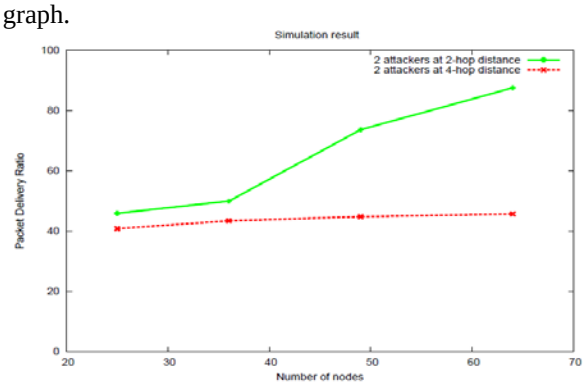

Figure 6.4: Comparison of PDR in case of 2 attackers (having different distances).

6.2. 3-Attacker Node:-

Further the same attack was carried out in the presence of 3 attacker nodes. Same set of nodes were taken again i.e. 25, 36, 49 and 64. All the simulation parameters were kept intact except the positions of attacker nodes. For each topology 3 different nodes were chosen as attackers. Each node was kept at a minimum distance of 2 hops. In some cases the distance between two attacking nodes was taken as 3 also.

This time in the graph figure 6.5 it was observed that the attack makes much more impact on PDR in case of larger topologies also. In previous cases we observed that attack was more effective for smaller topologies than for larger

topologies, whereas with 3 attacker nodes the attack is equally effective and severe in case of large topologies as well as smaller topologies. In this way we find that PDR gets dropped to 40 percent in case of 49 nodes and 64 nodes, which tells the story of success of attack in large topologies as well.

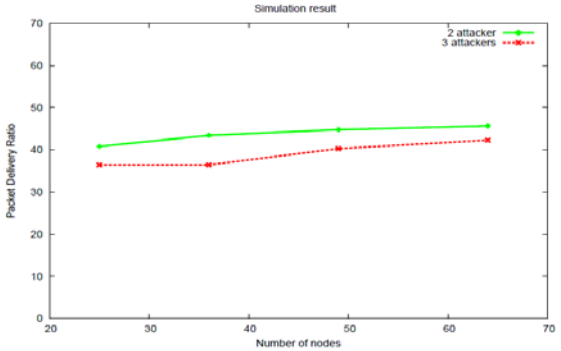

Figure 6.5: PDR comparison in presence of 2 attackers & 3 attackers

7. Proposed Detection Technique:-

In order to detect the presence of a malicious node in the network, the set of MPRs is observed for every node. This observation is carried out every 5 seconds as new TC messages are generated and broadcast after every such interval. Now for a particular node, if a node is becoming its MPR almost all the times, while remaining MPR set keeps on changing, then this MPR node can be an attacker. We maintain a count of occurrence of that node being selected as MPR. If the count exceeds a threshold value within a finite period of time, this node is an attacker which is performing malicious activities.

8. Conclusion and Future Work:-

On the basis of the experimental results that carried out on different network topologies, it is clear that OLSR is vulnerable to attacks. Especially it is prone to routing misbehavior attacks. As we see that in networks based on OLSR an insider node can easily be compromised and much kind of attacks can easily be launched. Though many secure versions have been proposed but only few threats were considered each time.

So a secure version of OLSR is still needed which can detect and remove at least a certain class of attacks. In previous efforts many detection techniques have been discussed, but it is still a challenge to design a complete package of security mechanism which can make OLSR secure enough to stand against one complete class of known attacks, for example all kind of DoS attacks or all kind of routing misbehavior attacks.

As far as for the proposed attack (Malicious Routing Table Exchange attack) a counter-measure is to be designed to remove the attack completely. However routing misbehavior attacks have been carried out in past as well and some detection techniques as well as counter measures are also present, but in our attack the method is slightly different, so there has to be some different countermeasure.

References:-

[1] Kortuem.G., Schneider. J., Preuitt.D, Thompson .T.G.C, F'ickas.S. Segall.Z: "When Peer to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks". 1st International Conf. on Peer-to-Peer Computing, August, Linkoping, Sweden, pp. 75-91 (2001).

[2] ao Yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: Challenges".

[3] S. Floyd and T. Henderson. "The newreno modification to TCPs fast recovery algorithm", IETF RFC 3782. October 1999.

[4] yoti Jain, Mehajabeen Fatima, Dr. Roopam Gupta. "Overview and Challenges of Routing Protocol And MAC Layer in MANET". Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT.

[5] Aarti, Dr. S. S. Tyagi. "Study of MANET: Characteristics, Challenges, Application and Security Attacks". Volume 3, Issue 5, May 2013 ISSN: 2277 128X

[6] Monika Ropak, Prof. BVR Reddy. "Black hole Attack Implementation in AODV Routing Protocol". ISSN 2229-5518, IJSER © 2013 http://www.ijser.org

[7] Enthony busson, Nathalie Mitton, Eric Fluery. "Analysis of Multipoint Relay selection in OLSR and Implication". CITI/INSA Lyon-INRIA Villeurbanne F- 69621.

[8] Amir Qayyum, Laurent Viennot and Anis Laouiti "Multipoint relaying: An efficient technique for flooding in mobile wireless networks", INRIA research report RR-3898,2000.

[9] T.H. Clausen,et al, "The optimized link state routing protocol evaluating through experiments and simulation", mindpass center for distributed system, Aalborg university Denmark.

[10] T. Clause .et al, "Optimized link state routing protocol", IETF.org/rfc3626.txt, Oct. 2003

[11] P. Jacquet et al, "Optimized Link State routing protocol", draft –ieff-olsr-04.txt-work in progress, March 2001.

[12] Erwan Ermel, Paul Muhlethaler. "Using OLSR Multipoint Relays (MPRs) to estimate node positions in a wireless mesh network". Inria-00121425 version 1-20 Dec-2006.