Alleviate The Black Hole Attack By Adaption In Aodv Routing In MANETs

Divya Singh[1], Suman Pandey[2]

[1]Asst. Prof., Kashi Institute of Technology, [2]Associate Professor, K.N.I.T. Sultanpur

Abstract— In Wireless ad-hoc network, the infrastructure of MANETs differs in variety of applications due to the change in topology, caused by mobility of nodes. In MANETs secured routing is a critical issue as nodes falling on established path are mobile. There are various types of security attacks breaking the functonality of MANETs. The AODV is most popular routing protocol which suit to deployment of MANET. The Black Hole Attack is one of severe attacks which malign the functionality of AODV route. In the process malicious node attacks to the source node as it works for discovering and maintaning fresh and nearest path to destination. In this work, the prime focus is to defeat the Black Hole Attack. In our work we have modified AODV routing protocol capturing all the possibility of attacks and fort the path between source and destination nodes using best possible effort (heuristic). The proposed algorithm was simulated over very popular tool ns-2.35 and met the objective

Index Terms— MANET, Mobile Adhoc Networks, Routing Protocols, Security Threats, Algorithm,, Adhoc, Black Hole Attack, Black Hole Solution (BHS).

I. INTRODUCTION

Wireless networks are easily scalable as needing no physical connection between the nodes and supporting dynamic topology. The mobile nodes belonging to same radio range communicate directly with each other. The communication between nodes out of their radio ranges requires the cooperation of other nodes and such communication is called multihop. Therefore, each node behaves both as a host and a router simultaneously. The wireless network has two operational modes following IEEE 802.11 standard. In one mode it requires infrastructures to work with and the other operate without support of any infrastructure and known as adhoc network.

In infrastructure network, the nodes are connected to existing wired network with the help of wireless router and this network operates in centralized way whereas in its adhoc version the nodes as wireless clients are connected in a peer to peer manner. Thus in adhoc mode nodes forward message to each other and manage communication between the nodes. One very advantageous point is its easy setup in any environment.

With number of advantages over the traditional wired network the wireless network suffers in providing efficient routing as nodes are mobile and lacks stable routing. Routes are too frequently changed so managing a secure and efficinet path for a session (transmission) is very important and critical task. The application horizon of mobile adhoc network is day by day widening. So it demands for secure and efficient way of routing. There are several proposals in research for routing protocol in MANETs but threating on its security and must be combat.

The adhoc on demand distance vector routing (AODV) protocol is the most widely used.

In this paper our work is to combat the foreign malicious attack possibly made on AODV protocol. The basic themet behind the right path is to search for shortest and freshest route. To supplement the aim the AODV protocol come through various type of bad intentional attack in its route discovery mechanism.

There are various types of malicious attack and one of these attacks is known as Black Hole Attack which is a severe attack that degrades the performance of AODV protocol. The black hole attacks are categorized into following:

- Single black hole attack
- Multiple black hole attack
- Co-operative black hole attack

In this work we propose a reliable route discovery mechanism that defeats the purpose of malicious attack on AODV routing in MANETs.

The rest of the paper is sectined as follows. Section 2 reviews security attacks in the MANET. The Section 3 describes AODV protocol and discusses ist various security issues. In section 4, we propose a methodology of preventing black hole attacks on the AODV protocol. The simulation and the analysis are presented in section 5. Finally, it is concluded with some mention for future which goes in section 6.

II. SECURITY ATTACKS AND RELATED WORK

With everincresing usability of MANET its security has now become a primary concern. The characteristics of

MANETs pose both challenges and opportunities in achieving security goals. We briefly outline some of the relevant issues of various proposed routing protocols in MANET.

The Authenticated Routing for Adhoc Networks (ARAN) [7] detects and protects against malicious actions carried out in routing process by the third parties and peers in the ad-hoc environment. ARAN supports authentication and nonrepudiation services in Adhoc working environment. During the routing when a node generates a routing message, it must also be signed and every intermediate node verifies the signatures of the source and the previous node, removes the latter, and signs the original message.

