Prevention of Multiple Rushing Attack Nodes in Multicast MANET

R.Thilagarasi [1], D.Geetha [2]
[1]*M.Phil Scholar, Department of Computer Science,*
Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India-642 107.
[2]*Assistant Professor, Department of Computer Applications,*
Sree Saraswathi Thyagaraja College, Pollachi, Tamil Nadu, India-642 107.

Abstract *- Wireless networks use radio frequencies in air to transfer and receive data instead of using physical cables. According to wireless network, Mobile ad hoc network is a self- organizing mobile nodes which doesn't have any topology, communication is achieved by means of wireless links. Security in Mobile Adhoc Network is a big challenge as it has no centralized authority. One of the security attacks is the Rushing Attack, which results in loss of data while delivering packet to right destination. Rushing attack quickly transmits the route request packet using high transmission power. In this paper we discuss about the prevention of Multiple Rushing attacks in Multicast MANET. The solution to prohibit the multiple Rushing Attackers in Multicast MANET is by using Ant Colony Optimization Boolean Expression Evolver Sign Generation (ABXES) algorithm and fixed threshold value for transmission speed (time) of packets at each node.*

Keywords *– Rushing attack, MANET, Multicast MANET, ABXES, Transmission speed*

I. INTRODUCTION

In MANET the nodes can join and leave the network randomly without warning and possibly without disturbing other nodes in the communication network, because mobile nodes are free to move in and around the network. There are many challenges facing MANET like power, unreliable physical channels, range limitations and half of the dual wireless without the support of any fixed infrastructure. MANETs are more vulnerable to security attacks due to lack of centralized control, easy eavesdropping, dynamic changes in mobile network topology, and limited resources.

The characteristics of MANET

- MANET is an infrastructure less network which has no central server, or specialized hardware and fixed routers.
- The nodes in MANET can act as both host and routers.
- The mobile hosts are small, light- weight and are supplied with limited power resource like battery.
- The network topology may change randomly due to movement of mobile nodes.
- The network setup can be made available on any place and time.

A. Attacks in MANET

Attacks in MANET can be classified on the basis of behaviour are given below,

i) Passive attack:

In this type of attack the attacker snoops the data exchanged in the network without altering it. To prevent legitimate nodes from these attacks powerful encryption techniques can be applied so that attacker is unable to crack the security. E.g.: Traffic analysis..,

ii) Active attack:

In this type of attack the attacker alters the data or destroys the data during transmission. E.g.: Denial of Service attack.,

Attacks in MANET can be classified on the basis of domain are given below,

i) External attack:

Attacks are carried out by the nodes that do not belong to the domain of the network (i.e.) unauthorized node in the network.

ii) Internal attack:

Attacks are performed by the nodes which are actually part of the network.

II. RUSHING ATTACK

In Rushing Attack the source initiates the route request packet, malicious node present in the network receives the request packet and floods it over the network to reach destination quickly. The destination node discards all other original request reply packet by accepting the fake RREP packet which comes early. In rushing attack the attacker quickly forward the packet by using duplicate suppression mechanism which forwards the route request packets quickly to reach destination than other true nodes. The RREQ packet in On Demand Routing protocol is forwarded between all nodes in the network to find route to reach right destination. The On Demand Routing protocols minimize the overhead of network by sending first route request packet to the destination in order to find route. The attackers in the communication network gets RREQ packets from source or from near by other legitimate nodes then forwards request packet to reach destination quickly

than any other true nodes packet in the network. On receiving request packet, the destination node thoughts it as a true RREQ packet sent by authenticate node only. So, it discards other lately arriving RREQ packet and established the communication route between source and destination with attacker in middle to transfer data packet. The attacker in rushing attack can be anywhere in the network [10] like follows:

A. Attacker at Near Sender

The below Fig: 1 shows node A as attacker which is near to sender node S. The RREQ packet originated from S the source node forwards the route 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 the packet which arrives through legitimate node B.

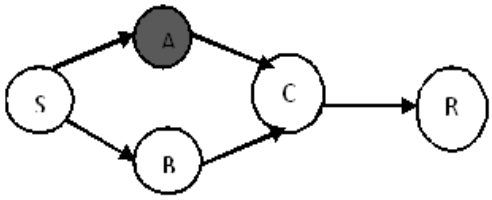

Fig:1 Attacker node near sender

B. Attacker at Near Receiver

The below Fig: 2 shows node A as attacker which is near to receiver end. Here the RREQ packet initiated from S the source is forwarded to B & D, B forwards it to C node, D forwards the packet to A & C, attacker node A then quickly forwards request packet to reach destination node R than the node C. Finally node R discards the lately arriving packet from legitimate node C.

