International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 9: September 2015, pp 1-5. www.aetsjournal.com ISSN (Online) : 2394-6237

Solution To Prohibit Rushing Attack In Mobile Ad-Hoc Network

Wilson Prakash. S , Sankaranarayanan S

Abstract— Mobile Adhoc networks (MANET) incorporates mobile nodes that forward information or packets from node to node through a wireless medium. The topology changes rapidly, there is no central Authority for routing of packets hence the communication is on mutual trust between nodes. Thus attention has been paid on developing a secure reactive protocol against various attacks. In this proposed work, prevention of rushing attack is presented over AODV. Thus we develop a Modified Secure Ad-Hoc On-Demand Distance Vector (MS-AODV) to address the rushing attack and reduce the overhead in network. It is a rushing attack prevention mechanism for the reactive protocols. Then we compared result with AODV.

Index Terms— rushing attack, MS-AODV, AODV, MANET, Mutual trust.

I. INTRODUCTION

A MANET is a self-organizing system of mobile nodes that communicates with each other via wireless links with no fixed infrastructure. The nodes in the MANET can dynamically join or leave the network frequently, without warning and without interruption to communication with other nodes. In MANET each node acts as a host as well as router for other nodes in network for transmission of data packets. Each of these nodes is provided with the wireless transmitter and the receiver for transfer the data between the nodes. This suitable applications for military battlefield, emergency rescue operation, vehicular communications, sensor networks, commercial use etc.

Security in Mobile Ad-Hoc Network (MANET) is the most important for the basic function of network. It often suffer from security attacks because of its manner like open medium, unstable topology, lack of central audit and management and no clear security mechanism. These factors have moved the MANET into battle field situation against the security threats. With the comparison of wired network Mobile Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANET). Traditional routing table was basically made for the hosts which are connected wired to a non-dynamic backbone. Due to which it is not possible to support Ad-Hoc networks mainly due to the movement and dynamic topology of networks. Due to various factors including shortage of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are unsafe for various attacks.

They are two types of attack:

A. Passive Attack:

In passive attack, the attacker does not interrupt the operation of the mobile node in the network. But, grabs the data from the network without altering it. Detection of the passive attack is very difficult since the files or system information.

B. Active Attack:

In Active attacks, the malicious nodes launch intrusive activities such as modifying, injecting, forging, fabricating or dropping data of packets. It can bring down the entire network or degrade performance significantly.

C. Wormhole Attack:

An attacker grab packets at one location in the network and tunnels them to another location. Routing can be mess up when routing control messages are tunneled. This tunnel between two attackers is referred as a wormhole.

D. Rushing Attack:

The rushing attack, which result in denial of services when used against all previously published on-demand ad-hoc network routing protocol. Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group. When a node send a route request packet (RREQ packet) to another node in the wireless network, if there an attacker present then he will accept the RREQ packet and send to his neighbor with high transmission speed as compared to other nodes. Because of the high transmission speed, the packet forwarded by the attacker will reach first to the destination node. Destination node will accept this RREQ packet and discard other RREQ.

II. RELATED WORKS

Udhayakumar et al. (2014) in their approach on "Security Attacks and Detection Techniques for MANET" it is visible that different security mechanisms are introduced in order to prevent such network. Hence this paper described the different network layer attacks and detection mechanism of attacks in MANET. However, history shows that attackers regularly find new ways to attack and cause damage to computer systems and networks. So, it is treated that enabling

Wilson Prakash S (PG Student), Network Engineering, Kalasalingam University, Krishnankovil, India. (Email: wprakash.s@gmail.com)

Sankaranarayanan S (Assistant Professor), Department of Computer Science & Engineering, Kalasalingam University, Krishnankovil, India. (Email: sankarme2007@gmail.com

a protection mechanism to learn from experience and to use the existing knowledge of attacks to detect new nosy activities in MANET is most important criteria in network security. A restrictive research has to be fixed on development of security measures. Therefore the protection mechanisms need to be tough enough to protect themselves and not introduce new vulnerabilities into the system.