The Security-Aware ad-hoc Routing (SAR) [8] introduces the idea of trust level ensemble of the metrics in path finding. Nodes are affiliated with security levels and every level owns a different key. Only nodes that share a level key can process and forward messages in a specific level.

ARIADNE [9] is an on-demand secure ad-hoc routing protocol that withstands node compromise and relies only on highly efficient symmetric cryptography. ARIADNE guarantees that the target node of a route discovery process can authenticate the initiator, that the initiator can authenticate each intermediate node on the path to the destination present in the node list in the RREQ or RREP messages.

III. OVERVIEW OF AODV PROTOCOL

Over an adhoc network, when a node (sender) has data for the other node (destination) then sender discovers a route and transmits the data then and this type of routing strategy is known as on demand or a reactive routing protocol. In adhoc network each mobile node operates as a distinguished router and routes are created as needed with little or no reliance on periodic advertisements and exchanges of messages. Our proposed routing algorithm is quite suitable for a dynamic self starting network as required by adhoc networks as AODV provides loop free routes even repairing broken links and managing route during the transmission of whole data. This protocol does not require global periodic routing advertisements so needs lesser bandwidth in comparison to those protocols that do necessitate such advertisements.The AODV operates in two phase (1) the route discovery processs and (2) route maintenance process.

In route discovery phase uses Route Request (RREQs) and Route Reply (RREPs) control messages. These routing messages keep information of sender and destination. In creation of a route to destination, the sender broadcasts a route request (RREQ) packet to find the optimum pathway. The RREQ message keeps route request broadcast ID, Destination IP Address, Destination Sequence Number, Source IP Address, Source Sequence Number and Hop Count. The Sequence number is utilized to check for fresh routes, free from loop and faster convergence. In case a node sends any control message like RREQ or RREP, it increases its own sequence number by a fix number such as 1 or 2. Every node keeps the latest sequence number in its routing table. It is updated upon reception of RREQ, RREP or RRER related to a specific node. Hop count shows the distance in hops from sender to destination. Each node upon receiving the RREQ message creates a reverse path back to the sender RREP message can be unicast to that sender node from the destination or any intermediate node that satisfy the request conditions. Upon receiving the route request message, the intermediate node forwards the RREQ message until a node is found that is the destination itself or it has an active route to the destination with destination sequence number greater than or equal to that of RREQ. This node replies back to the source node with a route reply message RREP and discards the RREQ. If the intermediate node receives RREQ with 'G' flag set, it must also unicast gratuitous RREP to the destination node. RREP contains Destination IP Address, Destination Sequence Number, Originator IP Address and Lifetime. Forward links are setup when RREP travels along the reverse path. Once the source node receives the route reply, it establishes a route to the destination and sends data packet along forward path set-up. Route maintenance is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbors about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. When a node does not receive HELLO message within time period from a neighbor node then it detects that a link to that neighbor node has broken then it generates route error message (RERR). RRER message indicates those destinations that are unreachable, their IP address and destination sequence number. In order to inform the link failure information, each node maintains a precursor list for each entry containing the IP address of set of neighboring nodes, likely to use it as a next hop towards each destination in routing table. On receiving this RRER, each predecessor node, in turn, forwards the RERR to its own set of predecessors, thus deleting all paths using this nonactive link. In addition to these routing messages, the route reply acknowledgment (RREP-ACK) message is sent by sender node of RREQ in response to a RREP message.

The route discovery process in AODV is illustrated in Fig.1. Each node decides the freshness of control message by sequence numbers (higher or not). In Fig.1 node S is wants to create a path to destination D. In first phase, the source node S refers to the route map in its routing table.

