Rushing Attack and its Prevention Techniques

Satyam Shrivastava

Department of Computer Science, MITM, RGPV, Indore

ABSTRACT

Mobile Ad-hoc Network is a collection of different type of nodes, which are connected to each other via wireless link. These nodes also communicate through wireless link. These nodes operated in two ways, as a router, to forward packet to other nodes in multi hop fashion, or as a host. Mobile Ad-hoc network is a wireless network, without fixed infrastructure or access point. Routing protocols use these nodes to forward packet from one node to another node. Many proposed routing protocol works in MANET as on-demand fashion. These on-demand protocols have faster reaction time and lower overhead. This paper is based on Rushing attack. In Rushing attack, a malicious node or an attacker rising the speed of routing process. In this paper, my aim is to list the techniques, which are used to overcome the rushing attack and also focus on how they work.

Keywords: Multicast, Security, MANET, Rushing attack, Prevention technique.

1. INTRODUCTION

Mobile ad-hoc network is a self organized system of mobile nodes and these mobile nodes are communicated with each other via wireless link. MANET has no fixed infrastructure or centralized authority such as base station or access point. Military battlefield, emergency rescue, vehicular communication and mining operation are example of MANET, because they have not infrastructure.

If we use multicasting in MANET, then security issues rises because sending a packet from one node to many node is more challenging than transmission of packet from one node to another node. This way attacker gets more change to hack the data.

Multicasting has advantage over the multiple unicast transmission; this way network bandwidth and resource may be saved. Multicast routing can be classified into two categories: tree-based and mesh-based. In tree-based multicast routing, there is a single route from source to destination. If this route break then the communication between nodes will not be possible. While in mesh-based multiple routing, every node connect to every other node in the network, so is a route break between two nodes then many alternative will be allow to forward packet from source to destination. In mesh-based multicast routing, network will frequently change the topology and found the path between the nodes. Example of tree based multicast routing protocol are MAODV, AMRIS, BEMRP and ADMR. Mesh based routing protocol are ODMRP, FGMP, CAMP, DCMP and NSMP [1, 2, 4, 8].

Security is main issue in ad-hoc network as compared to wired network. MANET is vulnerable to attack because the lack of centralized authority, lack of trust relationship between nodes and easy eavesdropping [2]. When we talk about group communication, then security of MANET is even more challenging and this happen because of presence of multiple senders and multiple receivers [1, 9]. Rushing attack, Blackhole attack, wormhole attacks are some routing attack.

Roadmap of this paper is as follows. Section 1 introduces the paper. Section 2 present descriptions about the rushing attack. Section 3 elaborates the prevention technique against the rushing attack. Section 4 concludes the paper.

2. 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 (RR packet) to another node in the wireless network, if there an attacker present then he will accept the RR packet and send to his neighbour with high transmission speed as compared to other nodes, which are present in the wireless network. Because of this high transmission speed, packet forwarded by the attacker will first reach to the destination node. Destination node will accept this RR packet and discard other RR packets.
packets which are reached later. Receiver found 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.

3. Prevention Technique Against Rushing Attack

3.1 Secure neighbour detection and secure route discovery procedure

Secure neighbour detection implies that two nodes detect a bidirectional link between themselves. Generally a node broadcast an advertisement to allow its neighbour to detect it. Most of the on-demand protocols perform the secure neighbour detection. In those on-demand protocols, nodes who receive a route request consider itself the neighbour of previous-hop node. When a node transmit a request is claim a path between sender and receiver, but this secure neighbour detection cannot prevent an attacker to receiving a request. If the address of previous-hop node is unauthorised, 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 a concept of secure route discovery. In secure route discovery sender broadcast the route request very rapidly. 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 technique, a receiving node collect all the route request and select a request at random and forward it. Two main parameter is used in this technique: The no. Of request packet to be collected and the algorithm by which timeout are chosen [3].

When the no. Of request is chosen to be large, randomized forwarding will heavily rely on timeout to trigger request forwarding will reduce security. Generally perfect topology 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 [3].

3.2 Impact of rushing attack at different position of attacker

For this technique, there are three scenarios

3.2.1 Attacker node at near sender

![Figure 1 Rushing Attack](image1)

![Figure 2 Attacker node at near sender](image2)
In the figure, S is the sender and R is the receiver. When S sends the RR packet then node A and D get the RR packet. As we know that A is the attacker then he sends the RR packet with high transmission speed as compared to D. The RR packet travel through A and D, but the packet through A will reach first to the receiver node R, then R receive this RR packet which came from A and assume that it is a valid request which came from efficient path. So R discards other RR packet.

In this case, the attack success rate is average [1]. This result comes after the several simulations under Linux using network simulator NS2 version ns-allinone-2.26 [1].

### 3.2.2 Attacker node at near receiver

![Figure 3 Attacker node at near receiver](image)

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

### 3.2.3 Attacker node anywhere in the network

![Figure 4 Attacker node anywhere in the network](image)

S wants to send the packet to R, for this it sends the packet to its neighbour’s node D, B and C. After that B send the packet to A and C send the packet to A and E. Similarly D sends the packet to E. A is a attacker node, so it quickly forward the packet to f and then R. R receive the rushed packet from f and discard the packet from G. In this case the attack success rate is least, but it is slightly higher than the near sender in which the attack success rate is low [1].

### 3.3 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 RR packet or increase the transmission speed of packet. That by receiver receives this rushed packet and discards other legitimate RR packet. To overcome this problem we use threshold value. Threshold value is a fixed value for a transmission. There is an instruction for all the nodes that the packet should be reached to the neighbour 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 neighbour node will inform about the attacker and can identify the attacker [2].
In figure node 1 send the packet to node 9. For this it decides the threshold value. Now assume, threshold value for this network is 5 second, means a packet will take 5 second in travelling to complete a hope. Node 1 sends a packet to 2 and 3. The packet will reach in 5 second then node 2 sends a packet to 4 and 5, it will also reach in 5 second and 3 sends a packet to 4 and A, Which will also reach in 5 second. Node 5 send packet to 6 and 4 send packet to 7 in 5 second. A is an rushing attacker so it will quickly send the packet to 8 and this packet reach in 3.5 second to node 8. Node 8 knows that the threshold value is 5 second and packet comes in 3.5 second, means there is an attacker so it inform to other node about the attacker and discard this packet. So that receiver node 9 will accept the packets which come from 6 and 7.

4. CONCLUSION

Rushing attack is an advance attack. Not many researches have done on rushing attack. This paper analyse 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.

REFERENCE