Aakanksha Jain et al. (2014) in their process of "Rushing attack prevention algorithm for MANET using random route selection to make DSR and AODV more efficient" basic information about the features and applications of ad hoc networks and rushing attack was given. The issue of security, confidentiality and data integrity in mobile ad hoc networks was addressed by examining various previous important routing protocols such as AODV, DSDV, and DSR. Previous work in the area of rushing attack was explained and described, along with the solutions that can assist in preventing rushing attack. This paper proposed the best solution in detail for preventing rushing attack in mobile ad hoc networks, SDSR and DSR developed to improve security in this network. Firstly, to reduce overhead by using the DSR algorithm and secondly, the message that received by the destination node itself to determine the safest and fastest route.

Satyam Shrivastava et al. (2013) in their process of "Rushing Attack and its Prevention Techniques" managed in two ways, as a router, to forward packet to other nodes in multi hop form, or as a host. Mobile Ad-hoc network is a wireless network, without any fixed infrastructure or access point. Routing protocols are use these nodes to forward packet from one node to another node. Proposed routing protocols works in MANET as on-demand form. These on-demand protocols have faster reaction time and lower overhead. This paper is based on Rushing attack. Rushing attack exploits this duplicate suppression mechanism by quickly forwarding route discovery packet in order to gain access to the forwarding group. In this paper, we focused on various techniques, which are used to overcome the rushing attack and also focus on how they work.

Gajendra Singh Chandel et al. (2013) describes the process of "Study of Rushing Attack in MANET" described various types of attacks, rushing attack have been described thoroughly. Rushing attack against on-demand ad-hoc routing protocol. It bring a denial-of-service against the ad-hoc routing have been described thoroughly and rushing attack against on-demand ad-hoc routing protocol. The attacker floods the network with bogus request and increase the traffic & thus the response time of nodes increases thus by using duplicate suppression mechanism gain access to information. In this paper a technique proposed of RAP (Rushing attack prevention) in which a threshold value set to a level for the response time.

Swarnali Hazra et al. (2012) in their work "Rushing Attack Defending Context Aware Trusted AODV in Ad-Hoc Network" proposed a new solution using trust approach, against the rushing attack problem for existing on demand routing protocol AODV, in ad hoc networks. With the help of proposed trust model, all CAT-AODV-R supported nodes cooperate together to detect and avoid misbehavior-1 (M1) or misbehavior-2 (M2) behaving rushing attacker nodes in a more reliable fashion. Our detection-avoidance scheme detects the misbehaving rushing attacker nodes and isolates them from the active data forwarding and routing on the basis of belief-disbelief decision which comes from evaluated trust value. More research into this novel mechanism for secure routing is necessary.

Parthiban et al. (2012) in their work on "Neighbour Attack and Detection Mechanism in Mobile Ad-Hoc Networks" described Neighbour attack, a novel and powerful attack against on-demand ad-hoc network routing protocols. This attack allows attacker to disturb multicast routes against previously proposed on-demand ad hoc network routing protocols. They have also presented Secure Neighbour Detection Mechanism (SNDM), a new mechanism that prevents the neighbour attack. They have arrived at the following conclusions regarding neighbour attack solution. The work of a small multicast group will degrade seriously under these types of attacks even the solution is available. A broad multicast group with a high number of senders and/or a high number of receivers can defend good performance under these conditions due to more alternative paths in the routing network. With regard to attack positions near the senders are the most detrimental positions since the original packets are cached early, before being cloned at branch points. However, when the number of attackers is smaller than the multicast senders, the maze center is the strongest attack position, causing the most packet damage.

ALshahrani et al. (2011) in their work on "Rushing Attack in Mobile Ad Hoc Networks" addressed the issue of security in mobile ad hoc network by examining various routing protocols such as AODV, DSDV, DSR and PAODV. Different types of attacks which threaten MANETs were overviewed. This paper studied in detail one of the solutions for preventing rushing attack in mobile ad hoc networks, SDSR and attempted to improve security in this network, with two important goals in mind: to lower overhead and to ensure there are safe neighbours in the network. This thesis proposed two solutions: firstly, to reduce overhead by using the old algorithm and secondly, the message that sent to the node itself to determine the safest and fastest route.

