Simulation and Performance Evaluation of AODV protocol against Blackhole Attacks in MANET

Khushbu Patel, Prayag Patel

***Abstract*— A mobile ad-hoc network (MANET) is an autonomous wireless network which consists of mobile nodes that communicate with each other over multi-hop wireless links. Due to the absence of any fixed infrastructure, MANETs are unprotected to various types of security attacks. Black hole is one of these attacks. Black hole is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node. There are lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. Here, a mechanism is proposed for the nodes which are deployed in MANETs in order to detect and prevent black hole attacks. We simulated the black hole attack in various wireless ad-hoc network scenarios and have tried to find a response system in simulations. The analysis guides us to the various performance parameters such as throughput, packet delivery ratio, and number of dropped packets evaluated over different scenarios**

***Index Terms*— MANET (Mobile ad hoc network), AODV(On-demand distance vector routing protocol),Blackhole Attack, IDS(Intrusion detection system**

I. INTRODUCTION

A Mobile ad hoc network is a collection of wireless nodes that can be dynamically set up ANYWHERE and ANYTIME, without using any pre-existing network infrastructure. There are no basic network devices, such as routers or access points to transfer data among nodes. Instead, each node acts as a router to establish a route and transfer data by means of multiple hops. Due to the mobility nature of nodes, the network topology changes rapidly and erratically over time. MANETs have many potential applications, like Sensor Networks, Medical Service, Personal Area Network, especially in military and rescue operations such as connecting soldiers in the battlefield or creating a temporary network in place of one, which collapsed after a disaster like tsunami [2]. Routing in ad-networks has been a challenging task ever since the wireless networks came into existence. The major reason for this is the constant change in network topology because of high degree of node mobility [1].

The available routing protocols are mainly categorized into proactive routing protocols, reactive routing protocols and hybrid routing protocol. In proactive routing protocols, the routing information of nodes is exchanged, sporadically, such as DSDV. In reactive routing protocols, nodes exchange routing information when it is needed such as AODV and DSR. Some ad-hoc routing protocols are a combination of the above two categories which we called as hybrid routing protocols. The primary goal of such an ad hoc network routing protocols are correct and efficient route establishment between a pair of nodes[3].

Due to the unique characteristics of MANET, There is no centralized gateway device to monitor the network traffic. Since the medium is open, both legitimate and malicious nodes can access it. Moreover, there is no clear separation between normal and unusual activities in a mobile environment. Since nodes can move arbitrarily, false routing information can come from a compromised node or a legitimate node that has outdated information[4].

The network layer in MANETs is susceptible to variousattacks viz. eavesdropping with a malicious intent, spoofing the control and/or data packets transacted, malicious modification/alteration of the packet contents and the Denial-of-service (DoS) attacks -Wormhole attacks, Sinkhole attacks, Blackhole attacks[5]. Here, a mechanism is proposed for the nodes which are deployed in MANETs in order to detect and prevent black hole attacks.

The rest of the paper is organized as follows: In Section 2, we briefly describe the working of the AODV routing protocol, In section 3, we discuss survey of the related work in the area, In section 4, we discuss the proposed solution, In Section 5, we describe the simulation environment, In Section 6, we describe the simulation results and analysis. Finally, we conclude in Section 7 with future scope.

II. THEORETICAL BACKGROUND

A. Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol

Ad-hoc On-Demand Distance Vector (AODV) [6] Routing Protocol is used for finding a path to the destination in an

Manuscript received May 06, 2014.

Khushbu Patel, Department of Computer Science Engineering Department, S.P.B.Patel Engineering College,Gujarat, India.

Prayag Patel, Department of Computer Science Engineering Department, S.P.B.Patel Engineering College,Gujarat, India.

