Detection & Prevention of Rushing Attack in Wireless Ad-hoc Network: A Survey

Shravan Kumar Upadhayay[1], Vikash Mainanwal[2], Manpreet Singh Kinra[3]
Computer Science Department,
Punjab Institute of Technology, Kapurthala
Punjab Technical University Main Campus
Punjab, India

***Abstract*— in this paper, we explained compressive survey of recent Prevention techniques of rushing attack for wireless Ad-hoc Network. Routing protocols deplete these nodes to forward packet from one node to another node. There is many proposed routing protocol works in MANET as on-demand fashion. On-demand protocols have faster reaction time and lower overhead. The paper is based on Rushing attack. In Rushing attack, a awful node or an attacker increasing the speed of routing process. In this paper, we enlisted the approach, which are used to eliminate the rushing attack and also focus on how they work. As a conclusion, we invoke a number of open research challenges with regard to prospects of rushing attack prevention techniques and other issues.**

***Index Terms*— Ad-hoc Networks; Wireless Ad-hoc Network; Rushing attack, Detection of rushing attack, Prevention techniques for rushing attack, Security, issues of rushing attack**

I. INTRODUCTION

An ad hoc network is a collection of mobile computers (or nodes) that helps to forward packets for each other to extend the limited transmission range of each node's wireless network interface. A routing protocol in such type of a network finds routes between nodes, allowing a packet to be forwarded through other network nodes towards its destination. In contrast to traditional network routing protocols, for example for wired networks, ad hoc network routing protocols must adapt more quickly, since factors such as significant node movement and changing wireless conditions may result in rapid topology change.

A Mobile Ad hoc Network (MANET) is a unit of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network structures. In the mobile ad hoc network, nodes can straightly communicate with all the other nodes within their radio ranges. The nodes that not in the direct communication range avail intermediate node(s) to communicate. As we can see that in these two locale, each node that has participated in the communication forms a wireless network automatically. Such type of communication in which each node participates to make a network can be viewed as mobile ad hoc network [10]. A self-configuring network which is formed by a collection of mobile nodes automatically without the help of a fixed infrastructure or centralized management is called mobile ad hoc network (MANET). In such a network each node contains a wireless transmitter and receiver, using which node communicates with other nodes which are in its radio communication range. Consistently a node has to communicate with some other nodes which are not in its radio range.

Ad hoc networks are targeted at environments where communicating nodes are mobile, or where wired network deployment is not present or not economical. Many of these applications may run in untrusted environments and may therefore require the use of a secure routing protocol. Furthermore, even when the presence of an attacker is not for seen, a secure ad hoc network routing protocol can also provide resilience against misconfigured nodes.

In this paper, we elaborates the detection & prevention Techniques for, *rushing attack in Ad-hoc Network*, which results in denial-of-service when used against all previously published on-demand ad hoc network routing protocols. Specifically, the rushing attack prevents previously published secure on-demand routing protocols to find routes longer than two-hops (one intermediate node between the initiator and target).Because on-demand protocols generally have lower overhead and faster reaction time than other types of routing based on periodic (proactive) mechanisms, on-demand protocols are better suited for most applications.

II. RELATED WORK

AODV is the type of reactive protocol which is on demand protocol. As its name implies it works only when user demand for communication related to the transmission and receiving the data packets. The AODV routing protocol is the up gradation of the destination sequenced distance vector routing. AODV protocol provides the better communication in the network without any congestion. The evident contribution related is as follows:

Yin-Chun Hu et al [2] presented in year 2003 a new type of attack " Rushing attack", this attack results in denial of services (DoS) when used against on-demand routing protocol. All on demand protocols are unable to detect this attack. This attack can also be performed by weak attacker. Thus a generic rushing attack prevention (RAP) have been developed it exploits no cost unless the underlying protocol fails to find a working route .This method provide provable prevention even for strong attackers.

