INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SURVEY ON DETECTING RUSHING ATTACK BY USING ROUTING PROTOCOL

[1]D. Anitha, [2]B. Vishnu Priya

[1]Assistance professor, anithasuresh2003@gmail.com
[2]Research scholar, vishnupriya261@gmail.com
Sri Ramakrishna College Arts and Science for Women
Bharathiar University, Coimbatore, India

Abstract: - Mobile adhoc network is a wireless and non self organization network. And in MANET it does not have any structure in other word we say it does not have topology. Here there is no centralized system, each node act as router to route the packet. If the source node need to transact the data to destination to overhear the neighbor node of source and check if there is route and that particular node is legitimate user or not. So while make transaction here we may affect by rushing attack. Rushing attack is nothing but in this attack the attacker use the duplicate suppression device to rapidly promote the route request packet to get access with the destination than any other legitimate node. By reaching first to the destination, attacker can identify the data shared by both source and destination. So here we have number of protocol to identify the rushing attack in the network. The paper present what are the technique used to detect the rushing because it may affect the quality of service.

Keywords: Rushing attack, SDSR, DSR, Random route selection, reactive proactive

1. Introduction

A mobile ad-hoc network is an independent system of mobile nodes which communicates to each other by means of wireless links. MANET is an structure less network. Network topology is active which changes by time. There is no centralized system to control the network. In the network the node act as routers to broadcast the network data and also works as a system. So in this MANET invader can easily participate in the network and Gather the information from authorized user.

Mobile ad hoc network has two type of mechanism to work (i.e.) reactive and proactive. Reactive procedure is a table driven and Proactive is nothing but the demand protocol. But here we see about the demand protocol. In the protocol it performs path detection when it needs to perform transmission. In this, source sends request packet for path discovery and receives response from destination on successful completion. So here attacker can easily hack the legitimate user's data. While detecting the route from source to transact the packet to destination at that time hacking is called as rushing attack.

Rushing attack contain in the any MANET it will affect the quality of service and it weaken the network. The network does not have any authentication. So detecting the rushing attack here we have number of technique or algorithm. The algorithm to detect the rushing attack is Secured Dynamic Source Routing (SDSR) protocol, ADOV protocol, random route selection, etc we just have look at about rushing attack and their techniques.

2. Rushing attack

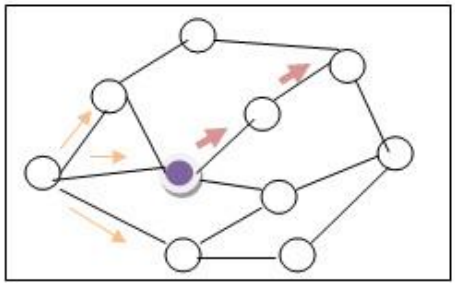

Figure 2.1. Rushing network

Rushing attack is an of use rejection of service attack, which is against the proactive protocols. Rushing attack also known as unexpected forward motion attack. A rushing attack use the duplicate suppression mechanism by which it quick forward the route discovery reply to the routing request transmit in order to gain the access to the forwarding data . In rushing attack the attacker may be close to the sender or close to the receiver and finally it may be anywhere in the MANET.

Here we have three possibility positions for attacker in MANET. They are

1. When the attacker node present near the sender
2. When the attacker node present near the destination
3. When the attacker node present anywhere in the network.

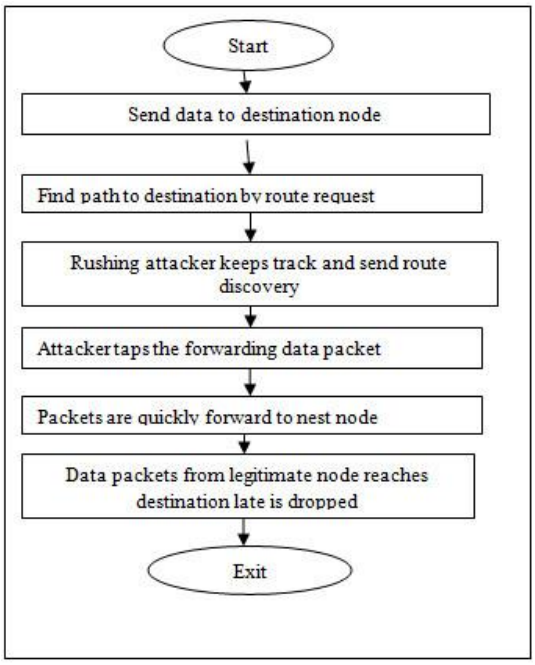

Figure 2.2 Working principle of rushing attack

2.1 When the attacker node present near the sender

The attacker node is close to the sender. The RREQ packet originated from the source node forwards the request packet to neighbor's node if any attacker present has a closest neighbor then that attacker node quickly forwards the packet to other legitimate node that node accept the request from attacker and reject other's node request.

2.2 When the attacker node present near the destination

Here there is not compulsory for attacker present nearest to the source node. It may be present nearest to the destination. The source node originate RREQ packet to their neighbor node. If all of them legitimate means they forward request packet to other node after complete their procedure, they should not rush to forward. After forwarding request to other node, it may be attacker then him send request quickly and make route to precede the transaction.