III. PROPOSED TECHNIQUE

Rushing Attack Formation Algorithm

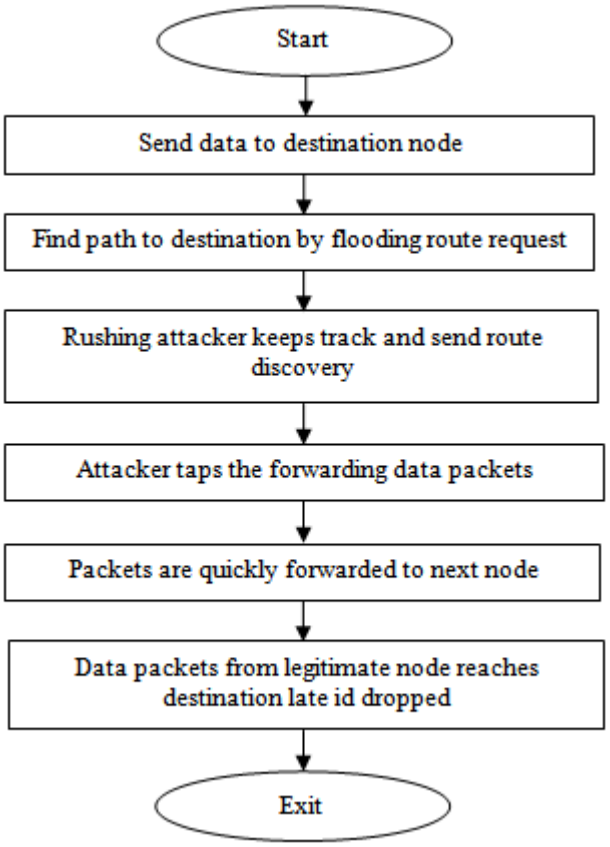

Figure 4.3 Rushing Attack Formation Algorithm

A rushing attacker uses the duplicate suppression mechanism thus the response timing of the malicious nodes is extremely fast and can send a route discovery to the sender, and gain access on the forwarding data. In this way the non-legitimate node keep sending the requests and hence accessing the networks queue. Because of this, attack requests sent by legitimate node will be considered as delayed request and hence discarded. The overall rushing attacks formation Algorithm given in flow chart.

The Concept of Average delay

To reduce the problem of rushing attack, we use the concept of average delay value. We know that in rushing attack, the attacker quickly forward the RR packet. That by receiver receives this rushed packet and discards other legitimate RR packet. To overcome this problem we use average delay value. It is a fixed value for a transmission. There is guidance for all the nodes that the packet must be reached to the neighbour node at the average time interval. If there is rushing attacker present in the network then it will quickly forward the packet and it will reach the neighbour node before the average time interval. If the neighbour node found any attacker by calculating time interval. It will inform about the attacker to all other nodes in the network.

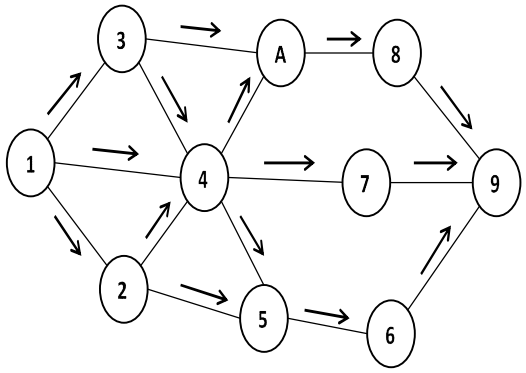

Figure 4.2 Rushing Attack with Threshold Value

In this figure 4.2 node 1 send the packet to node 9. Now assume, average delay value for this network is 8 seconds, means a packet will take 8 seconds for travelling from one node to another. Node 1 sends a packet to 2 and 3. The packet will reach in 8 seconds then node 2 sends a packet to 4 and 5, it will also reach in 8 seconds and 3 sends a packet to 4 and A, Which will also reach in 8 seconds. Node 5 send packet to 6 and 4 send packet to 7 in 8 seconds. A is an rushing attacker so it will quickly send the packet to 8 and this packet reach in 3 seconds to node 8. Node 8 knows that the average delay value is 8 seconds and packet comes in 3 seconds, means there is an attacker so it inform to other node about the attacker and it will not accept that packet. So that receiver node 9 will accept the packets which come from 6 and 7.

Proposed Rushing Attack Prevention Technique:

In this section, a new method is proposed for preventing the network from rushing attack, which exploits the duplicate suppression mechanism. The proposed method uses the AODV and DSR protocol to forward the packet.

