Detection of Blackhole Attack Using Intrusion Detection System in AODV Based MANET

Nikita Patel[1], Jay Amin[2]

[1] Department of Computer Engineering, LJIET, Ahmedabad, Gujarat, India

[2]Assistant Professor, Department of Computer Engineering, LJIET, Ahmedabad, Gujarat, India

ABSTRACT

Mobile adhoc networks (MANETS) are highly dynamic in nature. There is no central device which can monitor whole network traffic and any node can join and leave network at any time. Hence any type of intruder can attack on various routing protocols. There are several attack on MANET.Blackhole is one of the attack in which malicious node advertise itself as having shortest path and with highest sequence number.In this paper we have reviewed scenario of blackhole attack and various technique to detect and prevent blackhole attack in MANET.

Keywords – *AODV,Blackhole,MANET*

1. INTRODUCTION

MANET is self-configuring, infrastructure less network of wireless mobile devices which communicate with each other on the basis of mutual trust.MANET is widely used in milatary purpose, disaster recovery, and personal area network and so on. In MANET every node act as a router which passes data for another node while they are not within each other's transmission range. MANET are more vulnerable to malicious attack because of its feature like dynamically changing topology, open medium, lack of central monitoring management these attacks are wormhole attack, blackhole attack, jellyfish attack, granola attack, denial of service attack, snooping attack etc. In this paper we define a blackhole attack in AODV routing protocol in mobile adhoc network we used AODV because it is widely used in MANET and having several advantages over other routing protocols security in mobile adhoc network is important in network thus in this paper we have surveyed various blackhole attack detection and prevention technique. According how information is acquired routing protocols can be classified in to reactive, proactive and hybrid routing protocols.

1.1 Proactive or table driven routing protocol

These protocols constantly maintain the updated topology of the network every node in the network knows about the other node in advance in other words the whole network is known to all the nodes making that network. All the routing information is stored in tables. Whenever there change in network topology this tables are updated according to the change. The nodes exchange topology information with each other. They can have route information any time when they needed [6].

1.2 Reactive or on-demand routing protocols.

The reactive routing protocol is equipped with another application named on-demand routing protocol. As compare to the proactive routing, the reactive routing is simply starts when nodes desire to transmit data packets. The major advantage is the reduction of the wasted bandwidth induced from the cyclically broadcast. The disadvantage of reactive routing protocol method is loss of some packet. Example of this type of routing protocols are Ad hoc on-demand distance vector (AODV) and Dynamic source routing (DSR) protocol [6]

1.3 Hybrid routing protocols

The hybrid routing protocol as the name suggests have the combine advantages of proactive routing and reactive routing to overcome the defects generated from both the protocol when used separately. Design of hybrid routing protocols are mostly as hierarchical or layered network framework. In this system initially, proactive routing is employed to collect unfamiliar routing information, and then at later stage reactive routing is used to maintain the routing information when network topology changes. The familiar hybrid routing protocols are Zone routing protocol (ZRP) and Temporally-ordered routing algorithm (TORA) [6]

2. BACKGROUND AND RELATED WORK

2.1 AODV

AODV combines the properties of DSR and DSDV. It uses route discovery process to find rout from source to destination on demand it uses routing table for maintaining route information. AODV is reactive routing protocol so it does not need to maintain routes to nodes that are not communicating AODV protocol has two mechanism

2.1.1 Route discovery process

Route discovery process use two control message RREQ and RREP when any source node S wants to send data to destination D it first initiate route discovery process. Source node create RREQ packet which contains following fields node ID, source sequence number, destination sequence number, source ID and destination ID then broadcast this RREQ packet to all its neighbour when receiving this RREQ packet intermediate node checks its own routing table to see availability of path to destination if any such route available it unicast RREP message to source otherwise it re-broadcast this message to its neighbour till reaches destination and RREP is chosen with minimum hope count and highest sequence number.

