ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 4, April 2013

BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs

Vipin Khandelwal[M. Tech IC], Dinesh Goyal [Associate Professor]
Department of Computer Science and Engineering
Suresh Gyanvihar University,
Jaipur, Rajasthan, India

Abstract—Causing packet loss due to attacks by malicious nodes is one of the most important problem in MANETs. There are many ways by which packet loss can occur in MANETs such as broken links, transmission errors, no route to the destination and attacks caused by malicious nodes. To determine the exact cause of packet loss in wireless network is a challenging task. In this paper, we have investigated packet loss problem caused by a malicious nodes that performs the well known attack called BlackHole attack in the network. To mitigate the effects of such attack, we have also proposed a detection technique that efficiently detects the malicious nodes in the network. We have done simulations using NS-3 simulator. BlackHole attack is also called sequence number attack because it is created using and modifying sequence number field in routing control packets. We have performed the attack and its detection method on a of the well known and largely used MANET routing protocol known as Ad Hoc Distance Vector (AODV) routing protocol. We have simulated this attack and determined effect of this attack on network performance by different network scenario. Furthermore, we have implemented a detection method that helps to isolates the malicious nodes in the network.

Index Terms—Mobile ad-hoc routing, BlackHole attack, De-tection methods, Simulation, AODV protocol, Performance Eval-uation.

I. INTRODUCTION

Presently, there is rapid movement in infrastructure-less wireless mobile ad-hoc networks (MANET) due to their mobility and inexpensive nature. The main goal of an ad hoc network routing algorithm is to correctly and efficiently establish a route between a pair of nodes in the network. So that a message can be delivered according to the expected Quality of Service (QoS) parameters such as Packet Delivery Ratio (PDR), Routing Overhead and End-to-End Delay [7]. The establishment of a route among the nodes should be done with minimum overhead and bandwidth consumption. The highly dynamic topology changing nature of mobile ad hoc networks creates difficulty and complexity to routing among the mobile nodes within the network. [17].

Security in Mobile Ad-Hoc Network is the most important factor for the basic functionality of network. MANETs are more susceptible to security attacks than fixed network due to their features like dynamic topology, open medium, lack of central monitoring and management. The security solutions [20] for MANETs are to provide security services such as Availability, Confidentiality, Integrity, Authentication and No-repudiation.

It is quite difficult to determine which routing protocol is best. Each routing protocol has its own advantages and disadvantages. Security issues in MANET are very important concern for the functionality of the network. MANET has an open medium, changing its topology dynamically due to these characteristics so it can be accessible both legitimate users and malicious attackers. An Attacker first listen the network and after that perform some malicious activity and degrade the performance of the network. Many attack model have been already implemented. my detection technique is great help to isolates the malicious nodes in the network and improves the performance of the network under attack.

In this paper, we have implemented an attack and provide its detection technique on AODV routing protocol over MANETs. The attack that we implement is the well known attack called BlackHole attack. We have simulated packet loss problem by Node Failure, Distance Range and Network Congestion and determines how many packets are losses in the network. In ad-dition to this, we have simulated Black Hole Attack on AODV routing and also proposed its detection method and determined network performance under different network scenario. AODV uses two type's parameters i.e sequence number and hop count for forwarding routing control packets. Sequence number describes the fresh information of the network and hop count shows shortest routes. AODV routing protocol prefers freshers routes comparison shorter routes so malicious node takes the advantage assigning big sequence number in a route reply message and able to redirect the route.

The remainder of the paper is organized as follows. In Section II, we present an overview of related work done on attacks on MANETs routing protocols. Section III, we present the implementation details of attack and detection method we performed in this paper. In Section IV, result evaluation through simulations and analysis is discussed. Finally a conclud-ing remark with direction for future work is given in Section V.