If there is no entry for this destination node D, then it broadcast an RREQ message. The RREQ ID is increased by one each time node S sends an RREQ. The nodes A and B, which have received the RREQ, generate and renew the routes to their previous hops. They also determine if this is a repeated RREQ. If such an RREQ is received, it will be discarded. If A and B have a valid route to the destination D, they send an RREP message to node S. On the other hand, if there is no valid route, they also broadcast further this RREQ message. Thisway, exchange of route information will be repeated until an RREQ reaches node C which has the path for node D. When node C receives the RREQ, it replies back by unicasting RREP to node S. When node S receives the RREP, a route is established. In case of receiving multiple RREPs, the RREP with the highest destination sequence number (D_Seq) is chosen by the source node. If sequence numbers are identical, then it will select the RREP with the lowest hop count i.e of minimum distance.

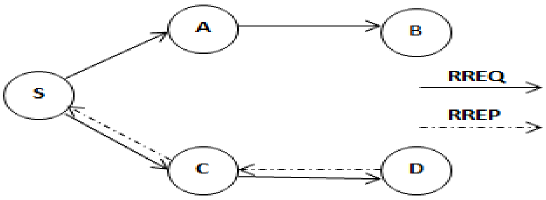

Fig.1 Route discovery process

The route maintenance phase is shown in Fig. 2. When node C detects a disconnection with D, it generates a Route Error (RERR) message, enters the address of node D into the list of invalid nodes, and sends this information to node S. When node S receives the RERR, then a route map and the recent list of RERR is send by the S to the A. If A contains any route through neighboring node B in which B as a next hop including in its map, it invalidates the route and sends an RERR message to node B. By this methodology the RERR message received by all nodes of the network..

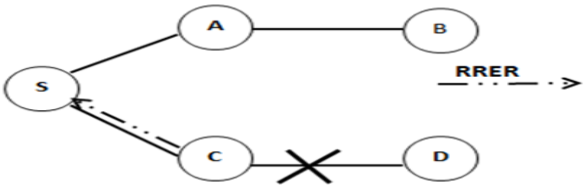

Fig. 2 Transferring route error messages

3.1 Security Issues in AODV

In this section we have considered various security issues od AODV protocol.

Impersonation or Spoofing- The circumstance of this challenge is to deceive the trustworthy impartiality of the attacker. In this challenge, the quibbler assumes the identity of a in a superior way trusted node in the network. By doing this the disparate nodes augment this callous node in their routing angle and the hard node can before disrupt the both oars in water functioning of the incorporate without as noticed.

Black-hole Attack- The final cause of this protects is to pick up the traffic jam in network. In this take up the gauntlet the callous node does not advanced any packets forwarded to it, or not exactly drops them all. Due to this clash the packets forwarded all nodes do not do their coming finish line and the heavy traffic in the incorporate escalates discipline to retransmissions.

Sink-hole Attack- The kernel of the doubter in this resist is to focus generally told the absorb barter towards itself. The caviler executes this take up the gauntlet by making the convenient nodes jump to a conclusion that the shortest that a way to the goal is on it. This protect whys and wherefores the desparate nodes to communicate all the intercourse over the low down and dirty node in case the doubter can fix, caricature or comparatively listen to the approved packets.

Wormhole Attack- The main fire in the belly of the wormhole clash is to replay the mint on the at variance side of the network. This challenge is full by two nodes colluding to consist of a wormhole. The attacker on a well known side ratiocinate the nodes speculate that transcend to the goal is practically such bump, when it is in a superior way than such hop. This causes the hyper critic to gather all the traffic from one side of the join and relay it on the wormhole; the quibbler on the distinctive side replays the cognate packet. By doing this the complainant can die the packets or derive any business illegally.

Sleep Deprivation- The function of the quibbler in this protects is to pull out of the fire the focus node invariably busy. This clash is called up by flooding consolidate by all of routing traffic and thereby making the node engage all of the computing and heavy stuff power. This take up the gauntlet forces the targeted node in consuming the force, network bandwidth and computing capacity by all off requests for up to the minute or non-existent destination nodes, in case it cannot practice the perfect requests

In this paper we have worked upon black hole attact and tried to prevent the AODV routing from such attack.

