IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Intrusion Detection System for Rushing Attack in MANETs

D.Shiny, K. Ganesh Reddy, Dept. of Computer Science and Engineering
Shri Vishnu Engineering College for Women,Bhimavaram, India

Abstract

MANETs are more vulnerable to various attacks, out of which rushing attack is one of the severe attack. The existing security mechanisms are inadequate to detect gray hole attack. In this paper, we propose a IDS for high detection rate of rushing attack with less control overhead. Our proposed IDS works based on trust node approach, and key functionalities of this approach are 1) maintaining trust of neighboring nodes and 2) increase/decrease trust of a node. Our Simulation results show that the proposed mechanism has a significantly high detection rate which improves network performance such as packet delivery ratio.

I. INTRODUCTION

MANETs are more vulnerable especially in network layer followed by MAC layer and Physical layer[3][2]. Network layer attacks can affect the network performance in the form of control plane attacks or data plane attacks, or both. The control plane attacks disturb the routing paths by flooding fake route requests and replay messages. In addition to this, attackers use the fake/stale control packets to join in active route. Once, attacker joins in active route, attacker can create the data plane attacks.

Data plane attacks are more severe than control plan attacks, because data plane attacker can perform various malicious activities such as drop, modify, inject fake packets etc. on received data packets. In this paper, we address a rushing attack in MANETs. It is a similar kind of blackhole attack (drop all packets), but more sophisticated attack as compared to blackhole attack [1]. Initially, a rusing node joins in active route by using fake/stale control packets. When the data packets start moving through this node, it drops the packets in selective intervals. Detecting this attack is more complex than blackhole because packet drops occur not only because of malicious behaviour, packet drops can also occur due to communication errors, hardware error and buffer overflow etc.

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Existing intrusion detection systems (IDS) mainly come under two approaches: node dependent approach and node independent approach to address gray hole attack in MANETs. Node dependent approach works on a group of nodes, where all the nodes trust each other for isolating malicious nodes from their group[4][5][6][7]. If a group node detect a malicious node then this information broadcasts to all its group members for isolating malicious node from their group.

In node independent approach, a node in a network directly monitors the other nodes behavior. Based on the monitored nodes behaviour, a node takes its own decision whether they are malicious or non-malicious nodes [8][9][10]. When we compare both the approaches, node independent approach has less false alarm rate compare than node dependent approach because each node in node independent approach takes decision on other network nodes based on its direct observations only. In addition to that, node independent approach creates less control overhead than the node dependent approach.

II. PROPOSED SYSTEM

In order to overcome existing problems we introduced the technique trusted node for rushing attack.This technique is used to detect rushing attack in MANET.

How trust node works?

- Make the group of nearer nodes into clusters.
- Trust nodes are placed middle of the cluster to monitor the neighboring nodes.

If trust node find any malicious node, then it forward the information to all other nodes in the network.

Proposed Algorithm

Algorithm

Step: 1 Trust node placed in the network to monitor the neighboring nodes and communicate with other trust nodes.

Step: 2 Formula for calculating trust nodes in the network

$$m=T^2/\pi\, r^2*1.5$$

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Where m=minimum number of nodes

T=total distance covered by nodes

r=each node radius

Step: 3 threshold value

Initially T=t (when the behavior of a node is normal)

The 'T' value decreases based on the misbehavior of a node as

(t-1,t-2).

Step: 4 Trust node can identifies in 3 ways

1. **Packets dropped-** the difference between the generated and received packets (t=t-2).

Packet drop= total number of packets generated/number of packets received*100

Pd=Gp|Rp

2. **Delay-** the difference between the sender generated time and receiver received time (t=t-1).

Packet delay=total time generated/total time received*100

d=Gt|Rt

3. **Non malicious** (t=t+1)

Step: 5 if any node trust value t=0 then that node is a malicious node this step drop periodically.

Step: 6 Trust nodes forward the malicious node information to remaining trust nodes.

Step: 7 All trust nodes sends the information to neighboring nodes, then receiver discard the packet and it finds new path for sending data.

III. RESULTS AND DISCUSSION

Simulation Setup

. Conventional AODV protocol doesn't provide any security related to rushing attack. Here, the AODV routing protocol is modified such that it detects the Rushing attack in wireless ad-hoc networks.

Table 5.1: Simulation Parameters

PARAMETER	VALUE
Number of nodes	20
Simulation time	100sec
Routing Protocol	AODV
Queue Type	Drop Tail
Packet Size	1500 bytes
Transport protocol	UDP

I have installed ns2.33 in Windows 7 using Cygwin. I have created the Rushing module in ns2.33.