II. RELATED WORK

In this section, we discuss the previous work done on dif-ferent kinds of attacks and there detection methods on various routing protocol in MANETs. Routing protocols of MANETs are vulnerable a lots of Attack. Because an attacker can attack in MANET in different manners such as sending false

routing information, sending unnecessary routing message [9]. In related research K. Konate [12] has described various attack against MANETs. Here I have described various attack against Mobile ad hoc network such as Flooding Attack, Link Spoof-ing Attack, Worm Hole Attack and Routing Table Overflow. In related research Meenakshi Patel [22] has described techniques of detection and prevention attack against routing in MANET. Bansal and Baker [13] have proposed a scheme that relies on first-hand observations. Directly observed positive behavior increases the rating of a node, while directly observed negative behavior decreases it by an amount larger than that is used for positive increments. If the rating of a node dips below the faulty threshold, the node is added to a faulty list. The faulty list is appended to the route request by each node broadcasting it to be used as a list of nodes to be avoided. A route is rated good or bad depending on whether the next hop is on the faulty list. If the next hop of a route is in the faulty list, the route is rated as bad. As a response to misbehavior of a node, all traffic from that node is rejected. A second chance mechanism for redemption employs a timeout after an idle period. After a timeout, the node is removed from the faulty list with its rating remaining unchanged.

Sen et al. have presented a scheme for detection of malicious packet dropping nodes in a MANET [14]. The mechanism is based on local misbehavior detection and flooding of the detection information in a controlled manner in the network so that the malicious node is detected even if moves out a local neighborhood.

Deng, Li and Agarwal [2] have suggested a mechanism of defense against black hole attack in ad hoc networks. In their proposed scheme, as soon as the RouteReply packet is received from one of the intermediate nodes, another RouteRequest is sent from the source node to a neighbor node of the intermediate node in the path. This is to ensure that such a path exists from the intermediate node to the destination node. For example, let the source node S send RouteRequest packets and receive RouteReply through the intermediate malicious node M. The RouteReply packet of M contains information regarding its next- hop neighbor node. Let it contain infor-mation about the neighbor E. Then, the source node S sends FurtherRouteRequest packets to this neighbor node E. Node E responds by sending a FurtherRouteReply packet to source node S. Since node M is a malicious node, and thus not present in the routing list of node E, the FurtherRouteReply packet sent by node E will not contain a route to the malicious node M. But if it contains a route to the destination node D, then the new route to the destination through node E is selected, and the earlier selected route through node M is rejected. While this scheme completely eliminates the black hole attack by a single attacker, it fails completely in identifying a cooperative black hole attack involving multiple malicious nodes.

III. PROPOSED METHODOLOGY

BlackHole Attack is a type of Denial-of-services (DOS) attack. This is also called Sequence Number Attack (SNA) because it is created by sequence number. Sequence number is monotonically increasing number and maintained by originator node of the RREQ and RREP message in the network. AODV routing protocol includes key features such as RREQ and RREP (For route discovery), RERR and HELLO message (For route maintenance), sequence number and hop count. AODV routing protocol has every route entry is assigned by destination sequence number in the routing table. RREQ and RREP message contains several of fields are shown in above figure?? and figure ??. In BlackHole attack a malicious node receiving the RREQ message from the neighboring node and more increase the destination sequence number and send reply message to the source node. Higher value of sequence number signifies the fresh information of the network. So source node accept route reply message from the malicious node and ignores lesser destination sequence number route reply message. Network traffic redirect through the malicious node.

A. Attack Methodology

When source node S wants to send data packet to desti-nation node D. It creates route discovery process by using RREQ message having destination sequence number suppose 6 send to neighboring node P, Q and R. Figure 1 shows an example of BlackHole attack on AODV routing protocol. When neighboring node receive RREQ message from source node S it updates routing table and further rebroadcast to their neighboring nodes. Each RREQ message is uniquely identified by using RREQ Id and Source Ip address that eliminate duplicates. Route reply message (RREP) is generated by either any intermediate node having fresh route information to the destination or destination node. In figure 1 M is a malicious

