Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Rushing Attack and Its Prevention in Mobile Ad-hoc Network

Chinkit Suthar
Computer Science and Engineering,
L.D. College of Engineering, Ahmedabad, India

Bakul Panchal
Assistant Professor of Computer Engg. Department,
L.D. College of Engineering, Ahmedabad, India

Abstract*— Mobile Ad-hoc Network contains mobile nodes which can move freely and communicate to each other without fixed infrastructure. These nodes can be routers or hosts. MANET is an autonomous system of mobile nodes and its major characteristics include dynamic topology, limited bandwidth, energy constrained operation, limited resources and limited security. Many protocols in MANET works based on On-Demand fashion. In this paper we analyzed Rushing Attack and its Prevention. In On Demand protocols the request packets received after first packet are removed as duplicate packets. In Rushing Attack, attacker exploits this property and forwards the request packet quickly and become the part of the route. So it does not let other legitimate nodes to communicate with destination. In this paper Rushing Attack and its prevention is reviewed.

***Keywords*— MANET, Rushing Attack, Rushing Attack Prevention**

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 not static. Mobile nodes move in the network during communication. Mobile nodes can be in the bus, train, building, etc. There is no centralized controlling node in the network. Mobile node works as routers to transmit the network information and meanwhile works as a end-point. As there is no centralized controlling node there is a security threat in the network. Attacker can easily join 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, sender requests for path discovery when it wants to perform transmission.

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

There are many security issues in MANET. In MANET attacker can get easily participate as a router in the transmission. So, secure routing protocols are required in MANET. Routing protocols in MANET are:

1) Proactive or Table driven protocol: In this network stores and updates the information about nodes in the router tables. As the network topology changes, tables are updated. Examples of these types of protocols are OLSR, DSDV, etc.
2) Reactive or on demand protocol: In these route discovery is performed when source requests for it to perform transmission. Examples of these types of protocols are AODV, DSR, SAODV, etc.

Hu, Perrig and Johnson presented “rushing attack” in their paper [1]. They discovered 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, different scenarios and prevention techniques for rushing attack.

II. Rushing Attack

In On demand protocols sender floods ROUTE REQUEST packets to all the neighbours. To avoid the duplication of REQUEST packet, only first REQUEST is forwarded and other are discarded. Hu, Perrig and Johnson have shown in their paper that for Rushing Attack, attacker exploits this characteristic of on demand protocol to perform attack [1].

When source initiates Route discovery it floods RREQ packets to neighbours. If attacker is able to forward the REQUEST packet to neighbour of the destination first, then the route which includes the attacker will be discovered. As the REQUESTs from other legitimate node arrive later, they are discarded as duplicates. So the legitimate nodes are unable to communicate with destination. So, rushing attack leads to Denial of Service attack [1].

In figure 1, S is sender and D is destination. A is attacker in the network. Now if S wants to communicate with D, it has to perform route discovery. S will send REQUEST packets to all its neighbours and neighbours will forward the REQUEST packet which comes first, to all its neighbours and so on. Here, B,C and A will receive the REQUEST packet. B will forward the REQUEST to E, C will forward to F and attacker A will forward the REQUEST quickly compare to B and C to E, F. Now E will receive the REQUEST from A first. So it will discard the REQUEST from B. Same way, F will forward the REQUEST from A and will discard the REQUEST from C. So REQUEST through attacker A will reach the destination D first. So the discovery path will be through attacker A. So it will not let other legitimate nodes to forward the REQUEST packets to destination. As attacker A is in the communication path, it will be able to drop the packets.

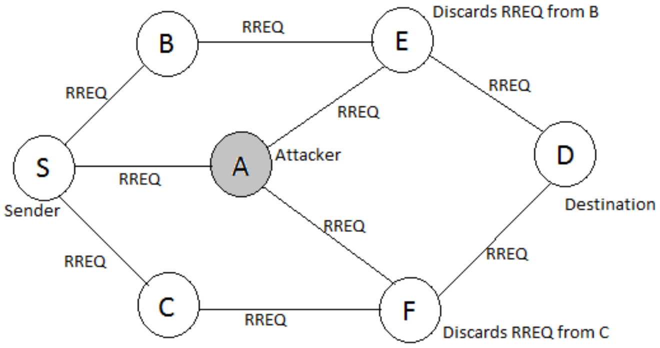

Fig.1 rushing attack formation

If an attacker forwards REQUEST packet more quickly than other legitimate node, route discovery will include the attacker in the route of communication. REQUEST packet can be quickly forwarded by following techniques [1]:

A. *Ignoring delay at either MAC or Routing layer*

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

B. *Flooding REQUESTs with bogus authentication:*

Legitimate node authenticates the REQUESTs it receive. Attacker floods REQUESTs containing bogus authentication and makes the legitimate nodes busy. So attacker makes the transmission queue of the legitimate node full. Legitimate node will not be able to forward the REQUEST packet quickly. So REQUEST packet forwarding will be slower.