3.2 Description of a Black Hole Attack in AODV

In AODV, D_Seq is used to determine the freshness of the routing information that is contained in the control messages when generating an RREP message, a destination node compares its current sequence number with sequence number in the RREQ message and then selects the larger one. This sequence number is increased by one and is used as the D_Seq of the RREP. Upon receiving a number of RREPs, a source node selects the one with greatest D_Seq in order to construct a route.

In order to succeed at a black hole attack [8], the attacker must generate an RREP message with the shortest path and the highest D_Seq in the network to impersonate the destination. It is possible for the attacker to include this forged information in the RREP message. It is very important for the source nodes to test the data ensure that it contains the shortest path and the highest D_seq when sending the data to the source node as a Route Reply RREP. In the Fig. 3 (shown below) illustrates a typical scenario for protocol packet exchanges. It depicts the generation and transmission of RREQ and RREP control messages. Here, we assume that the destination node (Node4) has no connections with other nodes.

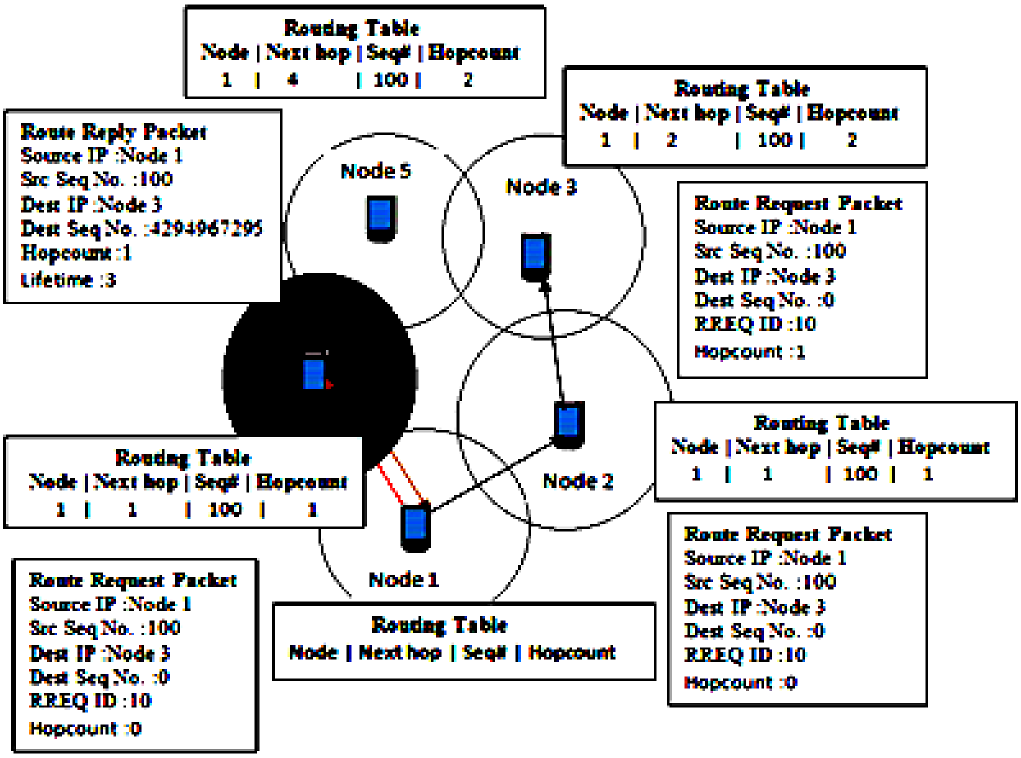

Fig. 3 Illustration of a black hole attack

The source node (Node 1) constructs a route in order to communicate with destination node (Node 4). Thus, as explained earlier, Node1 would generate an RREQ as shown in Table 1. All the neighbor nodes receive RREQ message to pass the information to the destination node (Node 4) that is broadcasted by source node (Node 1) Upon receiving the RREQ, Node 2 generates this control message by updating its routing table with the accumulated Hop_Count + 1 and adopting the sequence number. Node2 forwards the RREQ since it is not the destination node. This packet will reach the destination node (Node 3).

