© 2014 IJEDR | Volume 2, Issue 4 | ISSN: 2321-9939

Rushing Attack Prevention with modified AODV in Mobile Ad hoc Network

[1]Chinkit Suthar, [2]Bakul Panchal
[1]Student-ME(CSE), [2]Assistant Professor
[1]Comp uter Science and Engineering Department,
[1]L.D. C ollege of Engineering, Ahmedabad, India

***Abstract* - Mobile Ad-hoc Network contains autonomous system of mobile nodes which can move freely and communicate to each other without fixed infrastructure. These nodes work either as router or host. In MANET there is no centralized controlling authority and topology is not static. So this network is more vulnerable compared to wire d and wireless network. Many protocols in MANET work as on demand fashion like AODV. Rushing attacker exploits the duplicate suppression mechanism of AODV, to perform the attack. In this paper we have discussed about the rushing attack and its prevention technique. By modifying some property of AODDV, the attack can be avoided or the effect of the attack can be reduced. We have shown the results of prevention and the effect of the prevention to different size of network and different numbers of attackers.**

***Key Words* - Rushing Attack, Rushing attack Prevention, MANET**

I. INTRODUCTION

A mobile ad-hoc network is an autonomous system of mobile nodes which communicates to each other via wireless links. MANET is an infrastructure less network. Network topology is dynamic which changes with time. Mobile nodes can be in the bus, train, building, military vehicle etc. There is no centralized controlling authority in the network. Mobile node works as routers to transmit the network information and also works as a host. As there is no centralized controlling authority, the network is more vulnerable. Attacker can easily participate in communication in the network and may affect the network.

Mobile ad hoc network works mainly on two types of protocols: Reactive and Proactive. Reactive protocol is a table driven and Proactive is an on demand protocol. In an on demand protocol, performs path discovery when it wants to perform transmission. In this, sender sends request packet for path discovery and receives response from destination on successful completion.

MANET is wireless and dynamic topology network. So there are vulnerabilities like limited band width, lack of centralized authority, resource constraint, limited power supply, etc. So MANET is more vulnerable than the wired and wireless network.

There are many security issues due to its chracteristics in MANET. In MANET attacker can get easily participate as a router or a host in the transmission. There are different routing protocols in MANET. Routing protocols in MANET are mainly two: Proactive, which stores and updates the information of network in router tables. Examples are OLSR, DSDV, etc. Second is Reactive or on demand, which performs route discovery on request of sender for transmission. Examples are AODV, DSR, SAODV, etc.

Hu, Perrig and Johnson has introduced the attack in MANET, “rushing attack” in their paper [1]. They also presented Rushing Attack Prevention Component to prevent the rushing attack. That can be used for on demand protocol to prevent rushing attack. In this paper there is introduction of rushing attack, its prevention technique and simulation results and it s analysis.

II. RUSHING ATTACK

In MANET there are different types of proto cols like routing protocols or table driven protocols and on demand protocols. In On demand protocols sender floods REQUES T packets to all the neighbors. In AODV protocol, to avoid the duplication of REQUEST packet, only first REQUEST is forwarded and other are discarded. Hu, Perrig and Johnson h ave shown in their paper that for Rushing Attack, attacker exploits this ch aracteristic of AODV to perform attack [1].

When sender wants to communicate with other node, it performs route discovery. In that, it floods RREQ packets to neighbours, neighbours floods to their neighbors and so on until destination gets the request. If attack er is able to forward the REQUEST packet to neighbor of the destination first compared to other legitimate nodes, then the route which includes the attacker will be discovered. As the REQUEST s from other legitimate node arrive later, they are discarded as duplicates. So the legitimate nodes will not be able to communicate with destination. So, rushing attack leads to Denial of Service attack [1].

In figure 1, S is a sender node and D is a destination node. A is an attacker node. B, C, E and F are intermediate legitimate nodes. S wants to communicate with D. Now in on demand protocol, route discovery should be performed for transmission. So, S will forward Route Request packet RREQ to all its neighbors. RREQ from S will be received by A, B and C. Now, They will forward RREQ to their neighbors. Attacker A will forward RREQ to its neighbors quickly compared to B and C. So, E will receive the RREQ from A earlier compared to B. So, E will forward the RREQ to D, which is received from A. E will receive the RREQ from B later, so it will be discarded as duplicate packet. RREQ from F will also arrives at D after the RREQ of E. So, RREQ from F will be also discarded as duplicate packet. D will send the response to S, by the route it receives the request. So communication route is discovered which contains the attacker A. So A can easily perform attack and does not let other legitimate nodes like B, C and F to communicate.