6.1 PACKET DELIVERY RATIO

IJMTARC – VOLUME – IV – ISSUE - 16 - DEC 2016 ISSN: 2320-1363

Packet delivery ratio (PDR): defines as the ratio of the total number of data packets successfully delivered to the destination to the total number of data packets sent out by a source node.

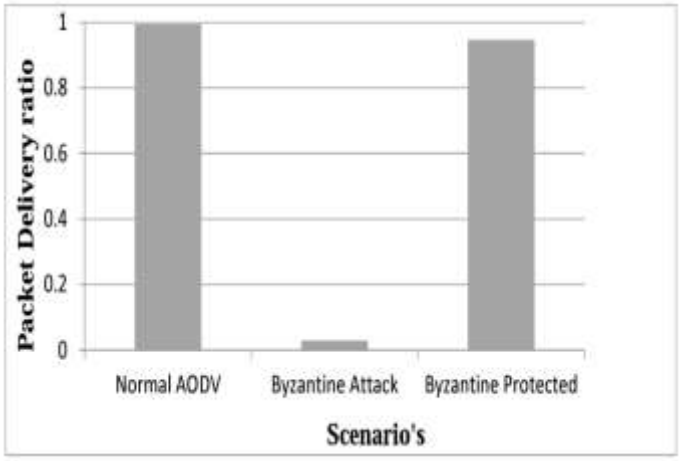

Figure 1: Packet delivery ratio

Under the attack the packet drop ratio will be more because the node will suddenly changes its behavior and drops the packet or modifies the packet. By our proposed solution the packet delivery ratio is almost equal to the normal AODV.

The Fig. 1 is plotted packet delivery ratio versus different scenario's where time taken on X-axis and packet delivery ratio taken on Y-axis. It is observed from the Fig. 1, that our mechanism gives increased throughput and packet delivery ratio because our method block the attacker node and choose another route after detection of Rushing attack. Using our detection mechanism with AODV gives increased throughput and packet delivery ratio in different scenarios.

IV. CONCLUSION

In this paper, we proposed an intrusion detection technique to protect MANET from rushing attack. Due to Rushing attack, initially packets are dropping rapidly, but after setting up IDS, a secure route is created and network behaves Rushing-free. This technique also effectively isolates the Rushing attack from source and destination by changing the traffic to other route. Eventually, our proposed

approach greatly improves the throughput and packet delivery ratio of MANETs. Due to Rushing attack, initially packets are dropping rapidly, but after setting up IDS, a secure route is created and network behaves Rushing-free. From the results, packet deliver ratios are 0.995, 0.0285, 0.9475 for Normal, Rushing attack and Rushing protected AODV respectively.

References

1. Shabir Sofi, Eshan Malik, Rayees Baba, Hilal Baba, Roohie Mir, “Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation”, ICCIT, 2012.

2. Mahamood ul Hasan MD, Syed Shaheen, “BSMR: Byzantine resilient secure multicast routing in multihop wireless networks" International Journal of Computer Trends and Technology- volume3,Issue2- 2012.

3. Tian Lan, Ruby Lee, and Mung Chiang, “Multi-path Key Establishment under Byzantine Attacks in Wireless Ad Hoc Networks”, INFOCOM, 2009.

4. M. Serafini, N. Suri. "The fail-heterogeneous architectural model". In *Proceedings of the 26th IEEE International Symposium on Reliable Distributed Systems (SRDS ’07)*, pages 103–113,Beijing,China,2007.

5. D.M. Shila, Yu Cheng, and T. Anjali. "Mitigating selective forwarding attacks with a channel-aware approach in wmns". *Wireless Communications, IEEE Transactions on*, 9(5):1661-1675,may2010.

6. M. Medadian, M.H. Yektaie, and A.M. Rahmani. "Combat with black hole attack in aodv routing protocol in manet". In *Internet,2009. AH-ICI 2009.First Asian Himalayas InternationalConferenceon*,pages1–5,nov.2009

ISSN: 2320-1363

7. Pushpita Chatterjee"TRUST BASED CLUSTERING AND SECUREROUTING SCHEME FOR MOBILE AD HOCNETWORKS", International Journal of Computer Networks & Communications (IJCNC), Vol.1, No.2, July 2009.

8. Rachedi et al: Trust and mobility based clustering algorithm for secure ad hoc networks, in Proc. of ICSNC '06, October, 2006.

9. Marc Bechler and Hans-Joachim Hof and Daniel Kraft and Frank Pahlke and Lars Wolf:" A Cluster-Based Security Architecture for Ad Hoc Networks", in Proc.of IEEE INFOCOM, 2004.

10. Y.-C. Hu, D. B. Johnson, and A. Perrig, "Secure Efficient Distance Vector Routing in Mobile Wireless Ad Hoc Networks," The 4th IEEE Wksp. Mobile Computing Systems and Applications(WMCSA'02), June 2002.