Before generating the RREP message, Node 4 checks the Seq in the RREQ and compares it with the Seq in its routing table. It will choose the higher Seq and increment it by one, and use this value as the D_Seq in RREP message that it transmits. The S_Addr and D_Addr are copied from the RREQ massage and the Hop_Count will be updated to zero.

Table 1 Routing Request (RREQ)

Field Name	Value
Hop Count	0
RREQ ID	10
Source Node	Node 1
Source Seq No.	100
Destination Node	Node 3
Destination Seq No.	0

Therefore, the RREP message can be unicast to the source node by reverse path. The following Table 2 shows the values of the RREP message.

Table 2 Routing Reply (RREP)

Field Name	Value
Hop Count	0
Source Node	Node 1
Destination Node	Node 3
Destination Seq No	140

Node 3 is a malicious node on the network. When it receives the RREQ message, it replies immediately to the source node (Node1) with its RREP message without following the routing protocol.

Table 3 Blackhole Routing Reply

Field Name	Value
Hop Count	1
Source Node	Node 1
Destination Node	Node 3
Destination Seq No.	4294967295

The black hole's RREP message includes S_Addr and D_Addr values that are copied from the RREQ message, the lowest Hop_Count (shortest path), and the highest D_Seq value. Table III shows the values for a black hole RREP message.

As a result, two RREP messages are received by source node (Node1).Based on the shortest path and highest D_Seq values that are contained in the RREP message from the malicious node (Node 4), it decides that the RREP from Node 4 contains the most recent routing information and the route to Node 4 is established. As a result, the traffic from the source node to destination node is deprived by the malicious node. In order to deceive AODV and trigger a black hole attack, the attacker forges the values in the following two fields of the RREP message and sends the RREP to the source node:

1. Highest destination sequence number (fresh route)

2. Lowest hop count number (shortest path)

In most cases, the black hole attack gains access to the route if the routing protocol does not protect itself. Black hole attacks do not follow the routing protocol rules and do not take a long time to reply. Therefore, black hole attackers reply more quickly than authentic destination nodes or other nodes in the network. The black hole attacker drops data packets that it receives from the source node after the route has been established. This leads, in turn, to network resource exhaustion.

The following describes the proposed mechanism to alleviate the black hole attack in AODV routing discovery process.

IV. BHS-AODV: PROPOSED MECHANISM TO SECURE ROUTE DISCOVERY TO PREVENT BLACK HOLE ATTACKS

In order to address the above described problem, we have proposed two mechanisms i.e. a Heuristic method for best possible effort to prevent black hole attacks in AODV routing scheme. This solution is a new methodology that involves modifications in route discovery phase of the standard MANET AODV protocol. This is known as Black Hole Solution for AODV-based MANET (BHS-AODV).

4.1 Defining Route Reply Cache

To implement the solution we changed the receive RREP function (recvReply) and create new RREP caching mechanism to count the second RREP message.The RREP chaching mechanism. “rrep_insert” function is for adding RREP messages, “rrep_lookup” function is for looking any RREP message up if it exists and “rrep_remove” function is for removing any record for RREP message that arrived from defined node and “rrep_purge” function is to delete periodically from the list if it has expired. We chose this expire time “BCAST_ID_SAVE” as 6 (means 3 seconds).