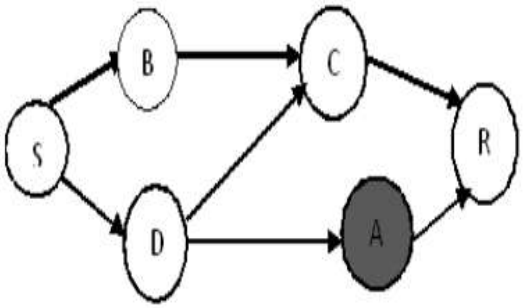

Fig:2 Attacker node near receiver

C. Attacker Anywhere in the Network

The attacker node A is in middle of the network as shown in below Fig: 3. The route request packet is initiated by source node S which forwards request packet to nodes B & D, the B node forwards it to C, node D forwards the packet to C & A, node E gets the request packet sent by the attacker node A than C. Finally the receiver R receives the route request packet sent by attacker node A than other legitimate node C.

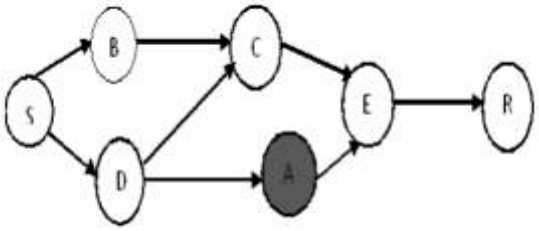

Fig:3 Attacker node anywhere in the network

III. MULTICAST MANET

Multicast is communication exists between single sender and multiple receivers on a network. Otherwise it transfers a single message to a selected group of recipients in the network. Multicast communication works well in streaming video, in which many megabytes of data are sent over the network. Single packet is copied by the network and sent to a specific subset of nodes in the network. The node addresses are specified in the destination address. Protocol used for point to multipoint communication allows efficient distribution of packets frequently used in access grid applications. Multicasting greatly reduces the transmission cost when sending the same set of data packet to multiple recipients. The option to multicast communication was made possible by digital technology to allow each digital broadcast station to split its bit stream into 2, 3, 4 or more individual channels of programming and data services. Instead of using multiple unicast transmissions, it is more advantageous to use multicast mode of communication which saves cost, bandwidth and resources. Since a single message can be delivered to multiple receivers in the network simultaneously at very short period. Multicast data packets may still be delivered to all targeted destination on alternative paths even when the route breaks.

Multicasting is efficient mode of communication because it provides data from single source to group of receivers simultaneously. The multicast group is composed of many senders and receivers. For connecting senders and receivers, each protocol constructs either a tree or a mesh as the routing topology. There are some nodes called forwarding nodes in the routing topology that are not interested in multicast packets but act as routers to forward packets to targeted receivers. In MANET multicasting is established by using different protocols[11] like MAODV (Multicast Adhoc On-Demand Distance Vector protocol), ODMRP(On-Demand Routing Protocol), MZRP(Multicast Zone Routing Protocol), etc.,

IV. EXPERIMENTAL RESULTS

The detection of Rushing attack was simulated in Network Simulator (NS-2.35) which is occur in network layer of the protocol stack. The simulator uses 50 numbers of mobile nodes. The simulator was running on Intel based machine having 2.30 GHz processor and 2.0 GB RAM.

The number of data sessions was held constant to limit the number of variables in the experiment because of the time required to run the large simulations with more data sessions. The simulation runs the experiment with 50 numbers of nodes.

The solution to prohibit the multiple Rushing Attackers in Multicast MANET is by using two different techniques. First technique is by using a special algorithm called Ant Colony Optimization Boolean Expression Evolver Sign Generation (ABXES) algorithm[7] which results in detecting the attacker node while establishing the zones in network topology. The second technique is by using fixed threshold value for transmission speed (time) of packets at each node which detects the rushing attacker while transferring the request packet to establish the attacker free route to reach destination [9], [11], [12].

Default parameters are shown in the below table

TABLE I
Default Parameters

PARAMETER	VALUE
Number of Nodes	50
Routing Protocol	MZRP
Key Value	NodeId with energy and Transmission Speed of Packet
Channel Type	Wireless Channel
Antenna Type	Omni Antenna
Maximum Packet Size	256

A. Packet Delivery Ratio

In general, PDR is defined as the ratio between the received packets by the destination and the generated packets by the source. In NS2 the packet delivery ratio the calculation of Packet Delivery Ratio (PDR) is based on the received and generated packets as recorded in the trace file.