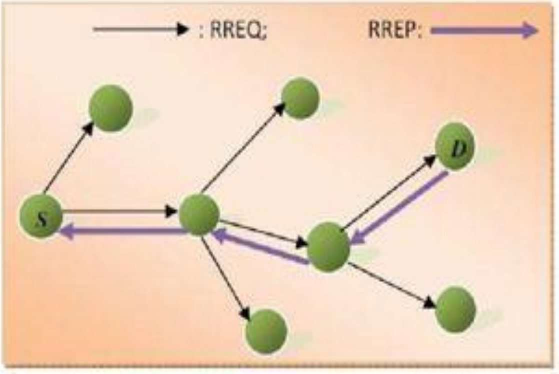

Figure.1: AODV protocol with RREQ and RREP Packet [7]

2.1.2 Route maintenance process

As MANET is highly dynamic in nature when node moves from one location to another location link between nodes is broken as shown in figure 2. When node D moves from one location to another location its neighbour node I sends RERR message to its neighbour and this message is broadcasted in network till it reaches destination

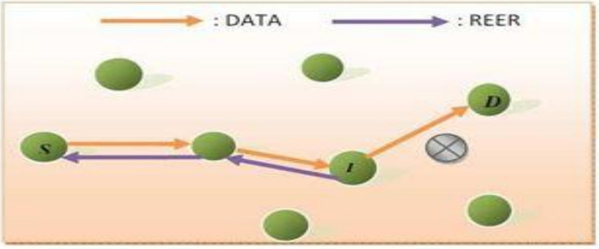

Figure 2: AODV protocol with RERR Packet [7]

2.2 Blackhole Attack

In blackhole attack malicious node advertise itself as having shortest route to destination with highest sequence number and by doing so it acquires route from source to destination and drops all the packets coming from source node without further forwarding them.as shown in figure 3 node A is malicious node now when source node wants to send data to destination D source node first broadcast RREQ message to all its neighbour.

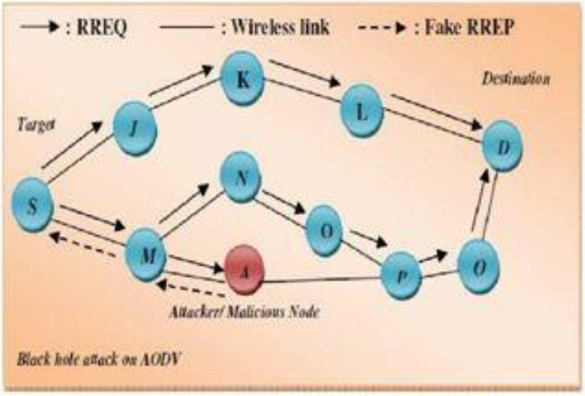

Figure 3: Blackhole attack scenario [7]

When malicious node A receives this RREQ message it immediately reply with very high sequence number and minimum hope count and then drops all the packet it receives.

Single blackhole attack

In this type of attack, one malicious node uses routing protocol to claim itself of being shortest path to destination node but drops routing packets and doesn’t forward packets to its neighbours.

Co-operative blackhole attack

Black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all receiving packets. A chance of serious damage arises if malicious nodes work together as a group. This is called cooperative black hole attack.

2.3. RELATED WORK

In [1] Ming-Yang Su proposed an anti blackhole mechanism (ABM) in which several intrusion detection nodes are deployed in network to identify malicious node. IDS node identify malicious node based on suspicious value and the suspicious value is decided based on abnormal difference between RREQ and RREP transmitted from any specific node and suspicious value will be increased by 1 when any node does not broadcast RREQ message for a route but it forwards a RREP for the route. In this mechanism several ids are within each other's transmission range so that they can share information about malicious node identified by them.

In [2] Subhashis Banrjee, Mousumi Saradar and Koushik Majumder proposed a technique to identify and remove blackhole node which include two phase blackhole identification and blackhole removal phase. In this method one addition RREQ packet is used to identify blackhole node this RREQ packet having sequence number higher than that in RREP received in first RREQ message. Now when we are sending this second RREQ message, according to nature of malicious node it reply with sequence number higher than that in second RREQ message so we can say that RREP is from malicious node and we can choose RREP from node having second highest sequence number.In blackhole removal phase is address of detected malicious node is stored in malicious node table and avoid the node in future communication.

