DETECTION OF BLACK HOLE ATTACK ON MANET

Harshil B.Jani[1], Hardik prajapati[2]
[1]M.tech, (D.C), Research Scholar, [2]Assistant Professsor,
Electronics & communication Dept, Indus University, Ahmedabad, Gujarat
Email: janiharshil091@gmail.com[1], hardikprajapati.ec@indusuni.ac.in[2]

Abstract

This Paper analyzes on detection of black hole attack in MANET. In mobile network (MANET) more security is required in the system compared to wired network .the wireless network are susceptible to many attacks like black hole, Sybil attack, worm hole attack etc. Therefore an effective intrusion detection system(IDS) is important to identify malicious nodes to detect & isolate the problem created by such nodes and notify the information of malicious node to the other node. In This paper, a Simulation of black hole attack is done.

Index Terms: AODV protocol, blackholeattack, MANETS, Black hole attack & network through put, flowchart, NS-2 Simulator

I. INTRODUCTION

A mobile ad hoc network (MANET) is a temporary multi-hop system comprised of mobile wireless nodes. Two nodes out of direct communication range need intermediate nodes to forward their messages for secure communication. Due to routing and open working environment, MANETs are vulnerable to attacks by selfish nodes or malicious nodes, such as packet dropping (black-hole) attacks Which drops selective packets and hence, .Encrypting authentication and mechanism,& providing a secure routing protocols, have been able to develop to ensure properties such as confidentiality, integrity etc.

However, those protocols require a centralized system which is by trusted third party, making them impossible for MANETs, In addition, secure routing protocols cannot prevent malicious or compromised nodes that are authorized participants to the network from doing any misbehavior by any node in the network.

Also the concept of trust is introduced into computing network to measure an expectation or uncertainty that an required action against attack as it has about another‘s futu action. Thus, Trust can be derived from direct interactions or from recommendations. In This Paper we analyze the behavior of black hole attack effect and provide trusted mechanism using AODV-IDS against black hole attack effect and simulation of it is done

II. **AODV:**

The main objective is to provide a secured & error free communication between the two nodes .in AODV routing in this section our goal is to check whether AODV protocol is ready to work out multiple loop-free paths in a route discovery process, hence AODV can be implemented even in the existence of unidirectional links only while other links techniquesis to direct in discovering bidirectional paths in such circumstances . AODV has numerous features which are similar with AODV& MAODV.It is dependent on the distance vector theory and utilizes hop-by-hop routing technique. Also to discover the route process..

Furthermore, AOMDV also discovers routes on demand using a route discovery method. The most important variation is the amount of routes found in each route discovery Process .

In AODV, RREQ transmission path is from the source to the target which is done to establish a multiple reverse path both at intermediary nodes in addition to the destination hop also Multiple

RREPs tracks this reverse route back to form multiple hop onward routes to the target at the source and intermediary nodes. Routing protocol is an adaptation of the DSDV

Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A

RREQ (Route REQUEST) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (RouteReply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination or not.

If not, it get backs the RREQ packet by broadcasting it to its neighbors. If its routing table does contain any entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the latest sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node is dependent on the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERROR) packet to all other nodes that uses this link for their communication to other nodes. In the following illustrated figure 1, imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet, nodes 'B' 'D'and'M' receive it. Node'M', being a malicious node, does not check up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node *M* can carry out many attacks against AODV. This Solutions provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks

Here the threshold decided is 5.5-10.5

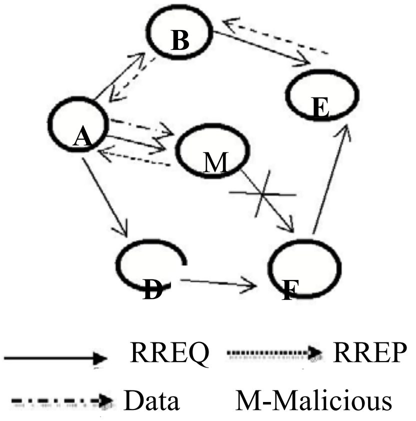
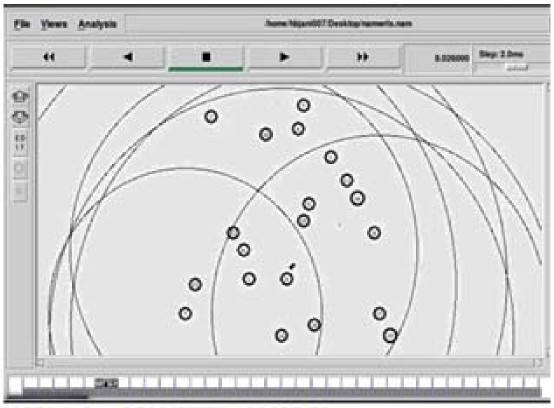