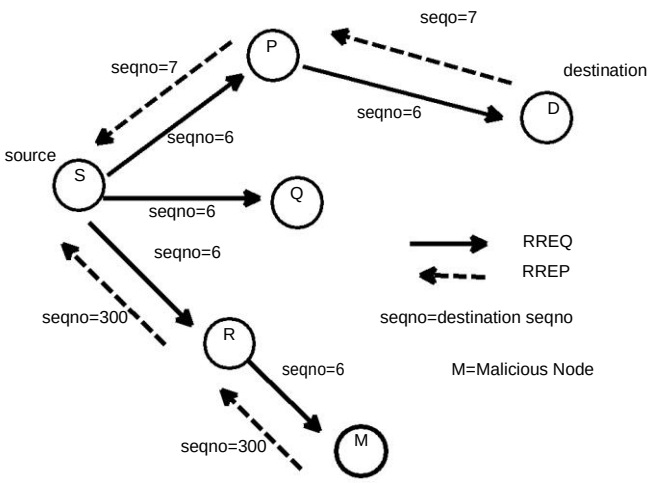

Fig. 1. BlackHole Attack on AODV

node, malicious node first listen the network. It means it received RREQ message from node R and change the value of destination sequence number and assigned higher sequence

number value suppose 300 in RREP message and without checking own routing table immediately sends out to its neighboring node R towards the source node S. When destination node D generate RREP message it increases sequence number value by one and sends to neighboring node P towards the source node S. When source node S receives multiple RREP it accepts greater sequence number RREP and ignores lesser sequence number RREP. In AODV Routing protocol higher sequence number denotes the fresh information of the network. Finally network traffic is redirected through malicious node M generated by source node S and performance of the network will be affected.

B. Detection Method For BlackHole Attack

Detection process is very complicated in Mobile Ad hoc network due to limited resources such as bandwidth, battery life and storage capacity. We should also concern minimum possible rise in routing overhead and end-to-end delay to implement any detection process in MANETs. In related research S.Kurosawa [16] has implemented detection method against AODV routing by by Dynamic Learning Method.

C. Pseudo Code for Black Hole Attack Detection Method

In this section, we present the algorithm that we have used to perform BlackHole attack detection.

- wait_RREP_Time denotes the waiting time for RREP at source Node.
- storeEntry denotes the routing table entry for storing RREP_Entry.
- new_RREP_tab denotes the new routing table for storing routing table entry.

```
Preprcess_RREP_RecvReply(Packet p) {
        RrepHeader RREP_Entry;
        p− >RemoveHeader(RREP_Entry);
        Get_t =Recv_RREP_Time;
        Set_t=Get_t+wait_RREP_Time;
        storeEntry.add(RREP_Entry);
while(Get_t<=Set_t) {
        new_RREP_tab.add(storeEntry);
        }
while(new_RREP_tab is not Empty) {
if((Dst_seq_No.storeEntry−RT.Src_seq_No)>RT.Src_seq_No)
{
        Node is Attacker
        new_RREP_Tab.DeleteRout(Dst_seq_No.storeEntry)
          }
        }
choose packet from new_RREP_tab and call normal method
RacvReply(Packet) of AODV.}
```

This detection module first stores all RREP at the source node and analyzes correct RREP that has fresh information of the route and responses to the method of the normal AODV routing process. Figure 2 shows Implementation of Detection module in AODV routing protocol against BlackHole Attack . In This process I have modified only working of source node by adding Preprocess RREP() function. This function contains a new routing table new_RREP_tab, one variable Get_t for receiving RREP time and another variable wait_RREP denotes waiting time of RREP at source node. By default source node waits 2.8 second if RREP does not receive with in time source node generate another RREQ message and broadcasts it. Source node accepts only RREP with fresh information in normal AODV routing process. But in this approach source node first call Preprocess_RREP() method and stores all RREP in newly created routing table new_RREP_tab. Each entry in routing table is assigned by destination sequence number.

After that we compare destination sequence number from new_RREP_tab and source sequence number from routing table. If destination sequence number is much higher than source sequence number it means source node discards this route entry in the new_RREP_tab routing table. Source node performs this process for all RREP that stored in new_RREP_tab routing table until new_RREP_tab table is not empty. The main goal of this approach is determine malicious node those modified destination sequence number. After this process Source node selecting a RREP from new_RREP_tab routing table and calls normal Receive Reply() method.

