Review On Rushing Attack And Its Prevention Techniques In MANET

R.Thilagarasi,
M.Phil Scholar, Department of Computer Science,Sree Saraswathi Thyagaraja College,Pollachi, Tamil Nadu, India-642 107.
Email: thipuvi@gmail.com
D.Geetha
Assistant Professor, Department of Computer Applications,Sree Saraswathi Thyagaraja College,Pollachi, Tamil Nadu, India-642 107.
Email: geetha_d74@yahoo.co.in

---**ABSTRACT**--

A Mobile ad hoc network is a self- organizing mobile nodes which doesn't have any topology and the communication is achieved by means of wireless links. The nodes in MANET are free to move to achieve mobility technique. MANET doesn't have any fixed infrastructure for communication so the nodes in network can free to move from one network to another. There is no centralized administration such as access point or base station. These features may lead the mobile node in several security attacks. In this paper we discuss about the cause of rushing attack and its various prevention methods. Rushing attack makes the packet to drop while travelling or it may result in denial of service (DOS). In this attack the attacker uses the duplicate suppression mechanism to quickly forward the route request packet to gain access with the destination than any other legitimate node. By reaching first to the destination, attacker can know the data shared by both source and destination. The protocols designed for MANET will prevent the nodes from many types of attacks during communication.

Keywords**: DOS,MANET,security attack, Rushing attack.**

----

1. INTRODUCTION

In MANET the nodes can join and leave the network randomly without warning and possibly without disturbing other nodes in the communication network. There are many challenges facing MANETs, such as power, unreliable physical channels, range limitations and half of the dual wireless without the support of any infrastructure. MANETs are more vulnerable to security attacks due to the lack of trusted centralized control, easy eavesdropping, dynamic change in network topology, and limited resources. The properties of MANET are as follows:

- May need to travel multiple links to reach the target destination.
- Mobility causes route changes.
- Routes between nodes potentially contain multiple hops.
- Don't need a pre-existing infrastructure i.e., don't need a built-in or defined network, routers, etc.,

Based on operation, attacks on MANETs are categorized in to passive and active attacks. In Passive attack the attacker snoops the data exchanged in the network without altering it. In active attack the attacker alters the data or destroys the data during transmission. The MANET protocols are classified as proactive, reactive and hybrid protocols. In proactive protocol every node in the network maintains the network topology information in the form of routing tables. Examples of proactive routing protocols are DSDV (Destination Sequence Distance Vector) protocol, WRP (Wireless Routing Protocol). The reactive protocol obtain routes only on demand which include DSR (Dynamic Source Routing) protocol, AODV (Ad Hoc On-demand Distance Vector) protocol etc., The Hybrid protocol is the combination of two protocols like globally reactive and locally proactive. Example: Zone Based Routing Protocol (ZRP).

2. RUSHING ATTACK - AN OVERVIEW

The rushing attack uses duplicate suppression mechanism by quickly forwarding route discovery packets, in order to gain access to the forwarding group. The RREQ packet in On Demand Routing protocol is forwarded to find route to reach destination. On Demand Routing protocols minimizes the overhead of network by sending first route request packet to the destination in order to find route. The attacker in the communication network gets RREQ packets from source or nearby other legitimate nodes then forward it to reach destination quickly than any other nodes in the network. The destination node thoughts it as a true RREQ packet sent by authenticate node. So, it will discard other lately arriving RREQ packet and established the route between source and destination with attacker in middle to gain access between two nodes. The attacker in rushing attack can be anywhere in the network [4][6] like as follows:

2.1 Attacker at near sender

The attacker node A is at near sender. The RREQ packet originated from S the source node forwards the request packet to A & B, A is the attacker node, quickly forwards the packet to C than B, then the packet from C reaches R quickly than other legitimate node.

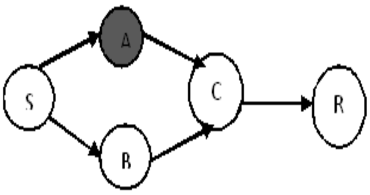

Fig:1 Attacker node near sender

2.2 Attacker at near receiver

The attacker node A is at receiver end. Here the RREQ packet initiated from S the source is forwarded to B & D, B forwards it to C, D forwards the packet to A & C, attacker node A then forwards it to reach destination R than the node C. Finally R discards the lately arriving packet from other legitimate node.

