A Survey on Various Prevention Techniques for Rushing Attack in MANET

Ankit C. Patel1 Shaishav N. Shah2
1,2SVM Institute of Technology Bharuch 392-001, Gujarat, India

Abstract—A Mobile ad hoc network (MANETs) is a group of mobile nodes that communicate with node to node via wireless links with no fixed infrastructure and no centralized administration. In MANETs many routing protocol works as on-demand routing protocol and these on-demand protocols have faster response time and lower overhead. In MANET there are many attacks that affect the routing and one of them is rushing attack. In this paper, we have study various prevention techniques, which are used to prevent the rushing attack. In Rushing attack, a malicious node or an attacker further the speed of routing process. Rushing attacks represent one of such possibilities. In these Rushing attacks, malicious nodes send the Route Request (RREQ) packets, asking for a route, to the destination node quicker than the legitimate nodes do.

Key words: MANET, Rushing Attack, Security, Prevention Technique

I. INTRODUCTION

A Mobile ad-hoc network is a self-configuration wireless network of mobile nodes and its every node are connected by wireless link. In MANET network topology is not static. The MANET’s main aim is anytime, anywhere and in any condition node to node communication. In the MANET two types of routing protocol (1) unicast routing protocol (one to one communication) and (2) multicast routing protocol (one too many communication). For Example of unicast routing protocols and multicast routing protocol show in figure 1 [3].

Fig. 1: Routing Protocol

Security is main problem in Mobile ad-hoc network as compared to wired network. MANET is open to attack because they have not centralized authority, have not trust relationship between nodes and simple eavesdropping. When we have a discussion about the security of MANET is even more difficult and this happen because of presence of many senders and many receivers. MANETs are weak security attacks due to Randomly Change network Topology, Limited Energy, No centralized control, Scalability of mobile devices. There are many protocols to use to solve the issue of routing in MANETs. In MANET general two types of routing protocol (1) Periodic protocol (2) On-demand protocol. Although these protocols help the MANETs work easily, but them vulnerable against many attacks [9].

In MANET the security of routing protocols one of the most important research areas over Ad-Hoc networks. Furthermore, rushing attack becomes one of the attacks against routing protocols in MANET.

We presented various types of attack in MANET in section 2. Then in section 3 Rushing attack and section 4, related work in rushing attack. In the next section, we concluded Rushing attack prevention techniques.

II. VARIOUS TYPES OF ATTACKS IN MANET

In MANET are two different attacks: passive attacks and active attacks.

A. Passive Attacks

In this type of attack attacker do not modify and exchange attacks but only listens. An attacker node does not break the proper communication operation. During this attack force confidentiality is occurred when another attacks uses the information gather by the passive attracters. These types of attacks are not easy to detect because attackers do not involved as a part of communication process. To prevent these types of attacks effective encryption techniques can be applied so that attacker is unable to break the security [11].

B. Active Attacks

In this type of attack attacker can modify the information on the network. Active attacks are Disturb performance of the network. Active attacks there are two different categories external attacks and internal attacks. In internal attacks are performed by the node in the network or performance that they are part of the network. Internal attacks are not easy to detect because nodes are the licensed in the network. In external attacks are not the part of the network and these types of attacks are prevented by using powerful encryption methods [11].

III. RUSHING ATTACK

In this when attacker node accept any request packet for route detection then it sends the packet in the whole network before any other nodes forward the request packet. Due to this if same request packets send by legitimate node to received nodes then they consider packet as duplication and take it. This way attacker will always be part of the route and it is extremely difficult to identify such harmful node [4].

In MANET while a node send a route request packet (RREQ packet) to another node, but there an attacker present in the network it will accept the RREQ packet and send to its neighbors with higher speed as compare to other nodes. At that time this high speed, packet forward by the attacker will first reach to the target node. Target node will accept this RREQ packet and remove other RREQ packets which are reaching later. Receiver starts this route as a validated route and these route use further communication.
Rushing attacks divided in two types:
- Rushing attack transfer by jellyfish attack
- Rushing attack transfer by byzantine attack

A. Rushing Attack Transfer by Jellyfish Attack

A jellyfish attacker first need to interrupt into the multicast forward group. It then delays data packets without need for a few amount of time before forwarding them. These results in much high end-to-end delay and thus degrade the performance of valid applications [8].

B. Rushing Attack Transfer by Byzantine Attack

The main goal of Byzantine attack is interruption or conclusion of the routing service. An adversarial node or group of adversarial nodes can modify, capture which can form routing self-loop, drop packets selected, synthetically delay packets, route packets along no optimal paths, or make a path look either long or short than real version [12].

In rushing attack attacker can be any position in the network like as follows:

1) Near the Source

The attacker node A is near to the source node send the request through RREQ packet forwarded to A and B, the attacker node A quickly forwards first C then B and the packet form C node reaches R quickly to other legitimate node[5].

2) Near the Destination

The attacker node is near to destination end. At this time the RREQ Packet initiate from S the source is forward to B & D, B Forwards packet it to C, D forwards the packet to A & C, but A is an attacker Node then forwards it to reach destination R than finally the node. Finally R rejects the newly arriving packet from other legitimate node [5].