Fig1: Black hole Attack in AODV

III.SIMULATION PARAMETERS

Channel type	wireles s
Simulator	NS 2.35
TRAFFIC TYPE	CBR
ROUTING PROTOCOL	AODV
SIMULA TION TIME	100-150 SEC
NO OF NODES	20
NO OF MALICIOUS NODES	1-2



NORMAL AODV WITH 20 NODES

FIG:2 NORMAL AODV 20NODES

Here The Simulation Of 20 Nodes Is Being Done .Here Normal aodv Of 20 Nodes Is shown & Given Communication Between them& There Is No Black Hole Node

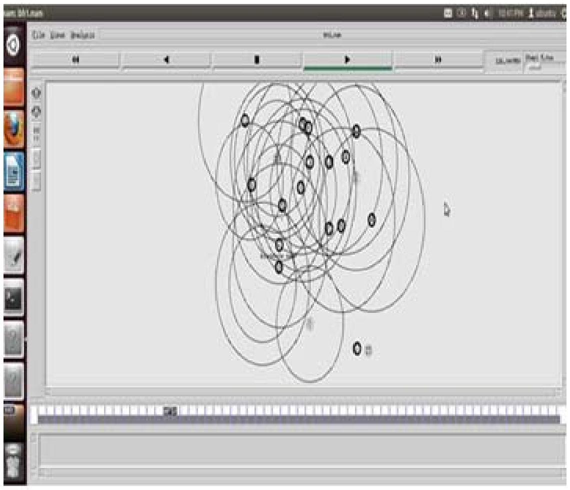
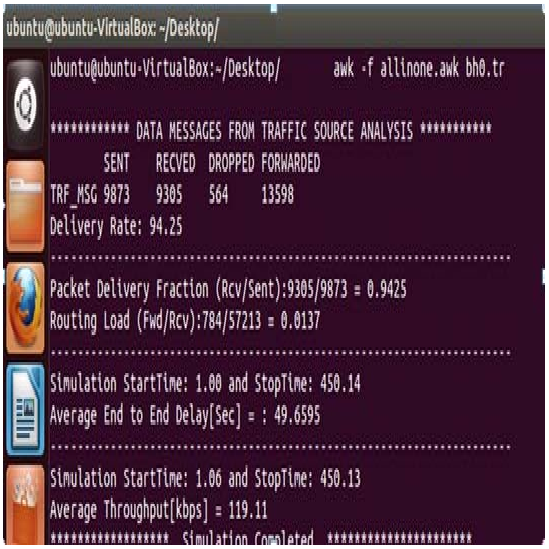


FIG 3:AODV WITH ONE BLACK HOLE NODE

HERE AODV WITH ONE BLACK HOLE NODE IS AFFECTED IN THE GIVEN AREA WHERE ONE MALICIOUS NODE IS ENTERED IN TO THE GIVEN FIELD WHICH ACTS AS NORMAL NODE BUT IS MALICIOUS AND DAMAGES THE SECURE COMMUNICATION