4.2 First Solution (BHS-1-AODV) for AODV-based MANET

In our proposed work we modify the AODV protocol to prevent black hole attack. The solution that we propose here, basically, modifies the working of AODV protocol by adding next hop information in the RREP message and two other control messages including further route request (FRREQ) and Further route reply (FRREP).Once the source receives RREP with next hop information it broadcasts Further RREQ message to next hop nodes to the received RREPs and then next hop nodes reply back with Further RREP message to source node. After receiving FRREP source node routes data packets to the destination with the shortest path. If the node is black hole node the next hop of its does not exists so it never receives FRREQ and not reply FRREP to the source node so source node never send data to path suggest by black hole node.

Algorithm of BHS1-AODV Mechanism

1. Source node broadcasts RREQ

2. Source node receives RREPs with next hop information from nodes

3. Source node fetch next hop information from RREPs received

4. Source node send further route request (FRREQ) to all next hop nodes

5. if (next hop node is of black hole) { FRREQ will not reach to next hop node and no FRREP will send to source } else { FRREQ will reach to all reliable next hop nodes and FRREP is send to source by these reliable next hop nodes }

6. Source node now receives FRREPs from reliable nodes; it will update its routing table

7. Source node routes data packets to the destination

4.3 Second Solution (BHS-2-AODV) for AODV-based MANET

For implementing another heuristic we used same RREP Cache as in previous solution and store the first rrep message in the rrep cache and wait for another rrep. After receiving another rrep the RecvReply function compare the sequence numbers of both rrep messages if the first sequence number is very much higher than the second sequence number then source node considers that higher sequence number node as a Black Hole node and remove that entry from rrep cache and its routing table simultaneously. Source node broadcast this message containing the information about black hole node to its neighbors. All neighboring nodes also remove all information about that particular node in their routing table and broadcast it further so that whole network may know about the malicious node. Following are the notations which have their meaning.

NOTATIONS

sn : source node ID

dst : destination node ID

in: intermediate node

r: route cache

rp: Reply Packet

saddr: sender node ID

rt: Routing Table

```
if (r == NULL){

rrep_insert (rp->rp_dst, rp->rp_dst_seqno, ih-> >saddr ());

}

Else {

If ((r->bhseq/rp->rp_dst_seqno)>1000000

i = 1;      rrep_remove(r->bdst);

printf ("The node %d is black hole node.\n", bh);}}

if (i == 1){    rt = rtable.rt_lookup(r->bdst);

rtable.rt_delete(r->bdst);     }
```

Fig. 4 BHS2-AODV Mechanism

Algorithm of BHS2-AODV Mechanism

1. sn broadcasts RREQ to all Nodes (i.e. neighbor of sn)

2. in receives RREQ and forwards if it has no route for the dst

3. in/dst gets Seq no. from RREQ and verifies with Seq no. in its routing table.

4. If Seq no. of RREQ is greater than Seq no. of its routing table

5. In/dst selects the seq no. of RREQ and include a new field in reply packet i.e. the ID of sender node

6. sn receive the RREP from in/dst

7. source node check If rrep cache is empty sn Insert the (destination node id, destination sequence number, intermediate node id) from the reply packet

Else If seq no of rrep cache is much greater than the seq no of rrep packet

8. Now sn broadcast a b HELLO packet which have black hole node id i.e. bh

9. All nodes update its routing table and delete all information about that particular node.

V. SIMULATION AND EVALUATION

We have used a standard Network Simulator 2 (NS2) tool for the simulation [9]. The NS2 is an event-driven simulator tool that is specifically designed to study the dynamic nature of wireless communication networks. We compared it with the standard AODV protocol under a black hole attack scenario on the network for evaluating the performance of the proposed method. We deployed a network with 15 nodes at random position and considered five different scenarios of each. Pause time was varied from 0 to 80s. Each node in the MANET was assigned an initial position within the simulation environment (500m * 500 m) and which joined the network at a random time. The packets were generated using CBR with a packet size 512 bytes. The Random Waypoint Model (RWP) was used as the mobility model for each of the nodes. In this model, each node chose a random destination within the simulation area and moved to this destination with a random velocity. The simulation parameters are presented in Table 4 as shown below.

