Review of Rushing Attack in MANETs
Swapandeep Kaur Chahal1 Dinesh Kumar2
1,2GZS Campus College of Engineering & Tech. Bathinda, Punjab, India

Abstract—Mobile Ad Hoc Network is a collection of multihop wireless mobile node that communicates with each other without centralized control. Each node in MANETs act as both router as well as host. Security is the most challenging task in MANETs. MANET is vulnerable to various kinds of network attacks such as black hole attack, grey hole attack, worm hole attack, rushing attack, Sybil, flooding attack, link spoofing, packet dropping attack, location disclosure etc. On-demand routing protocols in ad hoc networks were not originally designed to deal with security threats so as to malicious users have been searching ways to attack networks. Rushing attacks represent one of such possibilities. In these attacks, malicious nodes forward the Route Request (RREQ) packets, asking for a route, to the destination node faster than the legitimate nodes do. This is possible because the legitimate nodes only forward the first received RREQ packet for a given route discovery. Moreover, the attackers can tamper with either the medium access control or routing protocols to get quicker processing. As a result, the path through the malicious nodes is chosen, which renders throughput degradation.

Key words: Mobile Node, Rushing Attack, Intrusion Detection Technique, Malicious Node

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is a compilation of mobile devices without having any intended infrastructure to connect mobile devices to wired networks. Since there is no infrastructure, all important network operations like routing, forwarding must be handled by the mobile nodes that are each node act both as a router and as an end host at the same time. MANETs are very flexible and can be recognized quickly and easily using low cost equipments. Due to limited radio range of wireless nodes, the path among a pair of nodes may consists of many mobile nodes. MANETs have a wide range of applications such as collaborative, distributed mobile computing (e.g., sensors, conferences), disaster relief (e.g., flood, earthquake), war front activities and communication between automobiles on highways. Most of these applications demand multicast or group communication [3]. Mobile ad hoc networks are created from movable nodes that are dynamic type of network and communicate information across the network. The various security issues in MANETs are lack of secure boundaries, risks from compromised nodes inside the network, lack of centralized management facility, restricted Power Supply, scalability and efficient routing. There are various types of attacks such as black hole attack, wormhole attack, eavesdropping, location disclosure, flooding attack and rushing attack. In rushing attack, which result in denial of services when used against all earlier available on-demand ad-hoc network routing protocol [2]. Rushing attack exploits this duplicate suppression mechanism by rapidly forwarding route discovery packet in order to gain access to the forwarding group [1][8]. When a node send a route request packet to another node in the wireless network, if there an attacker present then he will accept the 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 packet and discard other packets which are reached later on. Receiver originates this route as a suitable route and use for further communication. This way attacker will effectively achieve access in the communication between sender and receiver.

Fig. 1: Rushing attack [4]

Fig. 2: Network displaying rushing attack [15]

II. RELATED WORK

In [1], authors have stated the position of Rushing attacks against routing protocols and the functionality of this type of attacks. As of the nature of wireless channels, MANETs are exposed against many threats and attacks. Next to this, the movement of the network nodes completes the security of routing protocols as one of the research areas over Ad-Hoc networks. Furthermore, Rushing attack became one of the general attacks against routing protocols in MANETs.

In [2], authors have proposed an IDS for packet dropping nodes in the network based on anomaly detection. Anomaly means abrupt increase or decrease in the patterns. In such kind of IDS, the behaviour of the nodes is measured in the network continuously. First the nodes are monitored when there is no black hole attack or grey hole nodes present. In this scenario, all the nodes will normally forward the packets that are intended to be delivered at the destination node. Now, if some malicious nodes enter the network and starts dropping the packets, their behaviour is analyzed against the past patterns when the communication was going normally.
In [6], authors describe the features, application, as well as vulnerabilities of mobile ad hoc network also presents an overview and the study of attacks and their mitigation in routing protocols. Each device in a MANET is free to move without any interference in any direction, linking to other devices frequently. Each should forward traffic dissimilar to its own use, and therefore be a router. Its routing protocol has to be able to handle with the new challenges that a MANET creates such as nodes mobility, security maintenance, and quality of service, limited bandwidth and limited power supply etc.