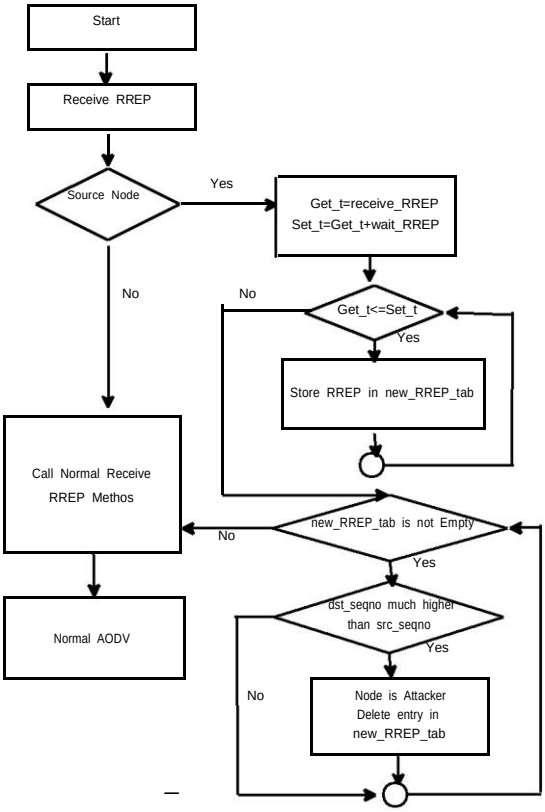

Fig. 2. Implementation Preprocess_RREP() Method in AODV

IV. SIMULATION RESULTS AND PERFORMANCE ANALYSIS

In this section, the results obtained from simulation on various scenarios are presented and discussed in detail. We have simulated BlackHole attack and determined effect of attack on performance metrics such as Packet Delivery Ratio

(PDR), End-to-End Delay (EED) by varying number of nodes, number of malicious nodes and mobility speed of nodes. Simulation parameters used to build the scenarios are shown in table I. All the simulation results are averaged using results obtained from five different simulation runs each time using different seed value. Simulations are performed using latest release of NS-3 [1].

Parameter	Value
Simulator	NS-3
Number Of Nodes	30
Simulation Time	100 Sec
Traffic Type	CBR(Constant Bit Rate)
Simulation Area	1000X1000
Packet Size	1000 Bytes
Network Structure	Grid Structure
Mobility Model	**Random Way Point Mobility Model**
Routing Protocol	AODV Routing
Speed,Pause Time	10 m/s ,2 sec
Application used	On Off Helper

TABLE I
SIMULATION SETUP PARAMETERS

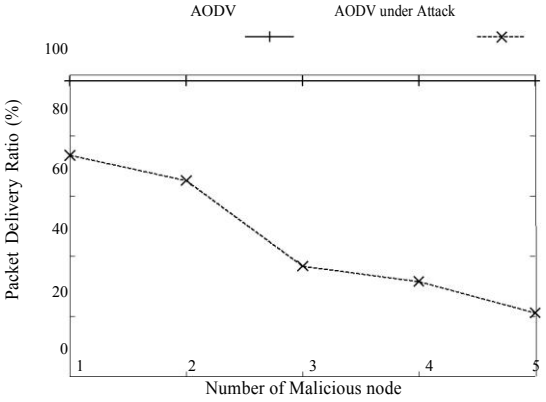

Fig. 3. Number of malicious Nodes v/s Packet delivery ratio

We have created a network by using simulation parameters shown in table I. Number of malicious nodes in the network are created randomly between one to five. When we increase number of malicious node in the network then packet delivery ratio decreases as shown in Figure 4. This is the obvious behavior we have expected because as the number of ma-licious nodes increases in the network the probability that the malicious node became the part of an active route increases.

Figure 4 shows when mobility speed is varying then Packet Delivery Ratio decreases under normal condition and under attack Packet Delivery Ratio also decreases. Because when we increase mobility speed than more links are broken in the network. Due to this routing overhead increases which increases

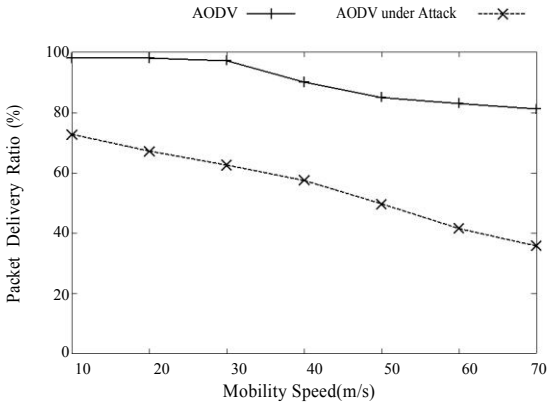

Fig. 4. Mobility speed v/s Packet delivery ratio

the network the malicious nodes get more opportunities to send false RREP packets in the network increases.