These are reactive protocol, so security requirement is high. The proposed method is based on the following model, which consist of nine steps. The proposed model is,

Source node decide to send the data to the destination, then it initiate RREQ packet and forward it to its neighbors.

i. Intermediate nodes check the source address of the RREQ packet. If RREQ packet from the same source already exist, then intermediate node discard the packet, otherwise intermediate node process RREQ packet.
ii. Then check the source address path if already exists, fetch the time information and process the packet as normal.
iii. Otherwise calculate the delay time by subtracting sent time from received time and compare with Average delay value which is already defined.
iv. If the delay time is lower than average time then declare the node as attacker and put the node information to block list. Block list information will be broadcast to every other node in the network. Otherwise fetch the time information and process the packet as normal.

IV. SIMULATION STUDY

Network Simulator (Version 2), widely known as NS2, is popular simulator in scientific environment. It is a discrete event simulator targeted at network research and focused on modeling network protocols such as ad hoc routing, sensor networks etc. NS2 is based on two languages. They are object oriented simulator (C++) and OTcl (object oriented Tcl) interpreter.

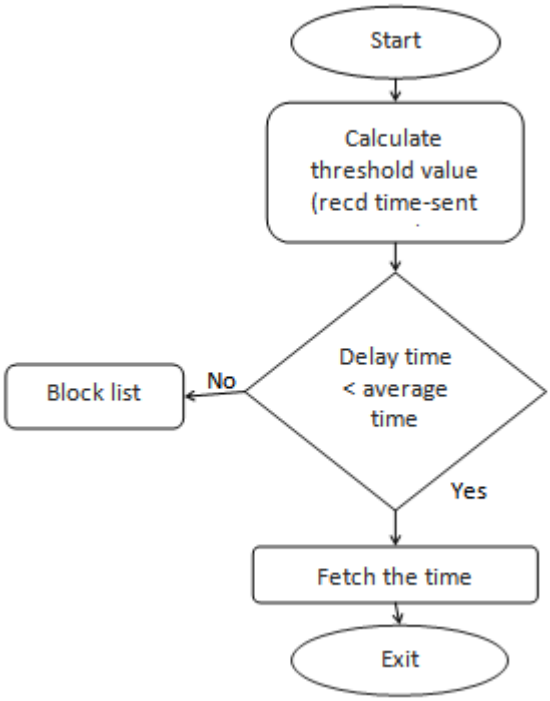

Figure 4.4 Proposed Rushing Attack Prevention Technique

The below graph helps to evaluate the performance of a MANET environment Rushing attack by calculating the Packet Delivery rate and Packet Dropped rate for each of these increasing transmission times in sequential order. The respective graphs drew with these parameters helps to analyze the performance.

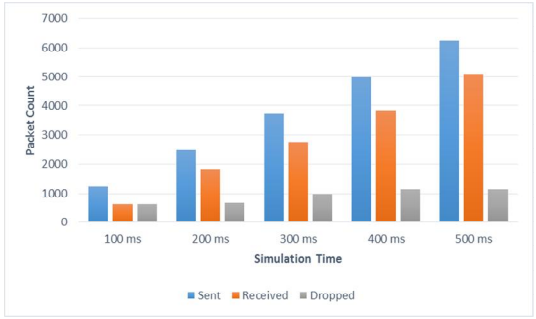

Figure 4.5 Simulation time vs. Packet count

The respective graphs drew with common parameters (Packet sent, Packet received, and Packet dropped ratio). The below graph helps us to compare the performance after prevention of rushing attacker with rushing attacker environment. After prevention, the packet dropped ratio drastically reduced and packet transmissions are working in normal way.

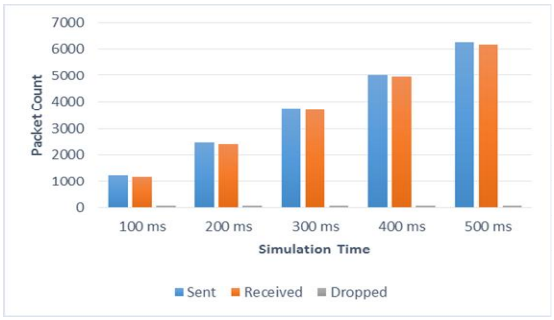

Figure 4.6 Simulation Time vs. Packet Delivery Rate

The performance of MANET environment is analyzed with increasing transmission time and calculating the Packet Delivery rate and Packet Dropped rate for each of these increasing transmission times in sequential order.