In [8], the authors have paid attention to rushing attack which threatens the security of the MANETs by studying this kind of attack and its impact on MANETs. Rushing attacks in mobile ad hoc networks cause system resources to become limited and isolates genuine users from the network. Consequently, this type of attack drastically influences network connectivity, weakens networking functions and capabilities such as control and message delivery. Research on rushing attack has been examined and the number of protocols recognized to get better solution for this attack. The authors have also examined the Secured DSR protocol which has been designed to address this attack. In addition, the authors have highlighted the strengths and weaknesses of the secured dynamic source routing protocol and establish that this is the best solution to tackle the rushing attack problem.

In [10], the authors have provided an alternative of rushing attack, which targets on the scheduling mechanism of ExOR. ExOR that makes the finest use of every broadcast and chooses the next hop after the transmission for that hop, is an opportunistic routing protocol in Wireless Mesh Network. As effectively increasing the throughput of the network, ExOR doesn’t take any safety measures into account. As ExOR attempts to schedule the transmission by the help of each node, the scheduling mechanism of ExOR is simply damaged by attackers. The attacker breaks the scheduling mechanism and forwards the portion in spite of higher priority nodes’ sending, that leads to the incorrect setting of other nodes’ forwarding timer. And then authors have projected the anti-rushing mechanism, a defense against the alternative of rushing attack for ExOR.

In [13], authors have stressed on the security of DSR protocol in order to avoid the rushing attack. Rushing attack is a malicious attack that is directed against on demand routing protocols that uses duplicate suppression at each node. The attacker exploits this property in order to prevent communication between the key nodes in the network. To attain this, it will try to be a component of the route that the source node uses to transmit data to the goal node. By capturing the path effectively, the attacker will disrupt the swapping of packets between the nodes, thus resulting in denial-of-service.

In [14], this paper has analyzed the result of rushing attack on SMT/SPR and also evaluated the significance of a variety of variants of rushing attack as applicable to SMT/SPR. Communication in mobile ad-hoc networks comprises two phases which are route discovery and data transmission. In a hostile environment, adversarial nodes can try to interrupt communication in both phases; therefore, to guarantee complete security, both communication phases should be protected. Physical security in MANET setups is very restricted and the possibility of spoofing, replay transmission, header modification, etc. always exists. Link level security, using encryption, does decrease threats, but the most vital issue remains with inter-router confirmation earlier to the exchange of network control information. MANET routing protocols have been improved to deal with the security needs. An attack that is rushing attack prevents discovery of routes ahead of two hops by all previously published protocols. Rushing attack prevention is a generic safe route discovery part, which can be applied on any on-demand route discovery mechanism against rushing attack. Any MANET node can maliciously disrupt and deny the communication of other nodes. Secured message transmission protocol safeguards data transmission against any random malicious behavior of network nodes. SMT uses secured routing protocol (SRP) in the route discovery phase.

III. CONCLUSION

In this paper presents MANETs and its security attacks taxonomy in conjunction with various attacks. It gives a study of rushing attack and its effect in MANETs. It also describes how formation of rushing attack can be made. In this context the effect of rushing attacks over AODV, which is defined as reactive distance vector protocol is presented in this work. Rushing attack is an advance attack. This paper analyzes the different technique to prevent the rushing attack or to reduce the harmful effect of rushing attack. But the earlier techniques are not adequate to prevent this attack.

REFERENCES


Review of Rushing Attack in MANETs
(IJSRD/Vol. 4/Issue 03/2016/508)

Networks.” Published online: 12 July 2012© Springer Science+Business Media, LLC. 2012.


[10] He Xianzong.; Tan Xiaobin ; Zhou Yu ; Qin Guihong, "Defense of a variant of rushing attack on ExOR." 29th Chinese Control Conference (CCC), IEEE 2010