2.3 When the attacker node present anywhere in the network

This type we should not tell where the attacker in the network it may be nearest to the source or nearest to the receiver or it may in between the source and receiver. So wherever the attacker, it forward the request fast then the other node and make route to the source and destination and utilize the transaction and the information.

3. Preventing protocol of rushing attack

To prevent the rushing attack here let we discuss about some protocol and their technique to prevent the rushing attack. Protocol is ADOV, SDSR, random route selection.

3.1 ADOV

Here the modified ADOV protocol is used to prevent the rushing attack. How it preventing means rushing attack it forward the request packet too fast to other node so that node accept the first arrival node and reject other node's request. But in the modified ADOV protocol it calculates the time for required to forward from one node to other. Based on that time the node accepts the request.

From this how they preventing the rushing attack means calculate time set as time out. Example if source node send request packet to his neighbor node. In that which node forward packet before the time that node's request is rejected. Other who forwards the RREQ after the time out that node request will be accepted.

Because if we get request from one node it has some formality to forward that particular packet to other but attacker node does not have these criteria so it forward quickly. So ADOV set time as parameter to control the rushing attack.

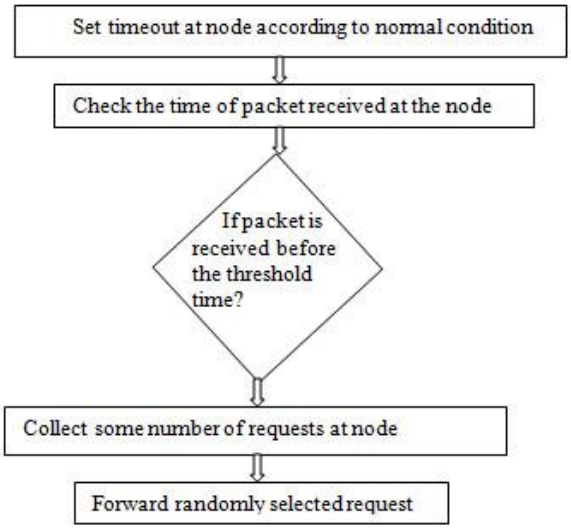

Figure 3 Preventing the rushing attack

3.2 DSR AND SDSR

In SDSR secured dynamic source routing protocol can also address the rushing attack in their algorithm. Because the SDSR is enhance protocol from DSR. In DSR routing protocol to reduce the overhead in the network it will accept the first RREQ from source node and make route but if the first node is an malicious node means then the network is full of denial of service so in SDSR routing protocol here we set certain time interval after that only the node forward RREQ packet to neighbor so here the rushing attack will reduced. Routing also is confidentiality.

Drawback in DSR:

- Lose of confidentiality
- Packet drops

Drawback in SDSR

Here we overcome the drawback what we address from DSR. In result of SDSR, the rushing attack in the network occur again when the node are isolated. So the above drawback occurs again.

4. Proposed technique

4.1 Random route selection

In random route selection is proposed model for DSR and SDSR. Here it overcome drawback in DSR and SDSR. This work based on the time. For example if source node send RREQ packet to their adjacent node i.e., C, D, E, B. Here the time is calculated for every adjacent node t1, t2, t3, and t4. It will not accept first request and proceed the path like a DSR and it will not wait for request packet for destination as a best path in SDSR. It select the path for transaction is random so it change his path continuously so the attacker should not follow us

Here the Tavg time is calculate as

Tavg= (t1+t2+t3+t4)/4

Based on that average time it will accepts the RREQ packet .which one is least time when compared to the Tavg that node's RREQ is rejected. Which one is longest time for forwarding that node's RREQ is accept.

5. Conclusion

In the MANET the rushing attack is one of thread to reduce the confidentiality; security and it make denial of service so here we have a technique to detect the rushing attack in the network. And analyze the routing protocol who address the rushing attack while routing in that we analyze on ADOV, DSR, SDSR and random route selection .here we proposed the random route selection for detect the rushing attack and it will further development in MANET.

REFERENCE

[1] Hu, Y., A. Perrig, and D. Johnson. "Efficient security mechanisms for routing protocols." 2003: Citeseer.
[2] Boukerche, A., "Performance evaluation of routing protocols for ad hoc wireless networks". Mobile Networks and Applications, 2004.
[3] 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.
[4] 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.
[5] YihChun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defence in Wireless Ad Hoc Network Routing Protocols", WiSe 2003, September 19, 2003, San Diego, California, USA. Copyright 2003 ACM 1581137699/ 03/0009.
[6] Rusha Nandy and Debdutta Barman Roy," Study of Various Attacks in MANET and El abortive Discussion of Rushing Attack on DSR with clustering scheme", Int. J. Advanced Networking and Application s 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] 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.
[9] Satyam Shrivastava , Dharmendra Mangal, "A New Technique to Prevent MANET against Rushing Attack", International Journal of Computer Science