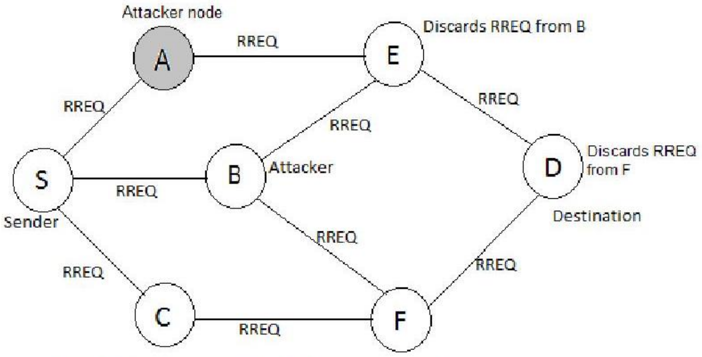

Fig 1 Example of Rushing Attack formation

As discussed earlier, rushing attacker performs attack by quickly forwarding request packet to destination compared to other legitimate nodes. Attacker may use different techniques for quickly forwarding the request packet.

Ignoring delay at either MAC or Routing layer:

There is delay between packet is accepted and packet is transmitted in MAC layer protocol. Node waits for allowed time slot to transmit the packet to avoid collision in transmission. If there is no delay by MAC, on-demand protocols generally specify a delay between receiving a REQUEST and forwarding it, to avoid collisions of the REQUEST packets in transmission [1]. Attacker ignores delay by MAC or routing protocol for transmitting request packet. So it can forward the REQUEST packet quickly, compared to other legitimate node.

Flooding REQUESTs with bogus authentication:

Legitimate node authenticates the REQUESTs it receive. Attacker floods request packets containing bogus authentication and makes the legitimate nodes busy in authenticating them. In this way, attacker makes the transmission queue of the legitimate node full. Legitimate node will not be able to forward or process the REQUEST packet quickly. So REQUEST packet forwarding or processing will be slower.

Transmitting REQUEST at higher transmission power:

Attacker may forward the REQUEST packets with higher transmission power. So it will be able to bypass the intermediate nodes. Transmission time will be less as the number of hops will be reduced and the processing time will be also reduced. So the REQUEST packet can be forwarded to destination quickly.

Performing Wormhole:

In Wormhole there is a tunnel between two attackers, by which they can communicate directly and quickly. At one end one attacker forwards the REQUEST packet and second attacker at the other end receives it. In wired network, transmission can be performed faster. So, if two attackers communicate using wired tunnel or performs wormhole, then it will be able to forward the REQUEST packet quickly compared to other legitimate nodes and legitimate node near attacker will not be able to discover the route.

III. PREVENTION OF RUSHING ATTACK

We do not forward the request which comes first. We can store some number of requests at node and select randomly from them to forward. So we can prevent from attacker, which exploits the property of AODV.

For prevention from higher transmission power or by wormhole, we can specify timeout at node. We set some timeout which is normal time for transmission from previous node to that node. If packet arrives before the timeout, we can identify it as the packet from attacker node. We can remove it and can inform other legitimate nodes.

Fig 2 shows the process of prevention from rushing attack. Here as in fig, we perform mainly to process combined. That is, discarding the packets which arrive before threshold time and randomly forwarding the request from collected requests.

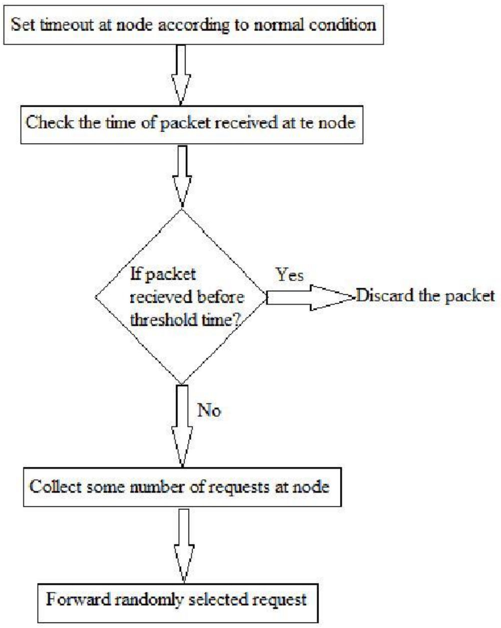
Set timeout at node according to normal condition
Check the time of packet received at te node
If packet recieved before threshold time?
Yes
Discard the packet
No
Collect some number of requests at node
Forward randomly selected request

Fig 2.Process of Prevention of Rushing attack

As in fig 3, When S forwards request pack et A,B and C will receive it. B and C will check the tim eout, if request is arrived before the time or not. If not, then stores the re quest and forwards randomly. Now at node E, the request from A will arrive first. E will check the timeout. If attacker forwards the packet quickly compared to normal time, E will discard the request from attacker A and will wait for next request. So we can prevent the network from attacker.