PDR = (No of Packet Received / No of Packet Sent) * 100

The graph analyze the packet delivery ratio result in case of under security and under attack.The result is shown in the below graph Fig: 4.

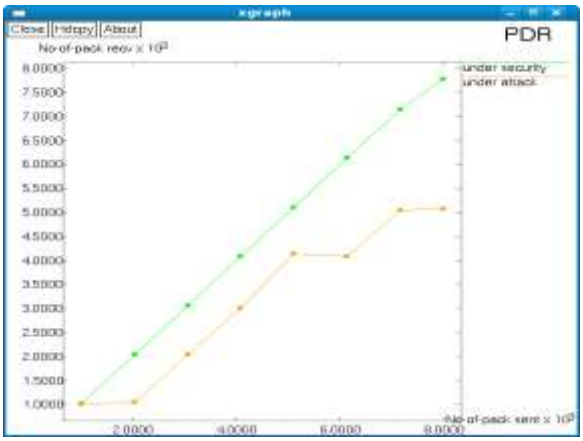

Fig: 4 Graph for packet delivery ratio

B. End-to-End Delay

The packet End-to-End delay is the average time that a packet takes to traverse the network. Time from the generation of the packet in the sender up to its reception at the destination's application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges. The graph analyse the packet end-to-end delay result in case of under security and under attack. The result is shown in the below graph Fig: 5.

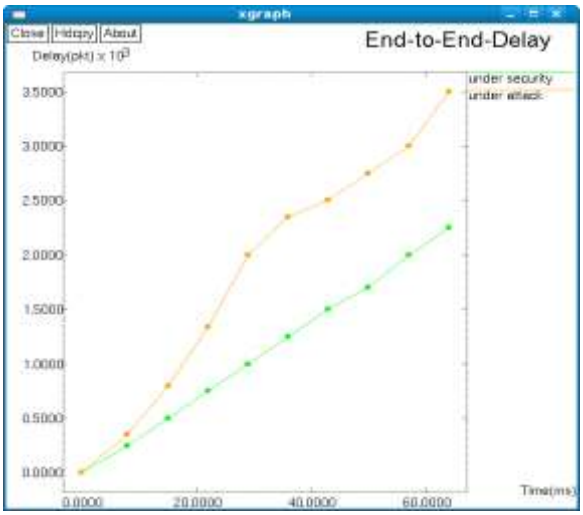

Fig: 5 Graph for end-to-end delay

C. Throughput

Throughput is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet. Analysis of throughput graph is done in three different cases, in

that Proposed MZRP (preventing multiple rushing attack) shows good result. The result is shown in the below graph Fig: 6

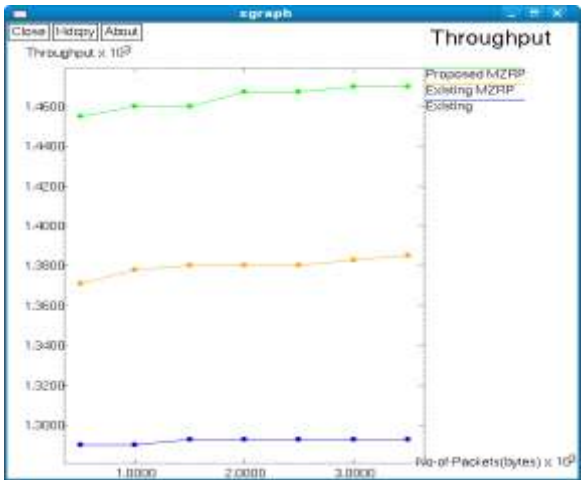

Fig: 6 Graph for throughput

D. Broadcasting

Broadcasting is the process in which a source node sends a message to all other nodes. When the size of the network increases and the network becomes dense, even a simple broadcast operation may trigger a huge transmission collision and contention that may lead to the collapse of the whole network. Thus broadcasting scenario is estimated in the graph format for easy analysis of broadcasting a packet. The result is shown in the below graph Fig: 7.