S. Albert Rabara, and S. Vijayalakshmi [3] proposed how rushing attacker works in multicasting network. Rushing attack is the action of disturbing routing mechanism by pumping a high speed malign MRREQ (Multicasting Route Request) to reach the last node, thus increasing the network traffic. The solution suggested is threshold technique (D3UT3) *in which a alarm is triggered when the number of requests is greater than the defined threshold value.*

Rusha Nandy, and Debdutta Barman Roy [4] presented how rushing attack works on DSR protocol. Self-organized clustering strategy have been scheduled. A parameter k has been defined for number of hop away from the cluster head. Thus the hop forms a cluster with its cluster head and routing is performed by transferring

data within the cluster or between the clusters. A rushing attack detection technique have been suggested in which the cluster examine the nodes of cluster .If the RREQ transmission frequency is greater than normal frequency than the node is malicious and hence removed from the cluster.

Desilva et al [7] proposed rushing attack prevention technique aka RAP. This paper have proposed an adaptive method of threshold value estimates where value is not fixed and predefined. Threshold value can also be statically computed.

V. Palanisamy and P.Annadurai [10] presented the rushing attack, in this attack the malicious node exploits twin suppression mechanism and quickly forwarding route discovery packets to gain access on the forwarding data .Thus attacker provide route discovery first and hence the possibility of false route selection increases .This paper compare the performance of attacker and its success rate in three scenario: near sender ,near receiver ,anywhere in network.

Hyojin Kim et al. [11] proposed here a innovative, robust routing scheme to contend ad hoc networks against rushing attacks. This scheme utilizes the "neighbor map mechanism". This mode focuses on route maintenance rather than using route discovery. By using this Procedure path recovery delay diminished and thus provide energy efficient solutions.

Swarnali Hazra and S.K.Setua [14] extended the AODV protocol which is based on trust model and provide secure network. This model is based on threshold value of trust ,the network consist of trust evaluating node which takes the decision to include or not to include the trustee node in routing path depending on the final trust value computed by the trust model . AODV is enhanced with different functional modules: Node Manager, Trust Module and Decision Manager. Trust based AODV secures the routing path by isolating the rushing attacker, based on their trust rate.

III. RUSHING ATTACK

Rushing attack is a zero delay attack and more effective when the attacker nearby source or destination node. On-demand routing protocols like AODV and DSR are more vulnerable to that attack, because whenever source node floods the route request packet in the network, an adversary node receives the route request packet and sends without any hop count update and delay into the network. Whenever the certain nodes receive the original source demand packets, they are dropped because consistent nodes, would have already received packet from the attacker and treat the currently received packets as duplicate packets. Thus, adversary is included in active route and disturbs the data uphold phase. Rushing attack can be taken place at source side or destination side or at the inside:

** The Consecutive conditions the rushing attacker is not included in active route

1. When source and destination nodes have direct communication link
2. When source and destination nodes have better route than rushing attacker route

** Rushing attack is more adequate when attacker near to source or destination node

A rushing attack uses duplicate suppression mechanism by which it quickly forward the route discovery reply to the routing request broad casted in order to gain access to the forwarding data; the rushing attacker gain access in forwarding group and thus can tap data. The Rushing attacker can forward route discovery or route request more quickly than the authentic node thus the chances of selection of path that includes attacker increases. The attacker can gain high speed in access of request by slowing down the response time of other nodes. The attacker can increase the jam in network by keeping the network transmission queues full of the nearby nodes. Hence nodes will respond to the request late due to bulky traffic. The authentic nodes will be buried authenticating request containing bogus authentications thus slowing down their response ability