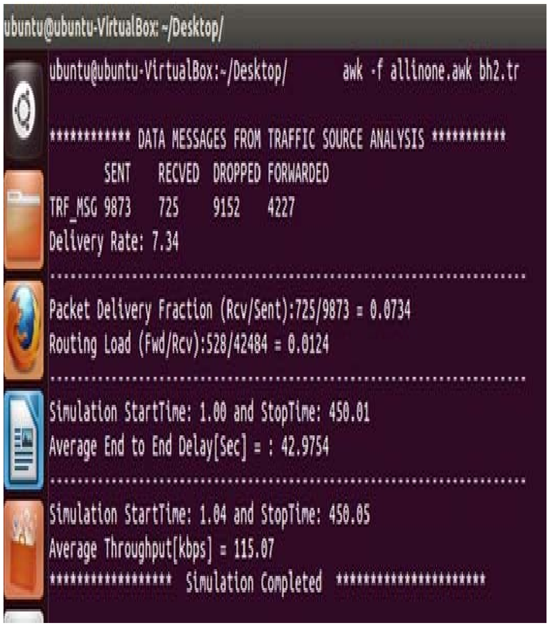
Normal Aodv



```
ubuntu@ubuntu-VirtualBox: ~/Desktop/
ubuntu@ubuntu-VirtualBox:~/Desktop/      awk -f allinone.awk bh0.tr

*********** DATA MESSAGES FROM TRAFFIC SOURCE ANALYSIS **********
       SENT    RECVED  DROPPED FORWARDED
TRF_MSG 9873   9305    564     13598
Delivery Rate: 94.25
.................................................................
Packet Delivery Fraction (Rcv/Sent):9305/9873 = 0.9425
Routing Load (Fwd/Rcv):784/57213 = 0.0137
.................................................................
Simulation StartTime: 1.00 and StopTime: 450.14
Average End to End Delay[Sec] = : 49.6595
.................................................................
Simulation StartTime: 1.06 and StopTime: 450.13
Average Throughput[kbps] = 119.11
**************** Simulation Completed ********************
```

AODV WITH BLACKHOLE NODE



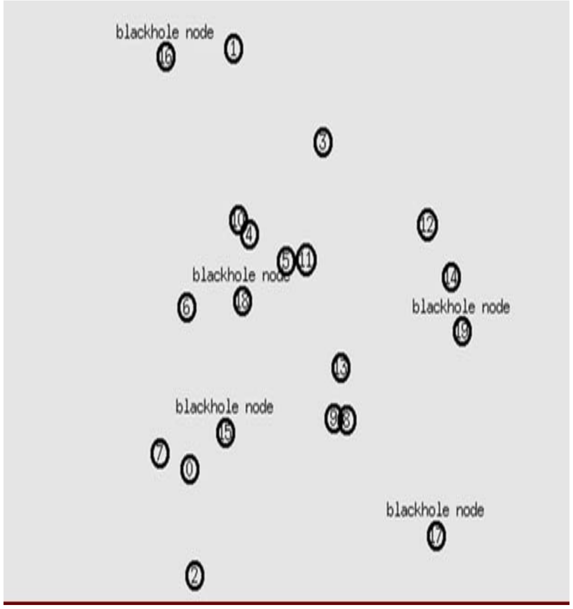
```
ubuntu@ubuntu-VirtualBox: ~/Desktop/
ubuntu@ubuntu-VirtualBox:~/Desktop/      awk -f allinone.awk bh2.tr

*********** DATA MESSAGES FROM TRAFFIC SOURCE ANALYSIS **********
       SENT    RECVED  DROPPED FORWARDED
TRF_MSG 9873   725     9152    4227
Delivery Rate: 7.34
.................................................................
Packet Delivery Fraction (Rcv/Sent):725/9873 = 0.0734
Routing Load (Fwd/Rcv):528/42484 = 0.0124
.................................................................
Simulation StartTime: 1.00 and StopTime: 450.01
Average End to End Delay[Sec] = : 42.9754
.................................................................
Simulation StartTime: 1.04 and StopTime: 450.05
Average Throughput[kbps] = 115.07
**************** Simulation Completed ********************
```

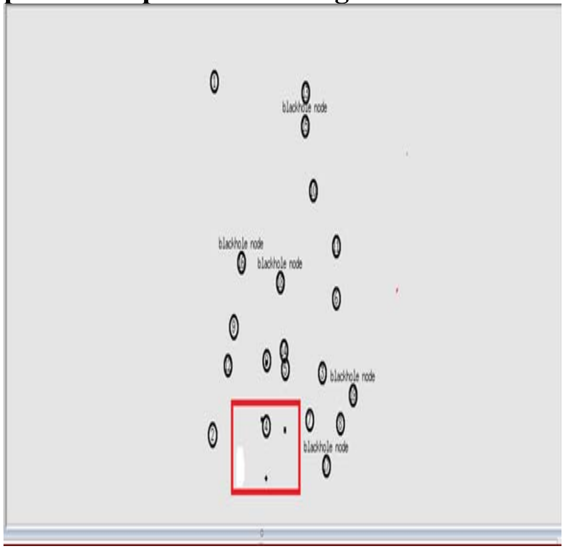
IV.DATA STATISTICS

Attack Node	Send	Recv	Drop	Forward	PDF	Routing load	End2end delay	Through put
0	9873	9305	564	13958	0.9425	0.0137	49.6592	119.11
1	9873	451	9422	11919	0.0457	0.0102	56.6143	184.66
2	9873	725	9152	4227	0.0734	0.0124	42.9754	115.07