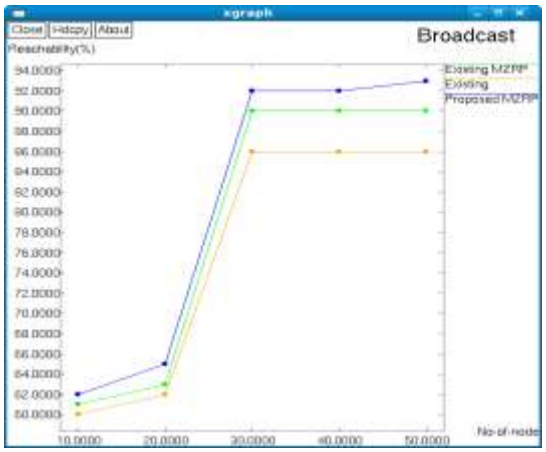

Fig: 7 Graph for broadcasting of packets over 50 nodes

The network performance in simulated environment are measured in case of throughput, end-to-end delay, packet delivery ratio, broadcasting., shows the proposed technique improves the network security by blocking the attacker node in further communication.

V. CONCLUSION

Detection of rushing attack is easy, but prevention of rushing attack is difficult because it needs to provide attacker free route to forward packets. Preventing attack node is by blocking that corresponding node for further communication. This is achieved by using the alert message sent to all other legitimate node about the attack node. Rushing Attack identified in this research is by comparing the key value and threshold value given to all nodes in the framed network. Key value is used when establishing the zone inside the network and threshold value is compared with the transmission speed of the packet to identify attack node. The performance of network is compared in presence of attacking node and its prevention method. The result is shown in case of packet delivery ratio and throughput which gives better performance when security technique is applied. Throughput and broadcast are also estimated in these cases which show best result in proposed technique.

VI. FUTURE ENHANCEMENT

This research prevents the Rushing Attack by blocking that node for further communication, and sends an alert message to all other nodes about invading of attacker node. Analyzing the performance of network in case of under two scenarios:

1. This work can be extended to future as identifying Multiple Rushing Attack and preventing it in multiple senders and multiple receivers environment using algorithm which prevents attack completely.
2. Another future work can be, to implement the Ant Colony Optimization Boolean Expression Evolver Sign Generation (ABXES) algorithm to identify and prevent many different types of attacks which occur in MANET.

REFERENCES

1. 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.
2. Athira V Panicker, Jisha G, "Network Layer Attacks and Protection in MANET –A Survey" *International Journal of Computer Science and Information Technologies*, Vol. 5 (3) , 2014, 3437-3443
3. Chander Diwaker, Sunita Choudhary, Poonam Dabas, "Attacks On Mobile Ad-Hoc Networks", *International Journal of Software and Web Sciences*.
4. Dewan Tanvir Ahmed, "Multicasting in Ad Hoc Networks", University of Ottawa
5. M.Jayaraman, Dr.M.Gunasekaran, Dr.K.P.Rajesh, " A Survey on Security Issues of Multicast Routing Protocols in MANET's", *International Journal of Scientific Research in Computer Science Applications and Management Studies*, ISSN 2319 – 1953, Volume 3, Issue 3 (May 2014)
6. Meena Bharti, Manish Goyal 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.

7. N.K. Sreelajaa, G.A. Vijayalakshmi Pai, "Swarm intelligence based approach for sinkhole attack detection inwireless sensor networks", *Applied Soft Computing* 19 (2014) 68–79
8. Nisha Dang, Pooja Mittal, " Cluster Based Intrusion Detection System for MANETS", *International Journal of Computer Applications & Information Technology*, Vol. 1, No.1, July 2012
9. Satyam Shrivastava , Dharmendra Mangal, "A New Technique to Prevent MANET against Rushing Attack", *International Journal of Computer Science and Information Technologies*, Vol. 5 (3) , 2014, 3460-3464.
10. 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.
11. Shaveta Jain, Kushagra Agrawal, "Prevention Against Rushing Attack on MZRP in Mobile Ad-Hoc Networks" *IJCST* Vol. 5, Iss ue 3, July - Sept 2014
12. 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.
13. Wilson Prakash. S , Sankaranarayanan S, "Solution To Prohibit Rushing Attack In MobileAd-Hoc Network*", International Journal on Applications in Information and Communication Engineering*, ISSN (Online) : 2394-6237,Volume 1: Issue 9: September 2015, pp 1-5
14. YihChun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols".
15. "Rushing attack against routing protocols in Mobile Ad-Hoc Networks" *Biometrics and Security Technologies (ISBAST), 2014 International Symposium* on 26-27 Aug. 2014