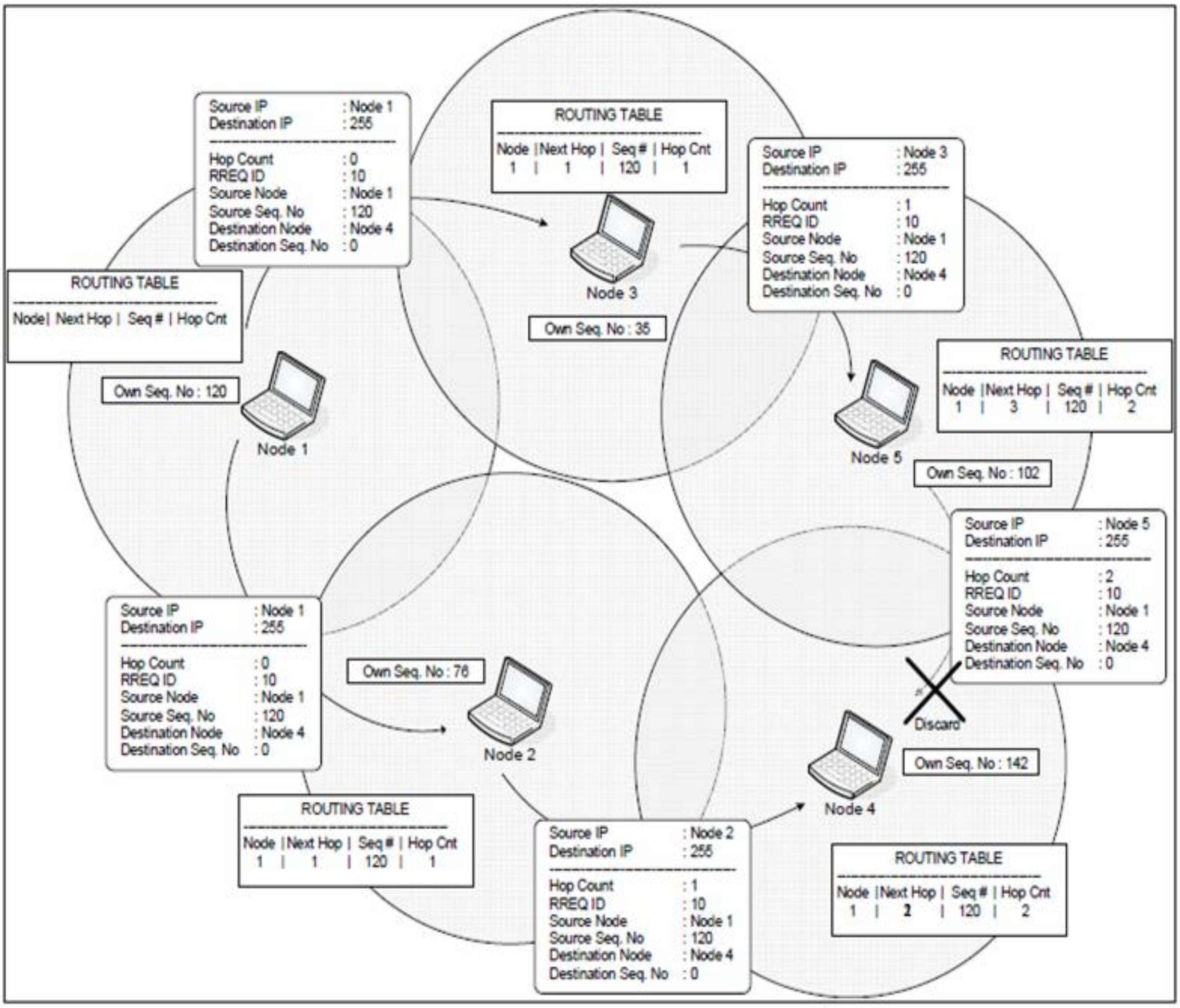
ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated

by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path.

Route Requests (RREQs), Route Replay (RREPs), Route Errors (RERRs) are control messages used for establishing a path to the destination, When the source node wants to make a connection with the destination node, it broadcasts an RREQ message. This RREQ message is propagated from the source, received by neighbors (intermediate nodes) of the source node. The intermediate nodes broadcast the RREQ message to their neighbors. This process goes on until the packet is received by destination node or an intermediate node that has a fresh enough route entry for the destination. Figure 1 shows how the RREQ message is propagated in an ad-hoc network.

Fresh enough means that the intermediate node has a valid route to destination formed a period of time ago, lower than the threshold. While the RREQ packet travels through the network, every intermediate node increases the hop count by one. If an RREQ message with the same RREQ ID is received, the node silently discards the newly received RREQs, controlling the ID field of the RREQ message. When the destination node or intermediate node that has fresh enough route to the destination receive the RREQ message they create an RREP message and update their routing tables with accumulated hop count and the sequence number of the destination node.

Afterwards the RREP message is unicasted to the source node. The difference between the broadcasting an RREQ and unicasting RREP can be seen from Figures 1 and 2. While the RREQ and the RREP messages are forwarded by intermediate nodes, intermediate nodes update their routing tables and save this route entry for 3 seconds, which is the ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol. Thus the node knows over which neighbor to reach at the destination. Figure 2 shows how the RREP message is unicasted and how the route entries in the intermediate nodes are updated.



Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

Source IP : Node 3
Destination IP : 255
Hop Count : 1
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	3	120	2

Source IP : Node 5
Destination IP : 255
Hop Count : 2
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

Source IP : Node 2
Destination IP : 255
Hop Count : 1
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	2	120	2

Fig.1 – Propagation of the RREQ message

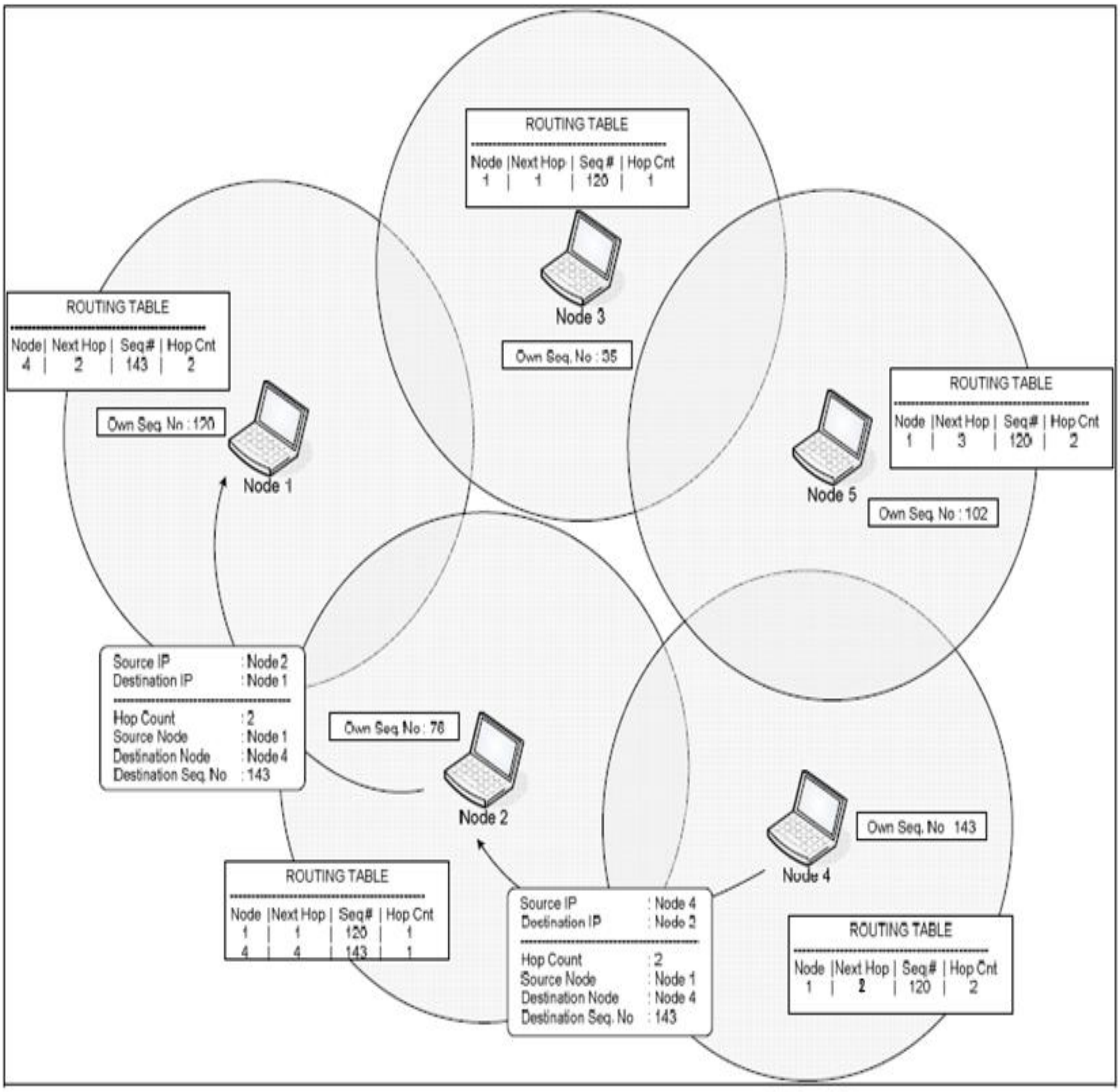


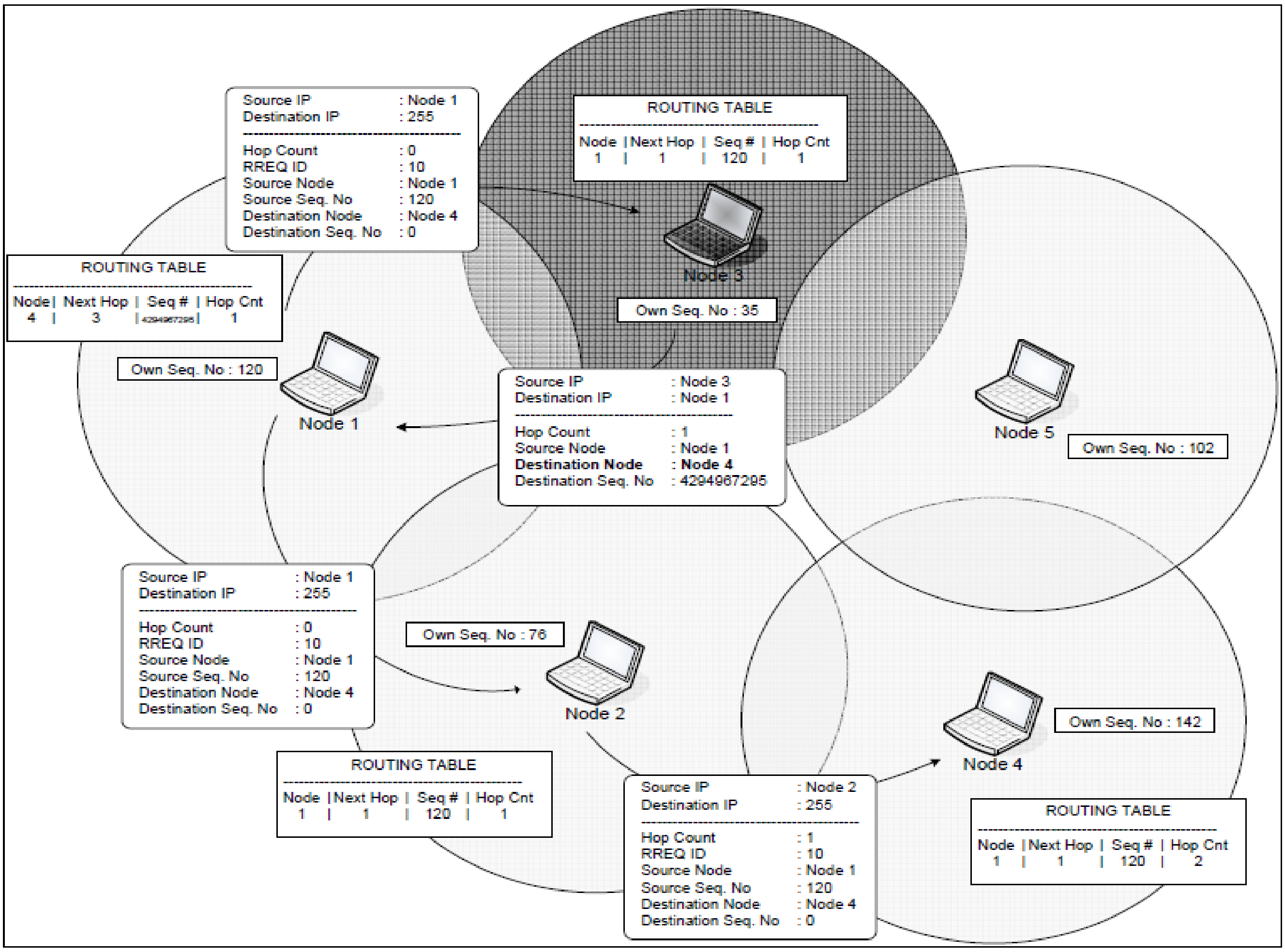
Fig.2 – Unicasting the RREP message

B. *Sequence Numbers*

Sequence Numbers serve as time stamps and allow nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message, RREQ, RREP, RERR etc., it increases its own sequence number. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is considered and route is established over this node by the other nodes. The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). If the sequence number of the node reaches the possible highest sequence number, 4294967295, then it will be reset to zero (0). If the results of subtraction of the currently stored sequence number in a node and the sequence number of incoming AODV route control message is less than zero, the stored sequence number is changed with the sequence number of the incoming control message.

C. *Black Hole Attack*

Black Hole Attack is briefly explained in the previous Chapter. In this Chapter we shall explain it in more detail as we have already explained the AODV protocol.



Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
4	3	4294967295	1

Source IP : Node 3
Destination IP : Node 1
Hop Count : 1
Source Node : Node 1
Destination Node : Node 4
Destination Seq. No : 4294967295

Source IP : Node 1
Destination IP : 255
Hop Count : 0
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	1

Source IP : Node 2
Destination IP : 255
Hop Count : 1
RREQ ID : 10
Source Node : Node 1
Source Seq. No : 120
Destination Node : Node 4
Destination Seq. No : 0

ROUTING TABLE

Node	Next Hop	Seq #	Hop Cnt
1	1	120	2

Fig. 3 – Illustration of Black Hole Attack

In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behavior in the scenario of the figures of the previous section.

In this scenario shown in Figure 3, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets.

III. Related Work

In this section, we will review the several solutions to black hole attacks.

In[7] solution the source node stores all the RREPs in the table called Cmg_RREP_Tab until receiving first RREP packet waits for MOS_WAIT_TIME. Meanwhile, the source node analyses all the stored RREPs from Cmg_RREP_Tab table, and discard the RREPs having a very high destination sequence number. Every node in the network maintains a table called Mali_node for storing the malicious node details to isolate the malicious node in the network. Moreover, in order to maintain freshness, the Cmg_RREP_Tab is flushed once an RREP is chosen from it. However, this solution fails to detect co-operative black hole attack and it has high processing delay.