Satyam Shrivastava [1] presented a rushing attack prevention technique. This paper has proposed a one of the method of threshold value calculation method. In this method value is not fixed. Threshold value can also be statically calculate. We know that in rushing attack, the attacker speedily forward these RR packet or increase the communication speed of packet. That by receiver receives this rushed packet and rejects other legitimate RR packet. To solve this problem author have used threshold value. Threshold value is a fixed value for a communication. There is an instruction for all the nodes that the packet should be achieve to the neighbor node at the fix time period. If there is rushing attack present then it will speedily forward the packet and packet will achieve before the time. The neighbor node will inform about the attacker and can classify the attacker.

Yin-Chun Hu et al [2] presented one type of attack i.e. “Rushing attack”. In rushing attack effect is denial of services (DoS) when compared with on-demand routing protocol. All on demand protocols are vulnerable to this attack. This kind of attack can also be performed by naive attacker. Thus a feasible generic rushing attack prevention (RAP) have been developed such that it exploits no or least cost unless the underlying working protocol fails to find a working route, prevention is much higher in this method by attackers.

Shaveta Jain and Kushagra Agrawal [3] presented how the rushing attack have an effect on MZRP routing protocol in Mobile Ad-hoc network and this paper show the impact of rushing attack at the different situation like attacker near source, near destination node and anywhere in the network. And also the threshold value use to prevent the rushing attack.

ALshahrani and Abdullah Saad [6] purposed on rushing attack which threaten the security of the mobile ad hoc network and its impact on mobile ad hoc networks. Over past year research on rushing attack is examined as well as the various protocols make improve the possible solution for rushing attack. This paper study the Secure Dynamic Source Routing protocol has been considering to address rushing attack, to reduce overhead and time required in network. Moreover it highlights the strength, weakness and some limitations of the Secure Dynamic Source Routing protocol, and find that the best solution to address the rushing attack problem.

V. Palanisamy and P.Annadurai [7] presented the Rushing attack. Rushing attack exploits this duplicate suppression mechanism by quickly forward route discovery packet in order to gain access to the forwarding group. Thus attacker provide route discovery first and thus the possibility of false route selection increases. In this paper, the goal is to calculate the impact of Rushing attack and their node position which affect the performance metrics of Average
Attack Success Rate (ASR) with respect to three scenarios: near source, near destination and anywhere within the network. The performance of the Attack Success Rate (ASR) with respect to above three scenarios is also compared.

Ghoreishi at al [8] proposed the rushing attack and its anticipation method. This paper has proposed the following method to prevent the rushing attack like Secure Neighbor Detection method, if two nodes are capable to communicate because of being in the same highest communication range, they can detect each other as neighbors. Therefore, the use of this technique the attacker is not capable to introduce two nodes, which are not within the highest communication range as neighbors. Moreover, it is not capable to show itself as a neighbor of another node without being able to hear the packets. And In the Secure Route Delegation (SRD) method, every node must be capable to verify that all the Secure Neighbor Detection (SNd) steps were done between every neighboring pair of nodes. To reach this goal, Secure Route Delegation (SRD) uses Secure Border Gateway Protocol (S-BGP).

Jain at al [9] proposed the rushing attack Prevention Algorithm for MANET by Random Route Selection to create DSR and AODV more capable. This algorithm has removed some disadvantage of DSR and SDRS algorithm and it can be more capable. In this paper overcome the weakness of the DSR and SDSR algorithm and these algorithm based on the random route selection and time based also. And finally two conditions: firstly, to reduce overhead by use the DSR algorithm and received the message by target node itself to determine the safe and fast route.

Bharti at al [10] presented the Detection of rushing attack by compare energy, throughput and delay with AODV protocol. And this paper author has implemented the AODV protocol and rushing attack. Then these protocol to compare end-to-end delay, packet delivery ratio (PDR) and throughput. In this paper rushing attack, attacker node sends the packet it very quickly to which acknowledgement received to sender become before then other nodes. So, rushing attack end-to-end delay is decrease and also throughput and packet delivery ratio (PDR) is decreases. This means more packets are lost. In future work can be done on exposure on different other attacks. Also the avoidance of attacks can be done.

V. CONCLUSION

In MANETs, number of sender and receiver is reliable time by time. A sender may have various links to the other node. In MANET station that they respond to only the first receive route request. This is the reason of weak point of a network to the rushing attack. In this when attacker node accept any request packet for route detection then it sends the packet in the whole network before any other nodes forward the request packet. Due to this if same request packets send by legitimate node to received nodes then they consider packet as duplication and take it.

In this paper, we have represented a survey on Rushing Attack and its Prevention Techniques in Mobile Ad-Hoc Network. In this paper a study of rushing attack and its effect in MANET. This paper analyzes the different methods to prevent the rushing attack or to decrease the offensive effect of rushing attack. But the previously listed methods are not enough to prevent this attack.

REFERENCES