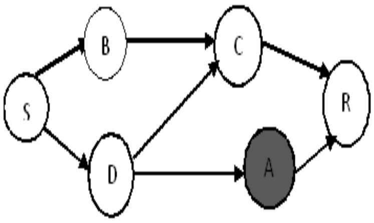

Fig:2 Attacker node near receiver

2.3 Attacker anywhere in the network

The attacker node A is in middle of the network. The route request packet is initiated by S the source, will forwards it to B & D, the B node forwards it to C, D forwards the packet to C & A, E gets the request packet sent by the attacker node A than C. Finally the receiver R receives the request packet sent by attacker node than any other node.

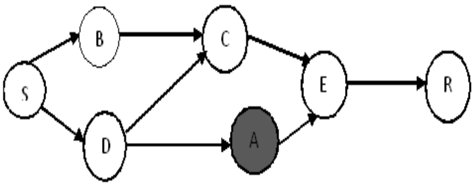

Fig:3 Attacker node at anywhere in the network

3. RELATED WORKS IN RUSHING ATTACK PREVENTION TECHNIQUES

The rushing attack in MANET acts as an effective denial-of-service attack against all proposed on-demand routing protocols to send the data. The On Demand Routing protocol establishes the route to reach destination by sending the only one copy of Route Request packet without flooding all packets at once to all its neighbor nodes. In particular, existing on-demand routing protocols such as AODV, DSR, LAR, Ariadne, SAODV, ARAN, AODV secured with SUCV and SRP only forward the REQUEST that arrives firstfrom each Route Discovery. In rushing attack, the attacker exploits this property of the operation to discover route.

3.1 Secure Neighbour Detection

In Standard Neighbour Detection [1][8] method the node in the network broadcasts its route request packet. The nearby node which received the route request packet treats that sender node is neighbour node which is true to communicate. So it establishes the communication with that node. This may result in attacker can also get in between the two nodes which needs to communicate each other.

This was overcome by Secure Neighbour Detection mechanism. By this the nodes in network verifies that the nearby node is within the normal radio transmission range to establish communication. The functionality of Neighbor Detection is to detect a bidirectional link between two nodes, in some form almost every routing protocol.

3.2 Secure Route Delegation

In route request propagation, we want to enable each node to verify that all the Secure Neighbour Detection[1] steps were performed between any adjacent pair of nodes in the REQUEST, i.e., verify that both nodes of each adjacent node pair indeed believes to be a neighbour. This is achieved by the Secure Route Delegation mechanism by enable the nodes to verify that all Secure Neighbour Detection was achieved. The two nodes which sent and received the REQUEST are within the transmission range of the network was analysed by this mechanism.

3.3 Specifying Timeout

In rushing attack, attacker forwards RREQ packet very quickly compared to legitimate nodes. Threshold value [8] is fixed time interval. Threshold value is given to all nodes and there is an instruction to all nodes that, the route request packet should reach after the threshold time value. The rushing attacker forwards RREQ quickly, so that route request packet (RREQ) will reach neighbor node before the timeout threshold value. So that RREQ from other legitimate nodes will not be considered and neighbor can identify the attacker

3.4 Randomized message forwarding

In traditional route request forwarding, the receiving node immediately forwards the REQUEST and suppresses all subsequent Requests done in DSR and SDSR routing protocols. In modified flooding [1][2][10], a node first collects a number of requests, and selects a REQUEST at random to forward. There are thus two parameters to our randomized forwarding technique like i) The number of REQUEST packets to be collected, and ii) The algorithm by which timeouts are chosen. If the number of REQUESTs is chosen to be too large, randomized forwarding will heavily rely on the timeout to trigger REQUEST forwarding, increasing latency and possibly reducing security.

3.5 Method based on Path Value

The attacker node can also identified by using the path value and its average value in the network [3]. The Rushing attack enters in the network as follows:

- Source node sends RREQ packet to all nodes which are near to it.
- If the target node got identified it establishes communication else it forwards the RREQ packet in path
- The attacker may present in the path in such case the attacker uses the duplicate suppression mechanism by quickly forwarding the RREQ packet.
- On receiving, the destination sends the RREP packet back to sender. Destination discards the other RREQ packet which lately arrives to it.

Identifying the attacker node in network is follows

- The source node broadcasts its RREQ packet to all neighbours. On receiving end the RREQ packet checks for its destination address.
- If request packet attains the target node it checks for source address to send RREP packet as acknowledgement to source node.
- The source node estimates the average of all nodes acknowledgement time called threshold value.
- Source node adds this threshold value with individual RREQ packet sending time to its neighbors called path value (i.e.,) addition of threshold value and RREQ packet sending time. Then calculate average of path value.
- If the node's path value is greater than average path value the source node selects it and made further analysis.
- The further analysis is made only if more path values are greater than average path value. As a result source node selects the path value which is closer to the average path value.