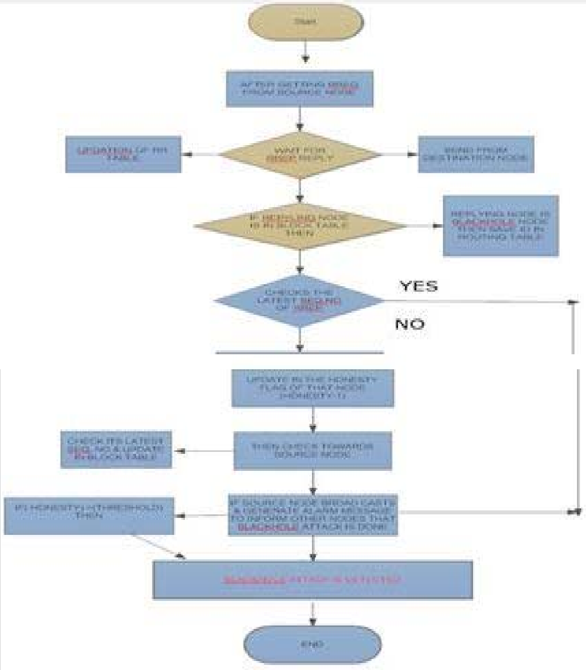
Here also the malicious nodes-5 detection of black hole attack is shown



Also the blackhole attack is done where the packet drop is shown in figure



V.Flowchart


Start
AFTER GETTING RREQ FROM SOURCE NODE
UPDATION OF RR TABLE
WAIT FOR RREP REPLY
SEND FROM DESTINATION NODE
IF REPLYING NODE IS IN BLOCK TABLE THEN
REPLYING NODE IS BLACKHOLE NODE THEN SAVE ID IN ROUTING TABLE
CHECKS THE LATEST SEQNO OF RREP
YES
NO
UPDATE IN THE HONESTY FLAG OF THAT NODE (HONESTY-1)
CHECK ITS LATEST SEQ. NO & UPDATE IN BLOCK TABLE
THEN CHECK TOWARDS SOURCE NODE
IF HONESTY<=(THRESHOLD) THEN
IF SOURCE NODE BROADCASTS & GENERATE ALARM MESSAGE TO INFORM OTHER NODES THAT BLACKHOLE ATTACK IS DONE
BLACKHOLE ATTACK IS DETECTED
END

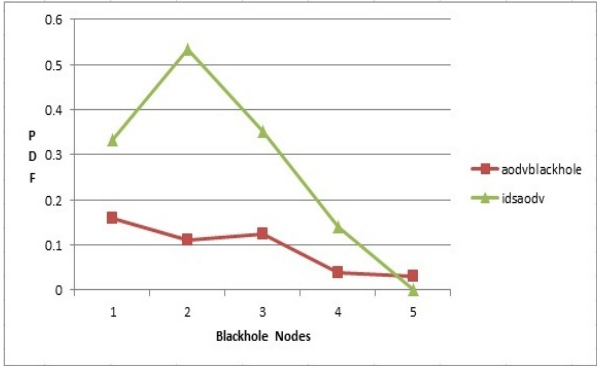
HERE the it starts the process is initiated by RREQ AND after getting the reply from the source node it initiates the given process and RREP initiates the above process is being done through the given routing table entry. Here new honesty is introduced which behaves as a normal node and (honesty-1) is done through the given flag through the given system to check it is malicious or not .

After sending RREP it waits for th neighbhours for the latest sequence number is to be achieved and the hop count by 1 through BLACKHOLE IS DETECTED ,Also neighbours inform the intermediate nodes by sending ALARM PACKETS about BLACKHOLE NODE IS DETECTED.