Then also, if request from attacker arrives after timeout, but before compare to other legitimate node, then E will store that request, rather forwarding it. E will wait for so me other requests to come. E will receive request from B . E will select the request from A and B randomly, and will forward it to D. So there is less chance of forwarding the request from A.

Here, in example there are less number of nodes. So, selection is from A and B is performed. But, in practical, there may be large number of nodes which forwards the requ ests to E. So from large number of nodes, chance of selection of forwarding A’s request is very less. In this way, by modifying the property of AODV; forwarding the first request, we can prevent the network from rushing attack.

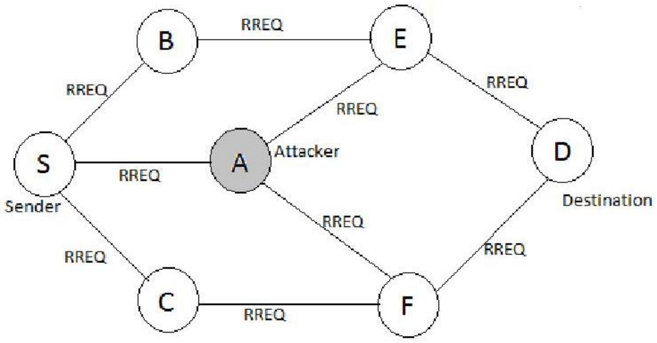

Fig 3.Ex ample Network for prevention process [3]

IV. SIMULATION RESULTS AND ANALYSIS

For Simulation we have used Network Simu lator 2.34. The properties of network for simulation are shown in Table 1. Nodes are created and the transmission is performed. Simulation is performed before prevention and after applyin g the prevention process.

Table 1 Simulation Properties

Property	**Value**
Nodes	25
Simulation Titme	100s
Protocol	AODV
Mobility	Random
Area	500m by 500m

From Figure 4, we can show that the droppin g rate of packet is higher when attack is performed. After applying prevention, we can show that the dropping rate is decreased. As we know that, in rushing attack some packets from legitimmate nodes are dropped as duplicate packet. After prevention, we can reduce the effect of attack by the mechanism as we discussed earlier.

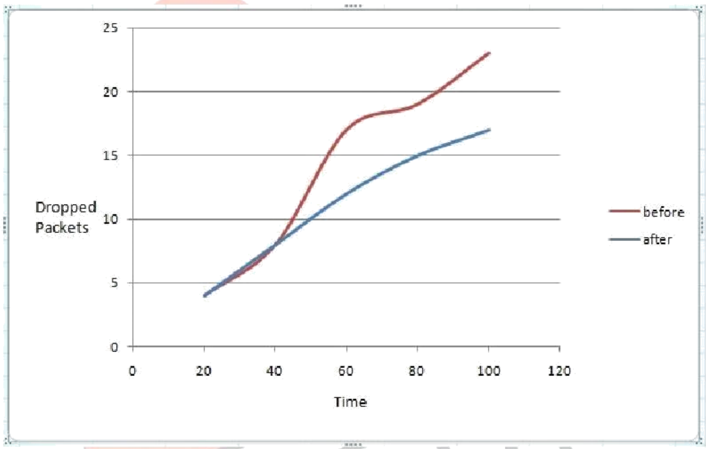

Figure 4 Result comparison

Simulation is also performed for this technique in different scenarios like different numbers of multiple attackers and different size of network or different numbers of nodes. Table 2 shows the simulation result with different numbers of attackers.

Table 2 Results of Simulation

Number of Attackers	Packet Delivery ratio
2	99.51
5	99.43
12	91.06
20	79.38

Fig 5 shows the graph, number of attacker nodes vs. packet delivery ratio. From that we can see that as number of attacker nodes increases, packet delivery ratio decreases. The effect of attack increases as the number of attacker nodes increases. As the number of attacker nodes increases, the probability of receiving a request packet from an attacker node is more. So, dropping rate or the effect of the attack is higher. The effect of preve ntion is reduces as the number of attackers increases.

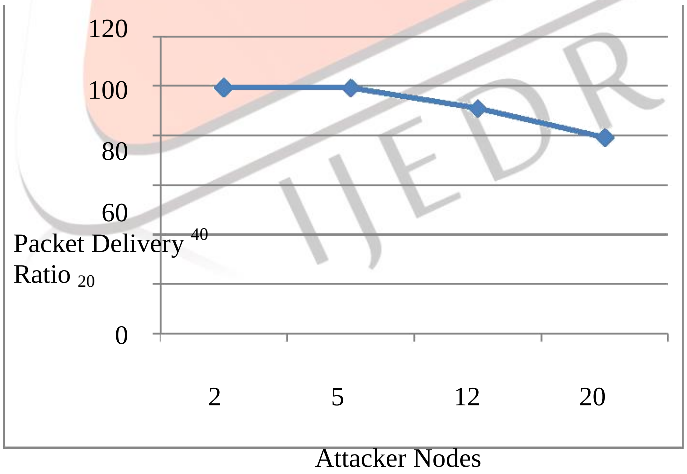

Fig 5 Attacker nodes vs. Packet delivery ratio

Simulation is also performed for this technique with different size of network. Table 3 shows the results of simulation with different numbers of nodes.