In [8] authors proposed have proposed the method DPRAODV (A dynamic learning system against black hole attack in AODV based MANET) to prevent security of black hole by informing other nodes in the network. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends ALARM packet to its neighbours. The routing table for that malicious node is not updated, nor is the packet forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The main advantage of this protocol is that the source node announces the black hole to its neighbours in order to be ignored and eliminated .An overhead of updating threshold value at every time interval along with the generation of ALARM packet will considerably increase the routing overhead. This method is not support cooperative black hole nodes.

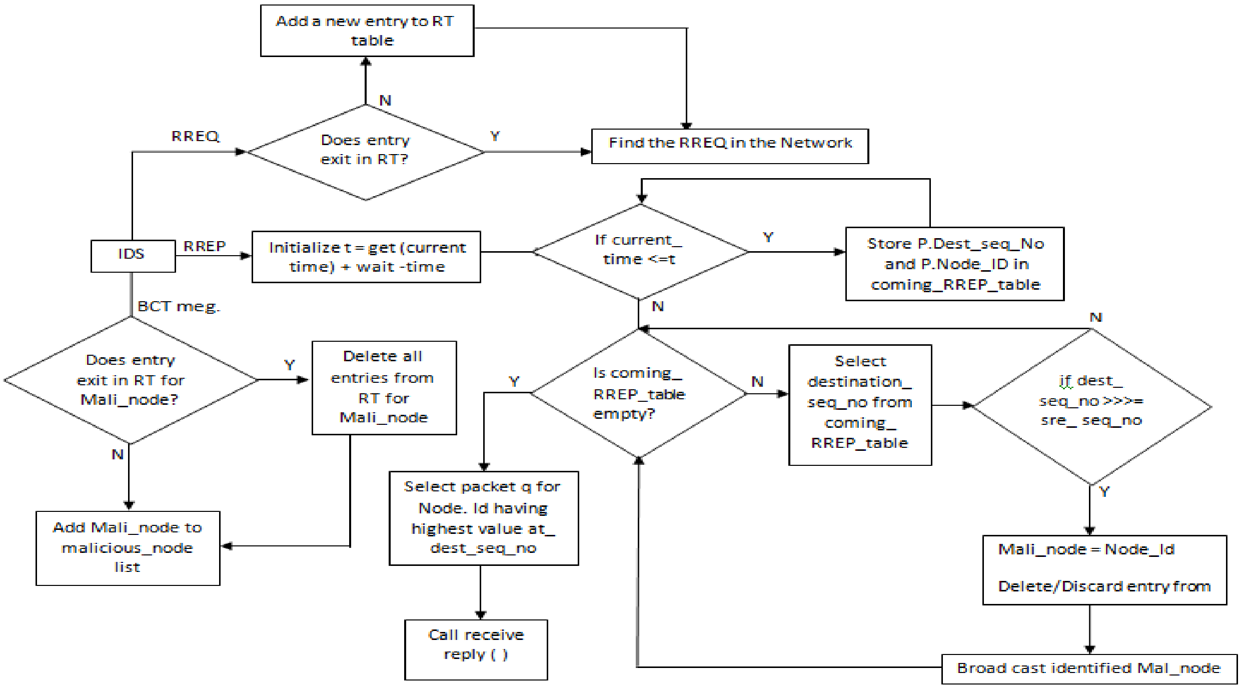
In [9] Authors Ming-Yang Su et.al discussed a mechanism, called an ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds a threshold level, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the malicious nodes on their blacklists to isolate the malicious node in the network cooperatively. The advantage of this method is that it can be able to detect cooperative black hole nodes in the MANETs. The main drawback of this technique is that mobile nodes have to maintain an extra database for training data and its updations, in addition to the maintenance of their routing table.

In [10], the authors discuss a protocol that requires the intermediate nodes to send RREP message along with the next hop information. When the source node get this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a FurtherRequest, it sends a FurtherReply which includes the check result to the source node. Based on information in FurtherReply, the source node judges the validity of the route.

IV. Proposed Solution

The solution that we propose here is designed to detect and prevent any alterations in the default operations of either the intermediate nodes or that of the destination nodes. The approach we follow, basically only modifies the working of the source node, using an additional function RREP. Apart from this, we also added a new table Coming_RREP_Tab, a timer WAIT_TIME and a variable Mali_node list to the data structures in the default AODV protocol, as explained further. In the original AODV protocol, by default, the source node accepts the first fresh enough RREP request coming to it. As compared, in our approach, we store all the RREPs in the newly created table viz. Coming_RREP_Tab until the time, WAIT_TIME.. In our solution, the source node after receiving first RREP control message waits for WAIT_TIME. For this time, the source node will save all the coming RREP control messages in Coming_RREP_Tab table. Subsequently, the source node analyses all the stored RREPs from Cmg_RREP_Tab table, and discard the RREP having presumably very high destination sequence number. As before, the node that sent this RREP is suspected to be the malicious node list. Once, such malicious node is identified, our solution selects a reply having highest destination sequence number from Coming_RREP_Tab table and Broadcast identified MN in the network. when node broadcast identified MN in network then this after receiving BCT message each node check entrey exit in its RT for MN. If exist Then delete all entries from RT for MN.if not exist then add MN to malicious_node list. The proposed solution maintains the identity of the malicious node as Mali_node, so that in future, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table for that node is not maintained. In addition, the control messages from the malicious node, too, are not forwarded in the network.