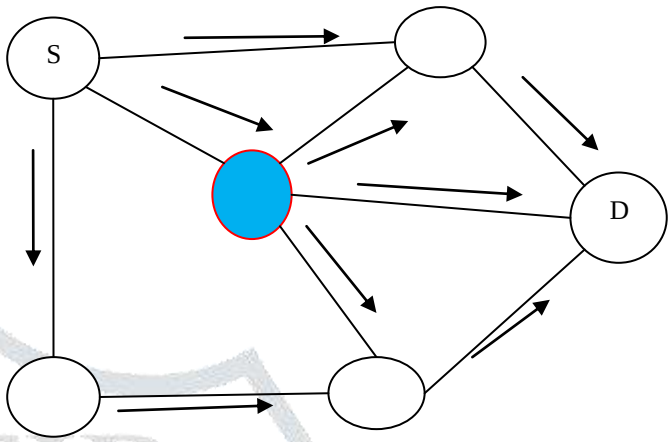

Figure 1 Rushing Attack

The rushing attack, which result in denial of services when used against all previously published on-demand ad-hoc network routing protocol [2].Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group [1, 8]. When a node send a route request packet (DD packet) to another node in the wireless network, if there an attacker present then he will accept the DD packet and send to his neighbor with high transmission speed as compared to other nodes, which are present in the wireless network. Because of this immense transmission speed, packet forwarded by the attacker will first reach to the destination node. Destination node will take this DD packet and discard other DD packets which are reached later. Receiver erect this route as a valid route and use for further communication. This way attacker will successfully gain access in the communication between sender and receiver.

A. Rushing Attack

Rushing attacks mainly divided in two types:

1. Rushing attack followed by jellyfish attack
2. Rushing attack followed by byzantine attack

Rushing attacker annoy the data forwarding phase by either jellyfish or byzantine attack.

IV. RUSHING ATTACK PREVENTION TECHNIQUE

A. Secure neighbor detection and secure route discovery procedure

Secure neighbor detection implies that two nodes detect a bidirectional link between themselves. Generally a node broadcast an advertisement to allow its neighbor to detect it. Most of the on-demand protocols perform the secure neighbor detection. In those on-demand protocols, nodes who receive a route request consider itself the neighbor of earlier-hop node. When a node relay a request is claim a path between sender and receiver, but this secure neighbor detection cannot prevent an attacker to receiving a request. If the address of previous-hop node is unauthorized, so an attacker can claim to be any node propagating a request and next hop will trust that information.

That is the reason to applying an approach of secure route discovery. In secure route discovery sender broadcast the route request very briskly. To reduce the rushing attack, a randomized path selection technique is used [3]. In traditional route request forwarding the receiving node receive the request and immediately forward the request but in modified approach, a receiving node compile all the route request and select a request at random and forward it. Two main parameters used in this technique: The no. Of request packet to be collected and the algorithm by which timeout are chosen [3].

When the number of request is elect to be large, randomized forwarding will densely rely on timeout to trigger request forwarding will reduce security. Generally perfect networks information is not available. When it is available then the timeout is based on number of between sender and receiver. Closer nodes should choose shorter timeout than far-away nodes. If topological information is not available then bode can randomly choose timeout. This approach reduce the security because every node trying to choose the shorter timeout.

B. The Concept of Threshold

To reduce the problem of rushing attack, we use the concept of threshold value [2]. We know that in rushing attack, the attacker quickly forward the DD packet or increase the transmission speed of packet. That by receiver receives this rushed packet and discards other certain DD packet. To overcome this problem we use threshold value. Threshold value is a fixed value for a transmission. There is direction for all the nodes that the packet should be reached to the neighbor node at the fix time interval. If there is rushing attacker present then it will quickly forward the packet and packet will reach before the time. The neighbor node will inform about the attacker and can identify the attacker [2]..

In figure node 1 send the packet to node 6. For this it decides the threshold value. Now assume, threshold value for this network is 5second, means a packet will take 5second in traveling to complete a hope. Node 1 sends a packet to 2,3 and 4. The packet will reach in 5second then node 2 sends a packet to 4 and 5, it will also reach in 5second and 4 sends a packet to 6 and A, Which will also reach in 5second. Node 5 send packet to 6 5second . 2 is an rushing attacker so it will quickly send the packet to 6 and this packet reach in 3.5second to node 6. Node 6 knows that the threshold value is 5second and packet comes in 4.1 second, means there is an attacker so it inform to other node about the attacker and discard this packet. So that receiver node 6 will accept the packets which come from 5 and 4.