In [3] Durgesh Shirsagar and Ashwini Patil proposed a real time monitoring scheme to detect and prevent blackhole attack.in this technique two counter fount and recount is used which is maintained by neighbour node of RREP originator node now when neighbour node forward message to RREP originator node fount will be

increased and when RREP orinator node forward packet recount will be increased,finally neighbour node forwards packect to RREP originator node until it reaches threshold thereafter if recount is zero,RREP originator node is identified as malicious node.

In [4] Yibeltal Fantahun Alem and Zhao Cheng Xaun proposed IDAD(intrusion detection using anomaly detection) technique which use host based IDS to prevent blackhole attack.In this technique IDS node provided with pre-collected set of malicious activity called audit data. Behaviour of every node is compared with audit data if behaviour of any node is resemble with audit data then that node is identified as malicious node and the IDAD system isolates the particular node by forbidding further interaction.

In [5] N. Jaisankar,R. Saravanan and K. Durai Swamy proposed a novel security approach to detect blackhole node in network.In this approach author added one additional field “next hope” in the AODV route reply packet structure before sending data packet,the first arrival of the packet with shortest path sent by the intermediate node has been checked. The route availability has been checked by the next hope node if there is no route, then intermediate node is identified as malicious node

3. PROPOSED SOLUTION

In original AODV protocol, the source node accepts the first fresh enough RREP packet coming to in our approach as show in figure we store all RREP packet in to coming RREP table till the initialization time does not expire. After that time we find average of all destination sequence number of packet stored in coming RREP table we call this value as threshold and then compare sequence number of every packet stored in coming RREP table with threshold value if this value is greater than threshold then we can say that it is RREP from blackhole node after identifying blackhole node we store node id in to MNT (Malicious Node Table) so it cannot be used by other node to transfer packets. Flow diagram for proposed work is shown in figure.

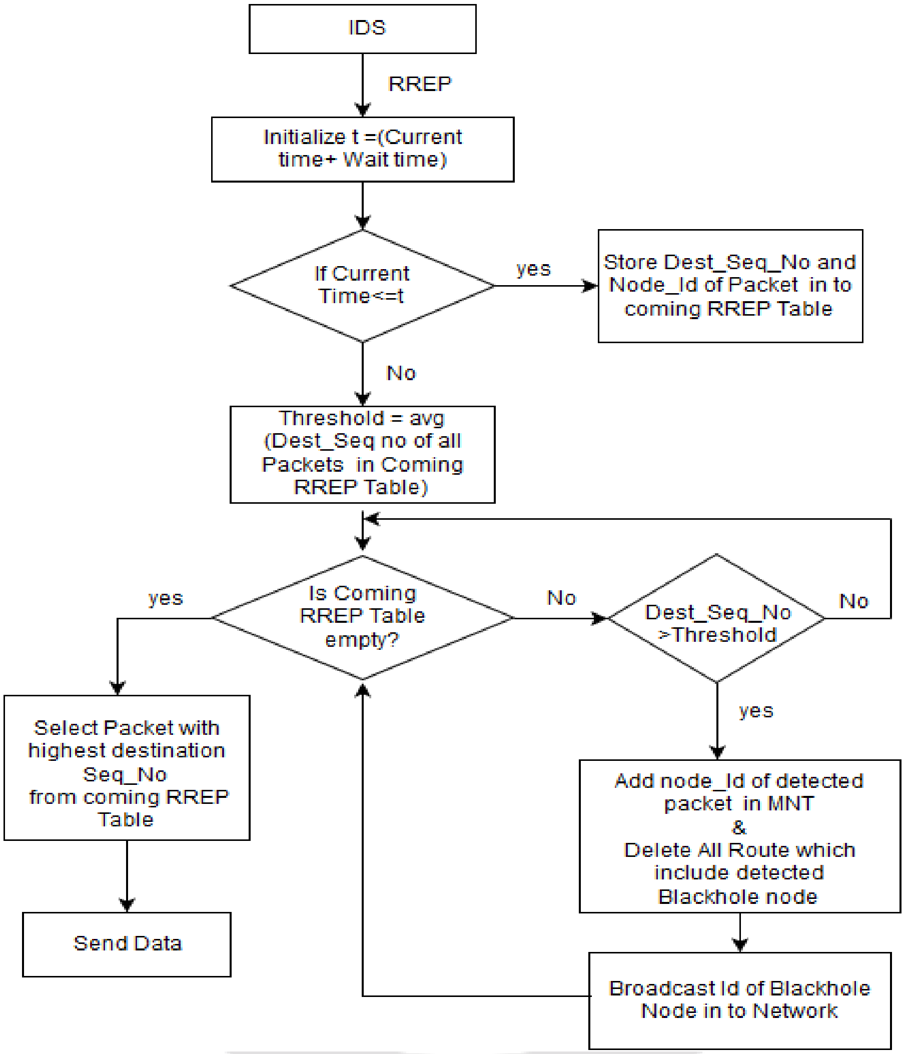
IDS
RREP
Initialize t =(Current time+ Wait time)
If Current Time<=t
yes
Store Dest_Seq_No and Node_Id of Packet in to coming RREP Table
No
Threshold = avg (Dest_Seq no of all Packets in Coming RREP Table)
yes
Is Coming RREP Table empty?
No
Dest_Seq_No >Threshold
No
yes
Select Packet with highest destination Seq_No from coming RREP Table
Send Data
Add node_Id of detected packet in MNT & Delete All Route which include detected Blackhole node
Broadcast Id of Blackhole Node in to Network