The proposed algorithm will work at Source Node as per following steps:


Add a new entry to RT table
N
RREQ
Does entry exit in RT?
Y
Find the RREQ in the Network
IDS
RREP
Initialize t = get (current time) + wait -time
If current_ time <=t
Y
Store P.Dest_seq_No and P.Node_ID in coming_RREP_table
N
BCT meg.
N
Does entry exit in RT for Mali_node?
Y
Delete all entries from RT for Mali_node
Y
Is coming_ RREP_table empty?
N
Select destination_ seq_no from coming_ RREP_table
if dest_ seq_no >>>= sre_ seq_no
N
Y
Add Mali_node to malicious_node list
Select packet q for Node. Id having highest value at_ dest_seq_no
Mali_node = Node_Id
Delete/Discard entry from
Call receive reply ( )
Broad cast identified Mal_node

Insrution Detection System

V. Simulation Environment

A. Simulation Tool

In this paper the simulation tool used for analysis is NS-2 which is highly preffered by research communities. NS is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing,and multicast protocols over wired and wireless (local and satellite) networks [1]. NS2 is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. This means that most of the simulation scripts are created in Tcl(Tool Command Language). If the components have to be developed for ns2, then both tcl and C++ have to be used.

B.Simulation Parameters

We have implemented Black hole attack in an ns2 simulator. CBR (Constant Bit Rate) application has been implemented. The problem is investigated by means of collecting data, experiments and simulation which gives some results, these results are analyzed and decisions are made on their basis. The simulator which is used for simulation is ns2. To evaluate the performance of a protocol for an ad hoc network, it is necessary to analyze it under practical conditions, especially including the movement of mobile nodes. Table 1 shows the parameters that have been used in performing simulation.

Table 1 :Simulation Parameters

Parameters	Value
Simulator	NS-2.34
Data Packet Size	512 byte
Simulation Time	500 sec
Environment Size	700×700 m
No of nodes	20
Observation Parameter	PDR,Throughput,Dropped Packets
No. of Malicious node	1
Traffic type	VBR
Routing Protocol	AODV
Mobility	20 m/s

C.Performance Metrics

Performance Metrics are quantitative measures that can be used to evaluate any MANET routing protocol. The metrics that compare the performance of normal AODV and AODV under blackhole attack are as follows:

Throughput represents the amount of data received by the destination nodes in some period of time.it is the measure of how fast a node can actually sent the data through a network.so throughput is the average rate of Successful message delivery over a communication channel.

$$\text{Average Throughput} = \frac{\text{Number of Bytes Received} \times 8}{\text{Simulation Time} \times 1000}\ \text{Kbps}$$

Packet delivery ratio (PDR) can be measured as the ratio of the data packets delivered to the destinations to those generated by the CBR sources. The PDR depicts how well a routing protocol can delivers packets from source to destination. The higher values give better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness .

$$\text{PDR (\%)} = \frac{\text{Number of Packets Received}}{\text{Number of Packets Sent}} \times 100$$

Dropped Packets refer to the number of packets sent by the source node that failed to reach the destination node. The routers might fail to deliver or drop some data packets after their arrival when their buffers are already full.

$$\text{Dropped Packet} = \text{Sent Packets} - \text{Received Packets}$$

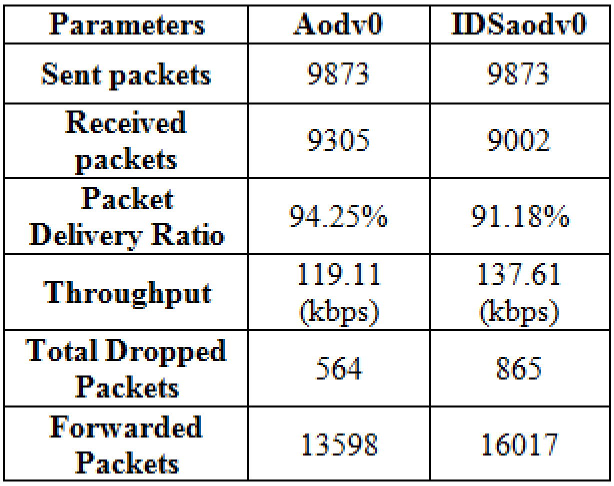
Packet forwarding is the relaying of packets from one network segment to another by nodes in a computer network.