.

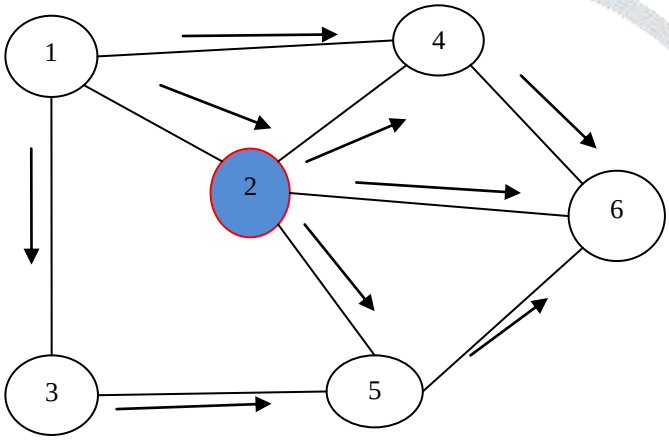

Figure 2 Rushing Attack with Threshold value[1]

C. Impact of Rushing Attack at Different position of attacker

a): *Attacker node at near sender*

In the figure, S is the sender and D is the receiver. When S sends the Packet to DD packet then node A and D get the RR packet. As we know that A is the attacker then he sends the DD packet with high transmission speed as compared to C. The DD packet travel through A and C, but the packet through A will reach first to the receiver node D, then D receive this DD packet which came from A and assume that it is a valid request which came from efficient path. So D discards other.

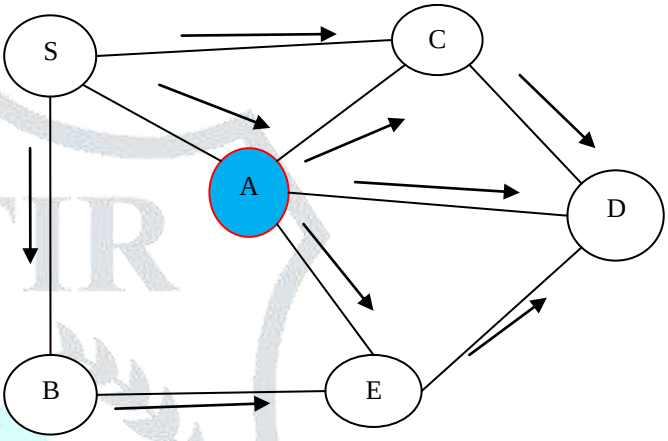

Figure 3 *Attacker node at near sender[1]*

b): *Attacker node at near receiver*

S wants to send the DD packet to D, for this S broadcast the packet. At the same time, C and A receive the DD packet. C further transmit the DD packet to A, B and D. A is attacker node, so it send the packet with fast speed in comparison of C and B. D Receive the DD packet which came from A and discard from C and B. In this case, attack success rate is high [1].

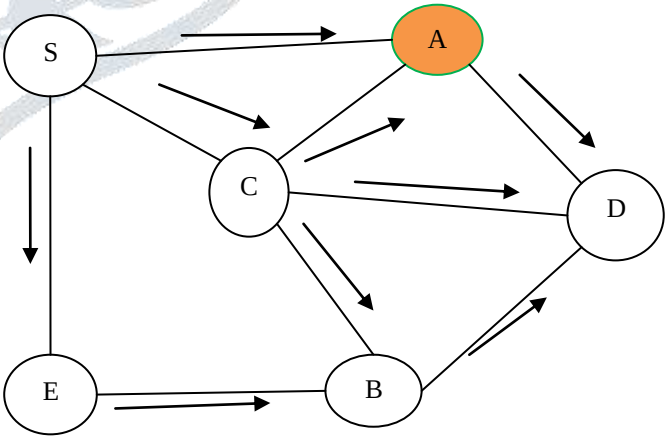

Figure 4 *Attacker node at near receiver[1]*

c): *Attacker node anywhere in the network*

S wants to send the packet to D, for this it sends the packet to its neighbor's node E, B and C. After that A send the packet to B and C send the packet to D. Similarly E sends the packet to B. B is a