The node with path value less than average time of path value is treated as rushing attacker to attain the access between two nodes.

3.6 Prevention of Rushing Attack in Cluster

A group of nodes which are near can form the cluster. The rushing attacker enters in cluster [4] is identified as follows:

- Genuine node sends cluster solicitation to the neighbouring nodes in a cluster.
- Rushing attacker keeps track.
- Rushing attacker sends cluster solicitation message to the neighbouring nodes of the cluster.
- If all neighbours of the cluster busy means the genuine node does not get cluster advertisement.
- The genuine node is deprived of the entry into the cluster.
- If all neighbours of the cluster are not in busy mode the rushing attacker repetitively sends the cluster solicitation message.

The prevention technique for this cluster is by calculating the transmitting frequency. The nodes in cluster checks for any malicious node arrived or not. The neighbor nodes will inform to the cluster head and to other nodes about the malicious node. The cluster head calculates the transmit frequency of the malicious node. If the attackers transmit frequency is greater than the normal frequency then it will inform to all other nodes in cluster to suspect the link with that malicious node.

4. IMPACT OF RUSHING ATTACK IN DOS

The rushing attack is also one type of denial of service attack against all currently proposed on-demand ad hoc network routing protocols including the ones that are secured. This type of attacks can be done by two ways [9] (i) sending route request packet with fake IDs and (ii) sending route request packet to a fake destination. An attacker may impersonate the mobile node by spoofing its IP and frequently sending route request packet for the same destination, causing the denial of service attack at the destination. Further the rushing attacker can send a route request packet for an invalid destination causes the intermediate nodes to send the message many times. This leads to denial of service because intermediate nodes are supposed to sign all the route requests (RREQ) they are broadcasting.

5. CONCLUSION

Rushing Attack in MANET uses duplicate suppression mechanism to forward route request packet quickly to reach the destination. While using On Demand Routing protocol to discover routes there is a chance of security attacks. In this paper various prevention techniques for rushing attack have been discussed. The protocols used for route discovery may use these mechanisms to strength its security. Due to Rushing Attack the network performance gets degrade or may result in loss of data during transmission.

REFERENCES

[1] YihChun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols".

[2] Aakanksha Jain, Samidha Dwivedi Sharma, "An Efficient Rushing Attack Prevention Algorithm for MANET Using Random Route Selection", *International Journal of Science and Research (IJSR)*, ISSN (Online): 2319-7064.

[3] Satyam Shrivastava , Dharmendra Mangal, "A New Techniqu e to Prevent MANET against Rushing Attack", *International Journal of Computer Science*

and Information Technologies, Vol. 5 (3) , 2014, 3460-3464.

[4] Rusha Nandy, Debdutta Barman Roy, "Study of Various Attacks in MANET and Elaborative Discussion of Rushing Attack on DSR with clustering scheme", *International Journal ofAdvanced Networking and Applications,* Volume: 03, Issue: 01, Pages:1035-1043 (2011).

[5] V. PALANISAMY, P.ANNADURAI, "Impact of Rushing attack on Multicast in Mobile Ad Hoc Network", *Journal of Computer Science and Information Security,* Vol. 4, No. 1 & 2, 2009.

[6] Satyam Shrivastava, "Rushing Attack and its Prevention Techniques", *International Journal of Application or Innovation Engineering & management,* Volume 2, Issue 4, April 2013, ISSN 2319 – 4847.

[7] Meena Bharti1, Manish Goyal2 and Rajan Goyal3," Detection of rushing attack by comparing energy, throughput and delay with AODV", IPASJ *International Journal of Computer Science,* Volume 2, Issue 11, November 2014.

[8] Chinkit Suthar, Bakul Panchal, "A Survey on Rushing Attack and Its Prevention in Mobile Ad-hoc Network", *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 4, Issue 3, March 2014, ISSN: 2277 128X.

[9] Sushant Kumar, Bibhudatta Sahoo, "Effect of Rushing Attack on DSR in wireless Mobile Ad hoc Network".

[10] Aakanksha Jain, 2Dr. Samidha Dwivedi Sharma, "Rushing attack prevention algorithm for manet using random route selection to make DSR and AODV more efficient", *International Journal Of Engineering And Computer Science,* Volume 3 Issue 6 June, 2014 Page No. 6520-6524.

[11] Gajendra Singh Chandel, Rajul Chowksi, "Study of Rushing Attack in MANET",*International Journal of Computer Applications,* Volume 79-No10, October 2013.