VI. Simulation Results

Table 2: Performance parameter without Blackhole Attack

Parameters	Aodv1	IDSaodv1
Sent packets	9873	9873
Received packets	451	3060
Packet Delivery Ratio	4.57%	30.99%
Throughput	184.66 (kbps)	165.32 (kbps)
Total Dropped Packets	9422	6817
Forwarded Packets	11919	12731

Table 3: Performance parameter with Blackhole Attack



Parameters	Aodv0	IDSaodv0
Sent packets	9873	9873
Received packets	9305	9002
Packet Delivery Ratio	94.25%	91.18%
Throughput	119.11 (kbps)	137.61 (kbps)
Total Dropped Packets	564	865
Forwarded Packets	13598	16017

A.Simulation Results

Here Aodv0 indicate without Black Hole Scenario means Normal AODV whereas IDSaodv0 for without Black Hole Scenario with ids Aodv1 indicate one node Black Hole Node AODV IDSaodv1 node Black Hole Node with ids.

B.simulation graph

Packet Delivery Ratio comparison

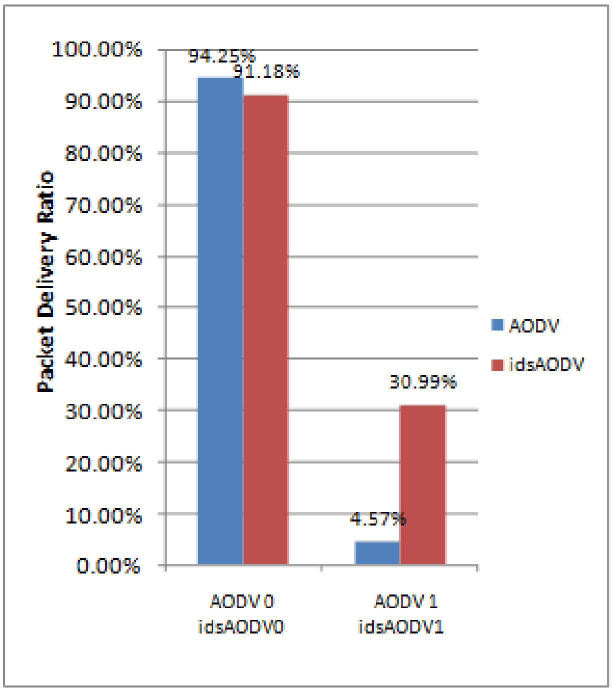


Fig. 5 :Impact of Blackhole Attack on the Packet Delivery Ratio

For without Black Hole Scenario (Normal AODV) the Packet Delivery Ratio is 94.25%. For IDSAODV Scenario without blackhole node the Packet Delivery Ratio is 91.25%.For with one Node Black Hole Scenario the Packet Delivery Ratio is almost 4.57%.For IDSAODV Scenario with one blackhole node the Packet Delivery Ratio is improved between 30.99%.

Throughput comparison

For without Black Hole Scenario (Normal AODV) the throughput is 119.11kbps. For IDSAODV Scenario without blackhole node the throughput is increase to 137.61kbps.For with one Node Black Hole Scenario the throughput is almost 184.66 kbps.For IDSAODV Scenario with one blackhole node the throughput is 65.32 kbps.

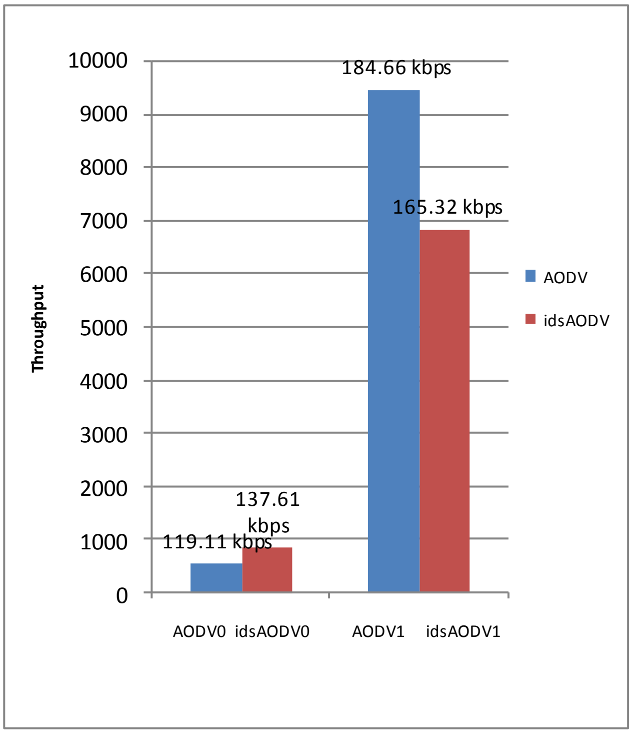


Fig 7: Impact of Blackhole Attack on the Throughput

For without Black Hole Scenario (Normal AODV) the Dropped packets are 564 from sent packets of 9873 . For IDSAODV Scenario without blackhole node Dropped packets are increase to 865 because of more security.For with one node black hole Scenario Dropped packets are 9422.For IDSAODV Scenario with one blackhole node the Dropped packets are decrease to 6817.