attacker node, so it quickly forward the packet to D. D receive the rushed packet from B and discard the packet from C. In this case the attack arrival rate is least, but it is marginally higher than the near sender in which the attack success rate is low [1]

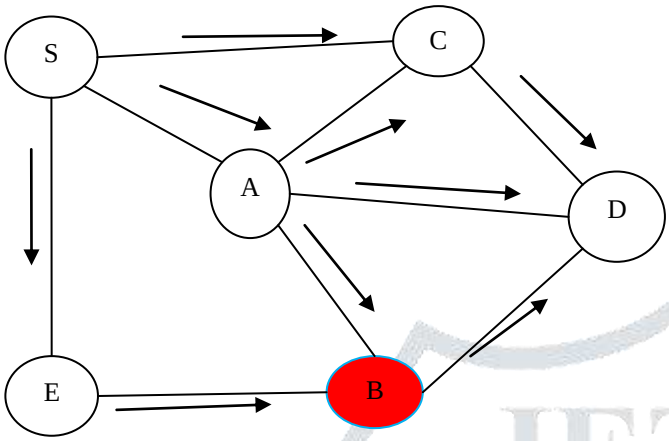

Figure 5 *Attacker node* anywhere in the network[1]

V. CONCLUSION

In this paper, we have presented a survey on Rushing Attack & its Prevention Techniques in Wireless Ad-Hoc Network. In this paper a study of rushing attack and its effect in MANE .This paper analyze the different technique to prevent the rushing attack or to reduce the harmful effect of rushing attack. But the previous listed techniques are not sufficient to prevent this attack. It also describes how rushing attack formation can be done. In this context the effect of rushing attacks over AODV; which is defined as reactive distance vector protocol is presented in this work .Its believed that this paper will inspire researchers to develop effective Rushing Attack Prevention Techniques and algorithm for MANET.

.

REFERENCES

[1] *Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, "A New Routing Attack in Mobile Ad Hoc Networks", International Journal of Information Technology Vol. 11 No. 2, pages 83 – 94.*

[2] *Yin-Chun Hu, Adrian Perrig and David B. Johnson, "Rushing attack and Defense in Wireless Ad Hoc Network Routing Protocols", Wise 2003, San Diego, California, USA.*

[3] *S. Albert Rabara, and S. Vijayalakshmi, "Rushing attack Mitigation in Multicast MANET (RAM3), IJRRCS,Vol.1, No.4, December 2010, pp. 131-138.* K. Elissa, "Title of paper if known," unpublished.

[4] *Rusha Nandy, and Debdutta Barman Roy, "Study of Various Attacks in MANET and Elaborative Discussion of Rushing Attack on DSR with clustering scheme", International Journal of Advanced Networking and Application, Vol. 3, Issue 01, 2011, pp. 1035-1043..*

[5] *D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing",Kluwer Academic Publishers, Vol 353, 1996, pp. 153-181.*

[6] *Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.*

[7] *Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, volume 5, Number 3, 2007, pp 338-346.*

[8] *Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59*

[9] *Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia*

[10] Gajendra Singh Chandel and Rajul Chowksi, "Study of Rushing attack in MANET," International journal of ucterion (IJCA), Vol. 79, No. 10, Oct. 2013.

[11] R. Chandra, V. Ramasubramanian, and K. Birman, "Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks,"Proc. 21st Int'l Conf. Distributed Computing Systems (ICDCS '01), 2001.