C. *Transmitting REQUEST at higher transmission power:*

Attacker can forward the REQUEST packet with higher transmission power. So it will bypass the intermediate nodes. Number of hops will be reduced and the processing time will be also reduced. So the REQUEST packet can be forwarded to target quickly.

D. *Perform Wormhole:*

In Wormhole there is tunnel between two attackers. At one end the REQUEST packet will be forwarded and received at other end. In wired network there is low transit time compared to wireless network. So if two attackers communicates using wired tunnel then it will be able to forward the REQUEST packet quickly compared to other legitimate node and legitimate node near attacker will not be able to discover the route.

III. ANALYSIS BASED ON POSITION OF ATTACKER

There are three different scenarios based on the position of attacker [4]:

- Rushing attacker can be at near sender
- Rushing attacker can be at near destination
- Rushing attacker can be at anywhere in the network

A. *Attacker is at Near Sender*

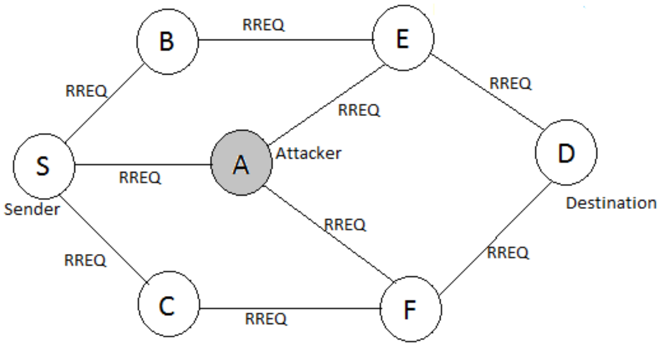

Fig.2 attacker is at near sender

As shown in fig.2 attacker node A is at near sender. There are minimum hops between sender and attacker. Here, S floods RREQ packet to all the neighbours including attacker A. Now attacker A will forward the RREQ packet to neighbours E,F quickly compared to B and C. So E and F will forward RREQ which has come from A. In this scenario attacker is near the sender. So there are many hops between attacker and destination. But it has to find only intermediate nodes and can quickly forward the requests to intermediate nodes. In this scenario the attack success rate is average [4].

B. *Attacker is at near Receiver*

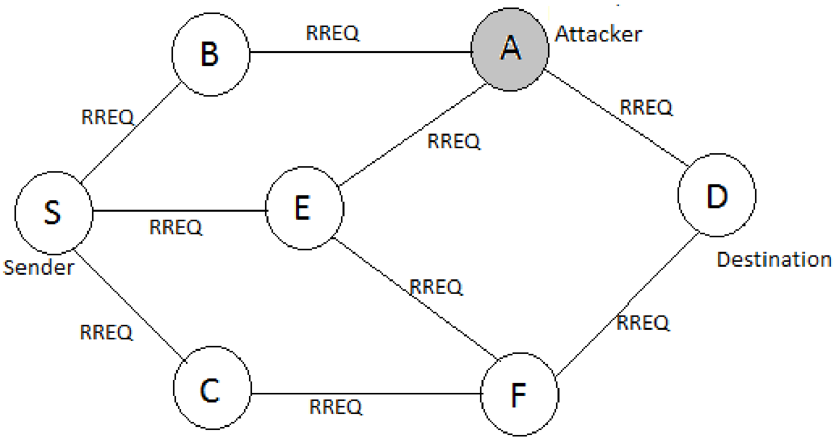

Fig.3 attacker is at near receiver

As shown in fig.3 attacker node A is at near receiver. S floods RREQ to neighbours B, E and F. Attacker A gets the request packet RREQ from B and E as it is neighbour of them. But it forwards the RREQ packet which came first. Here, attacker A forwards RREQ packet quickly compared to F. So RREQ from A will reach the destination D first. So route will be discovered through attacker A. In this scenario attacker A can directly forward RREQ to destination without intermediate nodes. Here, attacker A gets the REQUESTs from most of node. In this scenario the attack success rate is high [4].

C. *Attacker is at anywhere in Network*

As shown in fig.4, attacker node A is at anywhere in the network. S floods RREQ to B, E and C. Attacker A gets the RREQ from B and forwards the RREQ to its neighbour G. Here, attacker node A gets RREQ from some intermediate nodes and it has to also forward that requests to some other intermediate nodes. In this the chance of reaching the RREQ forwarded by attacker depends on the intermediate nodes between attacker and destination. In this scenario the attack success rate is low [4].