Figure 4: Flowchart for RREP Packet

4. METHODOLOGY EVALUATION

For the simulations, we use NS-2 network simulator. NS-2 provides faithful implementations of the different network protocols. At the physical and data link layer, we used the IEEE 802.11 algorithm. The channel used is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, we use AODV as the routing algorithm. Finally, UDP is used at the transport layer. All the data packets are CBR (continuous bit rate) packets. The size of the packet is 512 bytes. The packets transmission rate is 0.2 Mbps.Each data point represents an average of ten runs.

Table 1: Simulation Environment

Parameter	**Value**
Simulator	NS-2.34
Protocol	AODV
Simulation Area	500*500,700*700
Simulation Time	500sec
Pause Time	10sec
Number of Node	10,20,30,40,50
Type of Traffic	CBR

Metrics used for Simulation

Throughput: Amount of data transferred over a given period of time, here we measure throughput in kbps.

Packet loss rate: Packet loss rate can be calculated using the below formula.

(Number of packet dropped/Total number of packet sent)*100

4.1 Simulation Result

Figure shows the graph for Packet loss rate vs. number of blackhole node. Packet loss rate is less in our proposed scheme as compared to normal AODV with Blackhole attack.

Figure shows the graph for throughput vs. number of blackhole node. Throughput is high as compared to normalAODV with blackhole attack.