The below graph depicts the performance of a network. It shows the Control overhead decreases drastically when the prevention of MS-AODV protocol is applied in the network.

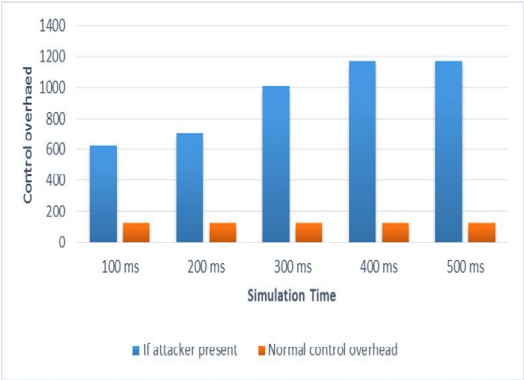

Figure 4.7 Simulation Time vs. Control Overhead

The below process represents increase of simulation time over the network. Since the malicious nodes drops the packets that are sent to the destination by acting as intermediate node between both the source and destination. Because of dropping packets throughput of packets transmission decreased. After implemented the prevention protocol (MS-AODV) the throughput of transmission is increased.

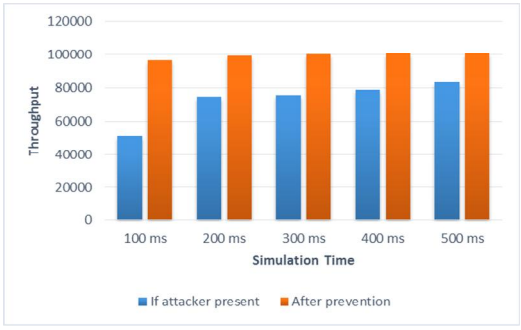

Figure 4.8 Simulation Time vs. Throughput

V. CONCLUSION

This paper gives a study of rushing attack and its effect in MANET. 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. This paper proposes Rushing attack prevention can be done by calculating delay time and compared with average delay time. The result depicts the proposed method working with 200 nodes.

REFERENCES

[1] Chinkit Suthar and Bakul Panchal, "A Survey on Rushing Attack and Its Prevention in Mobile Ad-hoc Network" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014.

[2] Shikha Jain, " Security Threats in MANETS: A Review" International Journal on Information Theory (IJIT), Vol.3, No.2, April 2014.

[3] K. Udhayakumar, T. Prasanna Venkatesan and R. Ramkumar, "Security Attacks and Detection Techniques for MANET" Discovery Journal, Volume 15, Number 42, April 10, 2014.

[4] Aakanksha Jain, Dr. Samidha Dwivedi Sharma, "Rushing Attack Prevention Algorithm for MANET using Random Route Selection to make DSR and AODV more Efficient" International Journal Of Engineering And Computer Science ,Volume 3 Issue 6 June, 2014 Page No. 6520-6524.

[5] Satyam Shrivastava, "Rushing Attack and its Prevention Techniques", International Journal of Application or Innovation in Engineering and Management (IJAIEM), Volume 2, Issue 4, April 2013.

[6] Gajendra Singh Chandel and Rajul Chowksi, " Study of Rushing Attack in MANET" International Journal of Computer Applications (0975 – 8887) Volume 79 – No10, October 2013.

[7] Sivakumar and Selvaraj, "Overview of Various Attacks in MANET and Countermeasures for Attacks " International Journal of Computer Science and Management Research Vol 2 Issue 1 January 2013.

[8] Swarnali Hazra and S.K.Setua, "Rushing Attack Defending Context Aware Trusted AODV in Ad-Hoc Network" International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.

[9] Gagandeep, Aashima and P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology, 2012.

[10] Parthiban, Amuthan, Shanmugam, and Suresh Joseph, "Neighbor Attack and Detection Mechanism in Mobile Ad-Hoc" Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, March 2012.

[11] Jan von Mulert, Ian Welch and Winston K.G. Seah, "Security Threats and Solutions in MANETs: A Case Study using AODV and SAODV" Journal of Network and Computer Applications 35 (2012) 1249–1259.