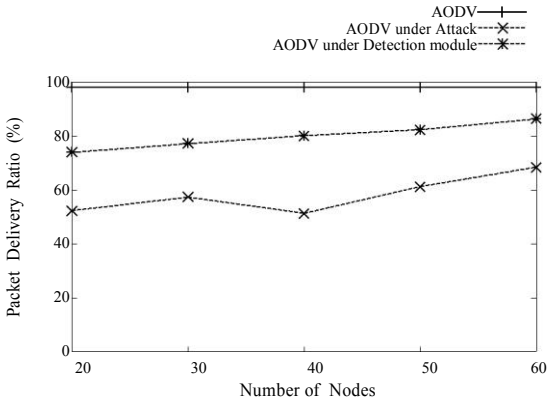

Fig. 5. Number of nodes v/s Packet delivery ratio

contention in network, therefore PDR decreases significantly. Furthermore, as the number of routes broken in

Figure 5 shows the results of attack with the increase in number of nodes in the network. As the number of nodes in the network increases PDR of AODV decreases due to increase in the number of intermediate nodes on a route. This is because the increase in number of intermediate nodes on an active route increases the probability of route failure. The PDR of AODV with attack decrease even more due to the probability that the malicious node become an intermediate node on an active route. On the other hand, the PDR of AODV with attack detection is greater than AODV with attack because our detection approach is able to identify more than 70 percent of malicious nodes which greatly increases the network PDR.

In Figure 6 and Figure 7 shows the affect of attack and its detection method on average end-to-end delay. We can observe from the figure that our detection method significantly decreases average EED.

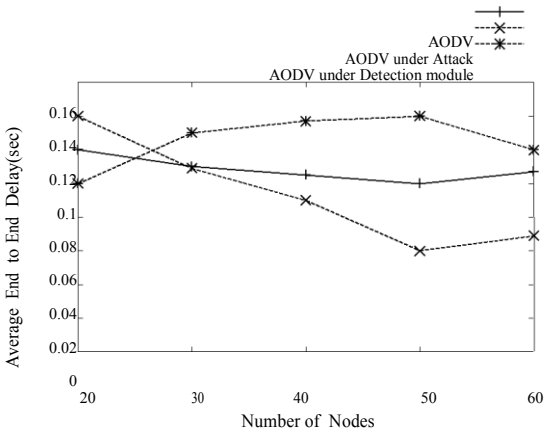

Fig. 6. Number of Nodes v/s Average Delay

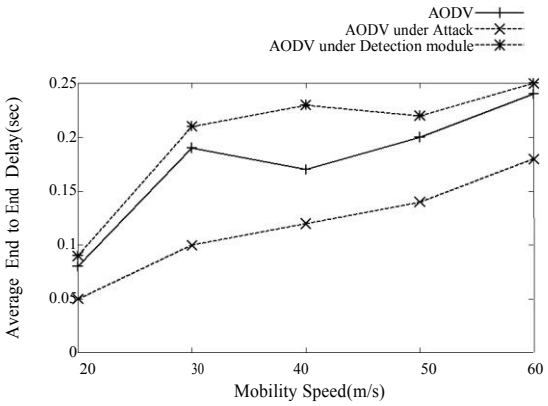

Fig. 7. Mobility speed v/s Average Delay

V. CONCLUSION

From the above shown graphs and tables we can understand that the malicious node degrades the the performance of the network. AODV routing protocol uses sequence number to determined freshness of the network topology information. Malicious node takes the advantage of this sequence number creates attack in the network by increasing higher value. So AODV lacks security [21]. Detection process is very difficult because MANETs has various resources constraints. We have also consideration performance metrics such as End-to-End Delay, Packet Delivery Ratio, Routing Overhead to implement any detection techniques in routing protocol. So here I have implemented detection module in AODV at source node. This technique does not change more functioning of the AODV routing protocol but introduces additional delay due to pre-process. This techniques is also useful for other routing protocol to isolates malicious nodes in the network.