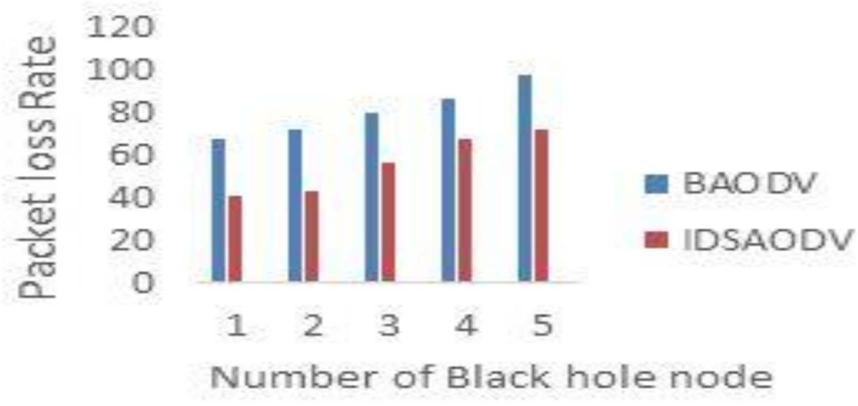

Figure 5: Graph of packet loss rate Vs. Number of blackhole node

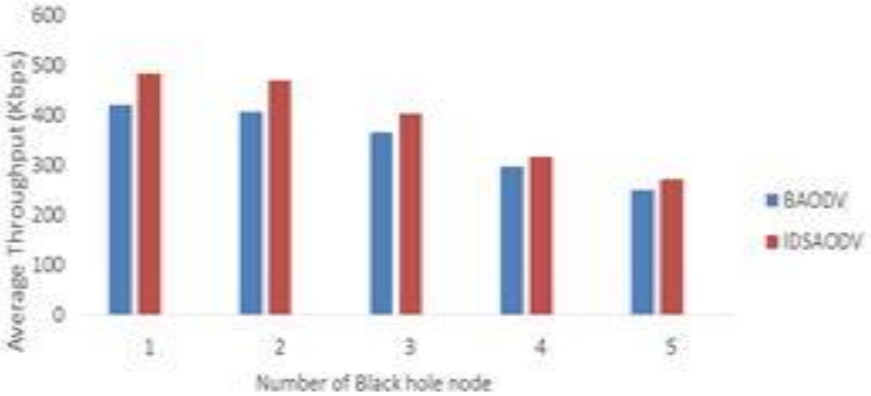

Figure 6: Graph Throughput vs. Number of blackhole node

5. CONCLUSIONS

In this paper an overview of MANET is given first. After that we introduce AODV protocol in MANET and the various authors have given several techniques for detection and prevention of black hole attacks in MANET but every technique has its own disadvantages in their respected solutions and we proposed Intrusion detection system to detect blackhole attack which decrease packet loss rate and increase throughput as compared to normal AODV with blackhole attack

6. REFERENCES

[1] Ming-Y ang Su “Prevention of selective blackhole attack in manet through ids” Elsevier Vol-34,Issue-1 ,15 January 2011, Pages 107–117

[2] Subhashis Banerjee, Mousumi Sardar, and Koushik Majumder “AODV Based Black-Hole Attack Mitigation in MANET” Springer International Publishing Switzerland 2014 Vol:247 ISSN 2194-5357 PP 345-352

[3] Durgesh Kshirsagar, Ashwini Patil “Blackhole Attack Detection and Prevention by RealTime Monitoring” Computing, Communications and Networking Technologies,2013 Fourth International Conference at Tiruchengode on date 4-6 July 2013 ISBN 978-1-4799-3925-1 PP 1 – 5

[4] Yibeltal Fantahun Alem, Zhao Cheng Xuan “Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection” IEEE international conference at wuhan on date 21-24 May 2010 vol:3 ISBN 978-1-4244-5821-9 PP V3-672 - V3-676

[5] N.Jaisankar, R. Saravanan, and K. Durai Swamy3 “A Novel Security Approach for Detecting Black Hole Attack in MANET” Springer-Verlag Berlin Heidelberg 2010 Vol:70 ISSN 1865-0929 PP 217-223

[6] sarita Badiwal,Vandana Verma “Survey of IDS in MANET against blackhole attack”International journal of Application or innovation in engineering & management ISSN 2319-4847,Vol 2,Issue 5,May 2013,PP 401-406.

[7] Dr.S. Tamilarasan “Securing AODV routing protocol from blackhole attack” International journal of computer science and telecommunications ISSN 2047-3338,vol 3,July 2012,PP 52-56

[8] A report on “Analysis of blackhole attack in MANET using different MANET routing protocol” by Irshad Ullah,Shoaib Ur Raheman at Berkelin Institute of Technology Sweden

[9] Gagandeep, Aashima, Pawan Kumar" Analysis of Different Security Attacks in MANETs" International Journal of Engineering and Advanced Technology ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012, pp-728-732

[10] Syed Jalal Ahmad, V.S.K. Reddy, A. Damodaram,and P. Radha Krishna "Detection of Black Hole Attack Using Code Division Security Method" Springer International Publishing Switzerland 2015 *Volume 2 ISSN* 2194-5357 *PP* 307-314

[11] Patel, Ravi, Khushbu Shah. *"Glance over VANET, ATTACKS over VANET and their IDS approaches."* IJIRT 1.1 (2014): 6.

[12] Patel, Ravi, and Khushbu Shah. "*Reputation Approach to detect BLACKHOLE ATTACK in VANET.*" IJIRT 1.2 (2014):6-12