VII. CONCLUSION AND FUTURE WORK

Here, We have proposed & implemented a black hole detection mechanism to detect and prevent black hole attacks. In proposed method not only blackhole nodes are prevented but also they are detected. Also the information of detected nodes are broadcasted to all other nodes to delete the entries of detected blackhole nodes from their routing table. The nodes who receives a broadcast message of detected blackhole nodes, are adding these blackhole nodes in the detected blackhole list so that all future communications can be avoided. For this we implemented an AODV protocol that behaves as Black Hole in NS2.

Dropped Packets comparison

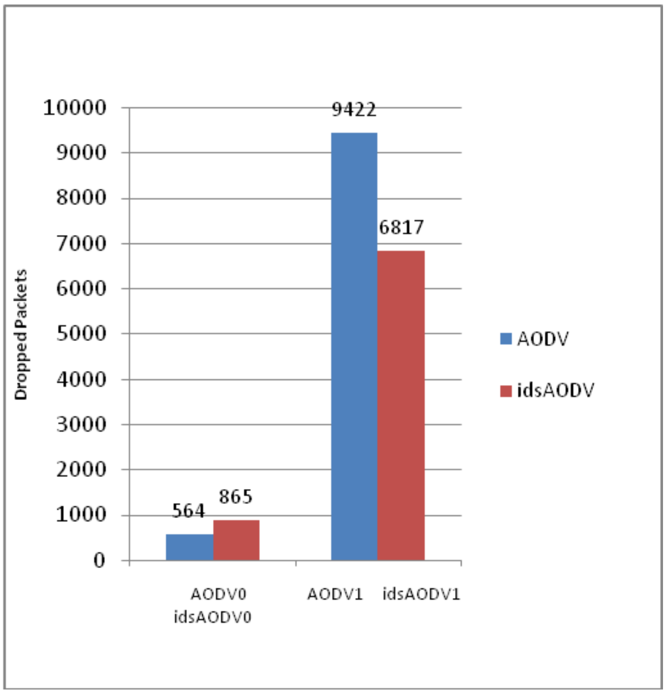


Fig 7:Impact of Blackhole Attack on the Dropped Packets

Having simulated the black hole attack , we saw that the packet loss is increased in ad-hoc network. Therefore to minimize the black hole effect, we implemented IDSAODV protocol .The IDSAODV protocol will improve the packet delivery ratio and minimize the data loss. The advantage of this approach is the implemented protocol does not make any modification in packet format hence can work together with AODV protocol. Another advantage is that the proposed IDSAODV does not require any additional overhead and require minimum modification in AODV protocol . For Future Work the proposed strategy is tested be carried for more than one black hole nodes, for various CBR traffic models, As part of our future endeavor, we aim to study the impact of varying pause time on the protocol.

REFERENCES

[1] Kapang Lego "Comparative Study of Adhoc Routing Protocol AODV, DSR and DSDV in Mobile Adhoc NETwork", Indian Journal of Computer Science and Engineering Vol. 1 No. 4 364-371.

[2] Sheikh R. Singh Chande, M.; Kumar Mishra, D.;, "Security issues in MANET: A review," Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On , vol., no., pp.1-4, 6-8 Sept. 2010.

[3] Madhusudhananagakumar KS , G. Aghila, " A Survey on Black Hole Attacks on AODV Protocol in MANET", International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011

[4] Dr.S.Tamilarasan, Securing and Preventing AODV Routing Protocol from Black Hole Attack using Counter Algorithm, International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July – 2012.

[5] Rajesh J. Nagar, Kajal S. Patel " Securing AODV Protocol against BlackholeAttacks" nternational Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 1,Jan-Feb 2012, pp.1116-1120

[6] C.Perkins, "(RFC) Request for Comments – 3561", Category: Experimental,Network, Working Group, July 2003.

[7] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.

[8] Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Bodv Based Manet." In: International Journal of Computer Science Issues, Vol.2, pp 54-59, 2009.

[9] Ming-Yang Su "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", Department of Computer Science and Information Engineering, Ming Chuan University Computer Communications 34 (2011) 107–117.

[10] H. Deng, W. Li, and D. P. Agrawal. "Routing Security in Adhoc Networks." In: IEEE Communications Magazine, Vol. 40, No. 10, pp.70-75, Oct. 2002.