REFERENCES

[1] "ns-3 reference". http://www.nsnam.org/, 2011.

[2] A.Boukerche. Performance Evaluation of routing Protocol for AdHoc Wireless Network, Mobile Network and Application, 2004.

[3] Md.Arafatur, Jannatul Naeem. A Simulation Based Performance Comparison of routing Protocol on Mobile Ad-hoc Network. In *International Conference on Computer and Communication, 2010.IEEE*

[4] Kumar B.R.,Lokanatha C.Reddy, Prakash S.Hiremath. Performance Comparison of Wireless Mobile Ad Hoc Network Routing Protocols. In *International Journal of Computer Science and Network Security,june 2008.*

[5] Suresh Kumar, Diwakar Pandey. Traffic pattern based Comparison of Two Reactive Routing Protocols for Ad Hoc Networks. *2009 IEEE International Conference*, pages 369-373,2009.

[6] C. Perkins, E.M. Royer and S.Das. University of California, Santa Barbara. RFC3561 - Ad hoc On-Demand Distance Vector (AODV) Routing, July 2003

[7] Avinash Patel,Linganagouda Kulkarni. QoS Parameter Analysis on AODV and DSDV Protocols in a Wireless Network. In *International Journal of Communication Network and Security*, pages 62-70, 2011.

[8] B. Kannhavong, H.Nakayama. A Survey of Routing Attacks in Mobile Ad Hoc Networks. In *IEEE Wireless Communication*, pages 85-91, 2007.

[9] Sudhir Agrawal, Sanjeev Jain. A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks. Journal of computing, January 2011.

[10] A.Bhattacharya, H. Nath Saha. A Study of Secure Routing in MANET: various attacks and their Countermeasures. IEMCON 2011 organised by IEM., january 2011.

[11] Priyanka Goyal Vinti Parmar. MANET: Vulnerabilities, Challenges, Attacks, Application. In *IJCEM International Journal of Computational Engineering Management*, Jan 2011.

[12] K. Konate, Gaye Abdourahime. Attack Analysis in mobile ad hoc net-works: Modeling and Simulation. In *2011 Second Internal Conference on Intelligent System, Modeling and Simulation*.

[13] Satyanarayan Vuppala, Alokparna Bandyopadhyay. A Simulation Anal-ysis of Node Selfishness in MANET using NS-3. In *Int. J. of Recent Trends in Engineering and Technology*, Nov 2010.

[14] S. Bhargava, D.P. Agrawal. Security Enhancements in AODV protocol for Wireless Ad Hoc Networks. In *2001 IEEE*.

[15] R.H Rashid Khokhar , Md.A. Nagdi. A Review of Current Routing Attacks in Mobile Ad Hoc Networks. In *International Journal of Computer Science and Security*, pages 18-29, 2009.

[16] S.Kurosawa, H.Nakayama. Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. In *International Journal of Network Security*, pages 338-346, Nov 2007.

[17] Kimaya Sanzgiri, Bridge Dahill. A Secure Routing Protocol for Ad Hoc Networks. In *10 th IEEE International Conference on Network Protocols*, 2002.

[18] Giovanni Vigna, Sumit Gwalani. An Intrusion Detection Tool for AODV-based Ad hoc Wireless Networks. In *Annual Computer Security Applications Conference*, 2004.

[19] Z. Ahmad, K.A. Jalil. Black hole effect Mitigation in AODV Routing Protocol. In *2011 IEEE*.

[20] M.N Lima, A.L. Dos, Guy Pujolle. A Survey of Survivability in Mobile Ad Hoc Networks. *IEEE Communications Surveys and Tutorials*, 2009.

[21] F.Mann Y.Abbas, N.Mazhar. Vulnerability Assessment of AODV and SAODV Routing Protocols Against Network Routing Attacks and Per-formance Comparisons. In 2011 Wireless Advanced.

[22] Meenakshi Patel, Sanajy Sharma. Detection and prevention of Routing Attacks in MANET using AODV. In *International Journal of Advanced Research in Computer Science and Electronics Engineering*, 2012.

Vipin Khandelwal
Student M.Tech IC
Suresh Gyanvihar University

Dinesh Goyal
Associate Proffesor
Suresh Gyanvihar University