Table 3 Results with different numbers of nodes

Numbers of nodes	**Packet Delivery Ratio**
40	99.03
60	81.64
75	71.17

90	53.62

Fig 6 shows the graph, Numbers of nodes vs. Packet delivery ratio. From graph, we can see that as the numbers of nodes in the network are increased, packet dropping ratio is decreased. So, the effect of prevention decreases as the nu mber of nodes in the network increases. The effect of attack is higher for larger numbers of nodes.

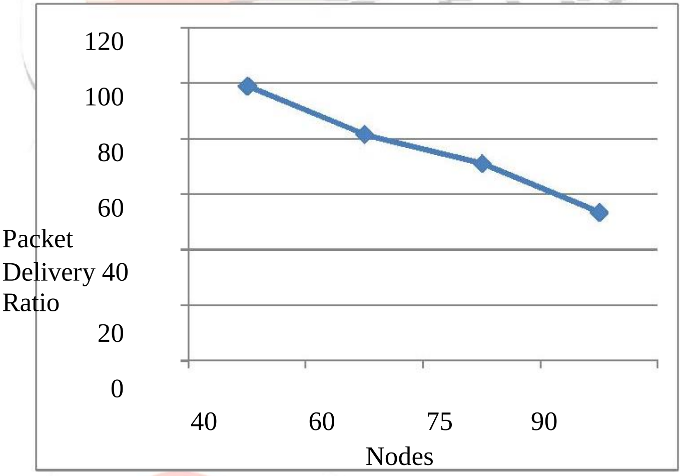

Fig 6 Number of nodes vs. Packet delivery ratio

V. ACKNOWLEDGMENT

I am thankful to my guide Prof. Bakul Panchal, Assistant Professor in Department of Computer Engineering for their valuable support. Also I am thankful to my Department for the technical support. I am thankful to my family and classmates for their support.

REFERENCES

[1] Yih-Chun Hu, Adrian Perrig and Da vid B. Johnson “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols”, Proceedings of th e 2003 ACM workshop on Wireless security, San Die go, CA, USA, pp. 3040, September 2003.

[2] Anil Rawat, P. D. Vyavahare and A . K Ramani “Evaluation of Rushing Attack on Secure d Message Transmission (SMT/SRP) protocol for Mobile Ad-H oc Networks”, Personal Wireless Communications, 20 05. ICPWC 2005. 2005 IEEE International Conference, page 62-66.

[3] Chinkit Suthar and Bakul Panchal “ A Survey on Rushing Attack and its prevention in M obile ad-hoc Network” International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Volume 4 Issue 3,March 2014.

[4] Satyam Shrivastava, “Rushing Attack and its Prevention Techniques”, International Jou rnal of Application or Innovation in Engineering and Manage ment (IJAIEM), Volume 2, Issue 4, April 2013.

[5] V. PALANISAMY, P.ANNADURAI, “ Impact of Rushing attack on Multicast in Mobile Ad Ho c Network”, International Journal of Computer Science and Informmation Security, Vol. 4, No. 1 & 2, 2009.

[6] S. Albert Rabara1 and S.Vijayalakshm i2, “Rushing Attack Mitigation In Multicast MANET (RAM3)”, International Journal of Research and Reviews in Co mputer Science (IJRRCS), Vol. 1, No. 4, December 2010 .

[7] Rusha Nandy and Debdutta Barman Roy,” Study of Various Attacks in MANET and El aborative Discussion Of Rushing Attack on DSR with clustering scheme”, Int. J. Advanced Networking and Application s Volume: 03, Issue: 01, Pages:1035-1043 (2011).

[8] Latha Tamilselvan and Dr. V. Sankaranarayanan,, “Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks”, Ad Hoc and Ubiquitous Co mputing, 2006. ISAUHC '06. International Symposium, page 42-47.

[9] Nishu Garg and R.P.Mahapatra, “MANET Security Issues”, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[10] Priyanka Goyal, Vinti Parmar and Rahul Rishi, “ MANET: Vulnerabilities, Challenges, Attacks, Application”, IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011.

[11] G.S. Mamatha and Dr. S.C. Sharma, “Network Layer Attacks and Defense Mechanisms in MANETS- A Survey”, International Journal of Computer Applications (0975 – 8887) Volume 9– No.9, November 2010.