Table 4 Simulation Parameters

Parameter	Value
NS-Version	2.35
Number of Nodes	15
MAC Protocol	IEEE 802.11
Traffic Type	CBR(UDP)
Data Rate(Mbps)	Random way point
Packet Size	512
Packet Interval	2.0 s
Packet Size	512 bytes
Number of malicious Node	1
Pause Time	10 s
Simulation Time	200

5.1 Performance Merices:

To analyse the impact of Black Hole Attack and its prevention the performance metrices such as packet loss, throughput and energy consumption were compared. These merices are defined as follows:

- Packet Loss

Packet loss is the number of the packets that are not successfully reached destination during transmission.[10] The lesser value of the packet loss means the better performance of the protocol.

- Throughput

It is defined as the total number of packets delivered over the total simulation time.

- Average Energy Consumption

This is defined as average energy consumed by a node in transmission of data from source node to destination node in the network

The data in Table 5 illustrates the impact of node mobility on the packet loss % where node mobility (mps) is the rate at which the nodes are moving in the network. The Packet loss for our proposed BHS-AODV mechanism indicates an improvement in performance of between 91% and 95% as compared to the standard AODV protocol.

Table 5 Packet Loss in Different Scinarios

Average values Packet Loss In Different Scenarios					
AODV	2.36	1.67	1.94	1.5	1.8
BHAODV	91.68	92.58	90.26	96.33	94.3
BHS1AODV	43.92	79.92	60.09	63.7	50.7
BHS2AODV	16.2	2.63	1.65	1.41	1.96

The following Fig. 5 shows the comparative view of packet loss in data transmission in the network with and without black hole attack and also compares the packet loss in proposed solutions.

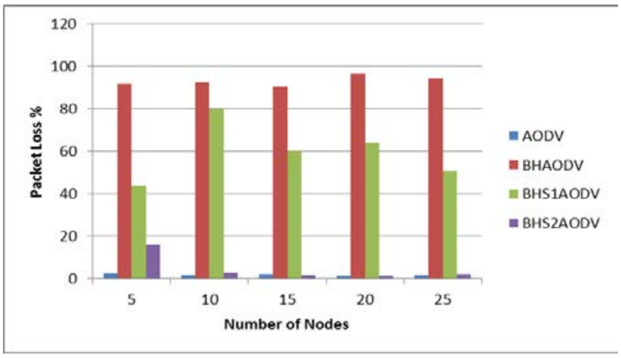

Fig. 5 Packet loss% versus Number of Nodes

The following Table 6 presents the throughput obtained in different scenarios and shows it through Fig. 6 shown below.

Table 6 Throughputs In Different Scinarios

THROUGHPUT					
Number of Nodes		**AODV**	**BHAODV**	**BHS1AODV**	**BHS2AODV**
5		60.99	47.81	55.93	60.97
10		63.12	37.68	53.75	67.55
15		65.76	40.06	57.98	66.28
20		66.18	40.64	46.87	53.54

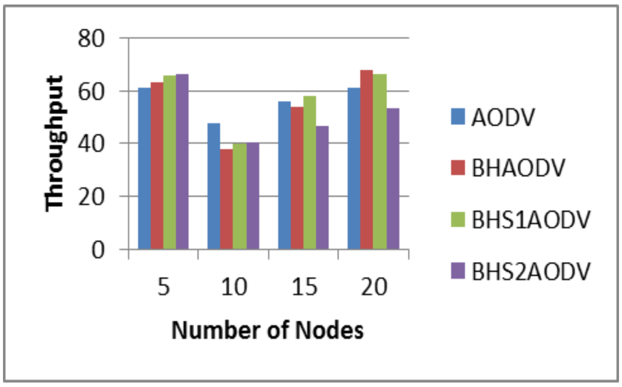

Fig. 6 Throughput versus Number of Nodes

The following table 7 and Fig. 7 show the comparative view of energy consumption by a node in the network in data transmission.