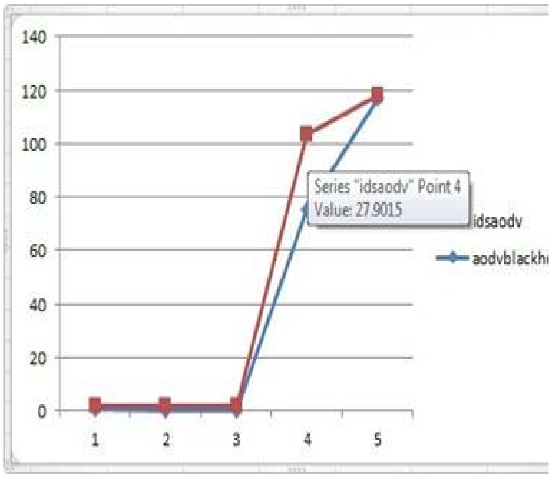
VI.GRAPH:

HERE THE GRAPH OF 5 MALICIOUS NODES IS TAKEN INTO CONSIDERATION BY FOLLOWING PARAMETERS:

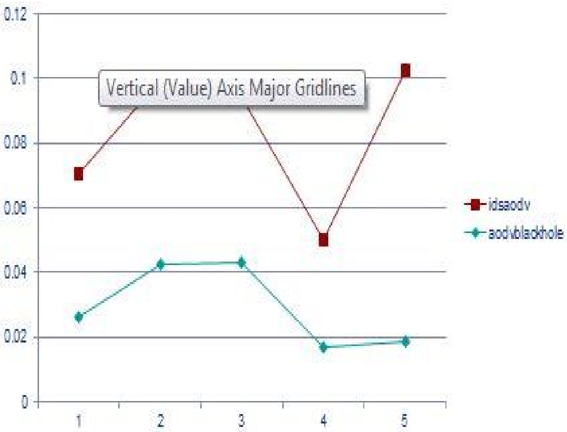
(1)**PDF**:



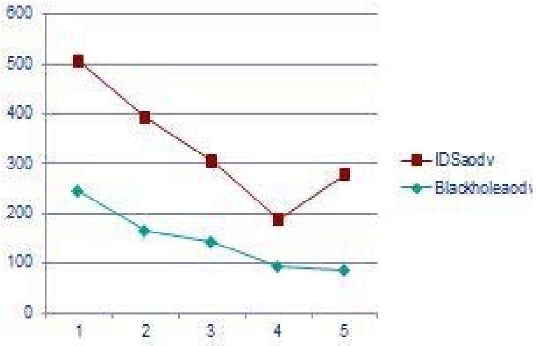
(2)ROUTING LOAD:



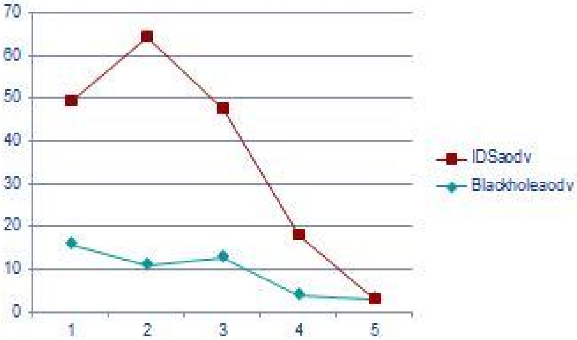
(3)END TO END DELAY:



(4) THROUGHPUT:



(5)DELEVERY RATE:



VII.CONCLUSION & FUTURE WORK:

In this Paper we show that trust system on top of AODV has an advantage over schemes that rely only on first-hand observations despite the limited amount of information and the additional problems of AOMDV.

Our PAPER focuses mainly on black hole attack but can handle also other misbehavior patterns like which drops packets. It can be improved to drastically changing policy, in order to handle the packets (like considering only data packets when control packets are forwarded well). Additional mechanisms to work in the field of QoS (quality of service) and to increase the fairness in the network are possible areas for future research. Our work is dedicated to AOMDV based IDS scheme and security of mobile ad-hoc network, but can be adopted to other routing algorithms as well as to mobile ad-hoc network.

VIII.REFERENCES:

❖ [1].X. Li Z. Jia P. Zhang-basedR.Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 4, April 2012) September 2002

❖ (2)Mohammed ERRITALI, Bouabid El Ouahidi, "***A Review and Classification of Various V ANET Intrusion Detection Systems***," Computer Communication at © IEEE2013

❖ (3) Debarati Roy Chaudhari, Dr.Leena Ragha, "***Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack",*** © Science Direct 2015.

❖ (4)S. Murthy, C. Siva Ram, and B. S. Manoj, Ad Hoc Wireless Networks :Architectures and Protocols, Prentice Hall, Chapter 7, 2004.

❖ (5) Y.F.Alem, Z.C.Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May,2010