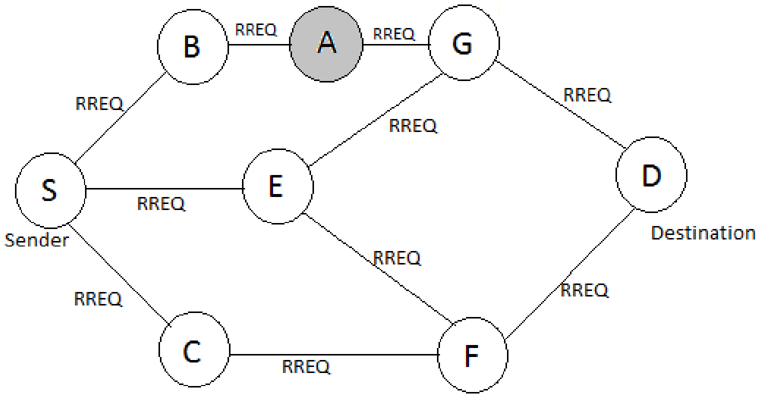

Fig.4 attacker is at anywhere in the network

IV. PREVENTION OF RUSHING ATTACK

A. *Secure Neighbour Detection*

Hu, Perrig and Johnson have shown this technique to prevent rushing attack. Rushing attacker can perform attack by forwarding RREQ with higher transmission power. Secure neighbour detection is protocol to verify that the sender and receiver of RREQ are in the normal wireless communication range [1]. In an on demand protocol, when node gets RREQ, it considers itself as a neighbour of the previous node which forwarded RREQ to it. So in this attacker can get RREQ and replay that easily. Attacker can get RREQ and replay to any node claiming that the RREQ from some other node. So the nodes which are not in the communication range find each other as neighbour. Secure neighbour detection prevents from these both situations. This technique does not let attacker to make the two nodes as neighbour which are not in the communication range. It also prevents attacker from claiming that it is neighbour of other node without direct link. Hu, Perrig and Johnson has shown three round mutual authentication protocol in their paper. It uses tight delay timing to ensure that the other party is within communication range [1].

B. Prevention From False Request Flooding by Attacker

If an attacker floods RREQ containing bogus authentication, it overloads network and keep busy the legitimate nodes in authentication. It generates delay in forwarding RREQ from legitimate nodes. This false request packets can be dropped by traffic regulation mechanism. It is based on the frequency of accepting the packet from neighbour node. Packets receiving at higher frequency from node are given least priority [2].

C. Randomized Message Forwarding

In an On demand protocol, node forwards RREQ (Request packet) which is received first. The RREQ received after first, are discarded. Rushing attacker exploits this property. So Randomized RREQ forwarding can be used. In this node does not forward the RREQ as soon as the first is received. Node collects some number of RREQ packets and chooses randomly from them to forward. So there is minimum chance of forwarding the RREQ from an attacker. In this two parameters are considered: number of RREQ collected and algorithm for timeout [1]. As perfect topology information is unavailable, numbers of requests to be collected are included by initiator in route discovery. If perfect topology information is available, then timeout to trigger RREQ forwarding will be depend on the number of hops between sender and RREQ forwarding node. Node near sender will choose shorter timeout then the nodes which are far away from sender [1].

D. Specifying Timeout

To prevent rushing attack threshold time out technique can be used [5]. In rushing attack, attacker forwards RREQ packet very quickly compared to legitimate nodes. Threshold value is fixed time interval. Threshold value is given to all the nodes and there is instruction to all the nodes that, the RREQ packet should reach after the threshold time value. If rushing attacker forwards RREQ quickly, then RREQ will reach at neighbor before the timeout threshold value. So that RREQ will not be considered and neighbor can identify the attacker [5].

V. CONCLUSIONS

In this paper rushing attack, its different scenarios and prevention techniques have studied and analyzed. Rushing attacker exploits the property of an on demand protocol; discarding the request packet comes after first. Different scenarios of attack based on position of attacker have studied. There are different ways to perform the rushing attack. Attacker can perform an attack by dropping the packets by participate in the communication or it does not let other legitimate node to communicate with destination. Various techniques have studied to prevent the attack and they can reduce the chance of attack.

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.

REFERENCES

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

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

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

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

[5] S. Albert Rabara1 and S.Vijayalakshmi2, “Rushing Attack Mitigation In Multicast MANET (RAM3)”, International Journal of Research and Reviews in Computer Science (IJRRCS), Vol. 1, No. 4, December 2010.

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

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

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

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

[10] 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.