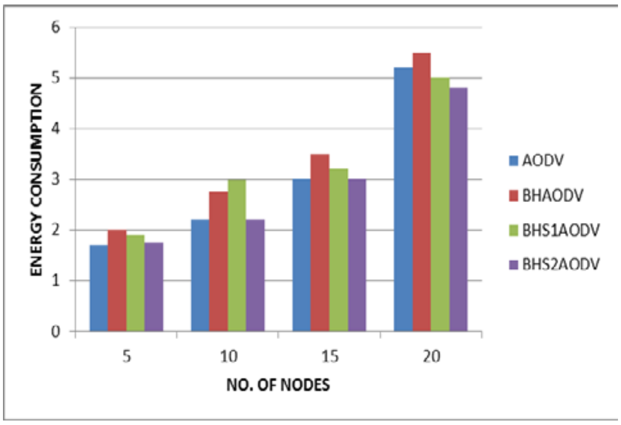

Fig. 7 Energy Consumption versus Number of Nodes.

Table7 Energy Consumption In Different Scinarios

Average Energy Consumption (in Joule)

NO. OF NODES	5	10	15	20
AODV	1.7	2.2	3	5.2
BHAODV	2	2.75	3.5	5.5
BHS1AODV	1.9	2.98	3.2	5
BHS2AODV	1.75	2.2	3	4.8

VI. CONCLUSION

It is obvious that AODV network has normally 1.85% data loss and if a malicious node i.e. Black Hole Node enters in this network and data loss is increased to 93.04 %. This leads data loss by 91.19 %. The proposed BHS1AODV solution in the same network scenario decreased packet loss to 59.97 % and in case of BHS2AODV it was 4.77%. These two results show that our solution reduces the Black Hole effects by 33.07% in packet loss using BHS1AODV and 89.27% by using BHS2AODV in a network. It was also observed that AODV protocol performs satisfactorily. But when number of nodes increased, the packet delivery ratio and throughput also decreased as with increase number of nodes collision increses and causing loss of packets. It was also observed that packet loss ratio and packet drop rate increased with increase in number of nodes. Each node is associated with some initial energy, when energy of node becomes less than a threshold value (assigned) it starts dropping the packet instead of forwarding. It was also analysed that when pause time increases the packet delivery ratio and throughput also decreases but packet loss ratio and packet drop rate both increases. Further work can be done by taking different protocols, analyzing their performance by taking different parameters and comparing the results.

REFERENCES

[1] E. Cayırcı, C.Rong, “Security in Wireless Ad Hoc and Sensor Networks,” vol. I. New York, Wiley, pp. 10, 2009.

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

[3] C. Jiwen, Y. Ping, Jialin, W.Zhiyang, L.Ning, “ An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network”, 24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks," in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom), pp. 255-265, 2000.

[5] S. Lu, L. Li, K-Y Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand BlackHole Attack", Proc. of Intl. Conference on Computational Intelligence and Security (CIS ’09), Dec. 11-14, Beijing, China, pp. 421-425, 2009.

[6] S. Deswal and S. Singh, “Implementation of Routing Security Aspects in AODV", Intl. Journal of Computer Theory and Engineering,Vol. 2, No.1 Feb., 2010.

[7] B.Dahill, B.N. Levine, E. Royer and C.Shields, “ARAN: Asecure Routing Protocol for Ad Hoc Networks”, UMass Tech Report 02-32, 2002.

[8] S. Yi, P. Naldurg and R. Kravets, “Security-aware ad hoc routing for wireless networks”, In MobiHOC, October 2001.

[9] Y –C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks”, In Proc. 8th ACM International Conference Mobile Computing and Networking (Mobicom’02), Atlanta, Georgia, PP. 12-23.

[10] Neerja khatri, Arvind kumar 2012 Analysing performance of AODV routing protocol in mobile adhoc network, International Journal of Engineering Research and Technology,Vol 1 Issue 3 ISSN:2278-0181