Optimizing Performance of Routing against Black Hole Attack in MANET using AODV Protocol

Prerana A. Chaudhari[1] Vanaraj B. Vaghela[2]
[1]PG Student Student [2]Principal
[1,2]Department of Electronics and Communication Engineering
[1]Sankalchand Patel college of Engineering Visnagar, Gujarat Technological University.University of Gujarat (India)
[2] Jashodaba polytechnic institute, Sidhpur ,Gujarat Technological University .University of Gujarat (India)

Abstract— MANETs (Mobile Ad hoc Networks) must have a secure way for transmission and communication and this is a quite challenging and vital issue as there is increasing threats of attack on the Mobile Networks. Security is the cry of the day. In order to provide secure communication and transmission, we must understand different types of attacks and their effects on the MANETs. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. A MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes, there is no central point for network management, no authorization facility, vigorously changing topology and limited resources. Here, a mechanism is proposed for the nodes which are deployed in MANETs in order to detect and prevent black hole attacks. The proposed mechanism is incorporated in AODV routing protocol and is implemented and simulated in Network Simulator 2.

***Key Words*:** Mobile Ad hoc network (MANET), Ad-hoc On-demand Distance Vector (AODV), Black Hole attack

I. INTRODUCTION

To meet the necessity for a quick and reliable information exchange, communication networks have become an integral part of our society. The prosperity of any organization mostly depends on its ability to communicate. Ad hoc wireless networks will enhance communication capability importantly, by providing connectivity from anyplace at any time. In recent years, Mobile Ad- hoc Networks (MANETs) have optically recognize widespread applications in commercial, domestic and strategic areas and with more focus on their security.

Mobile Ad Hoc Network is an Ad Hoc Network however Ad Hoc Network is not MANET. MANET is "Mobile ad hoc Networks". Mobile is transportable Ad Hoc implies temporary basis Networks, the flexible data applications that uses networks to communicate, so MANETs are the formation of ad hoc networks for communication between two nodes. MANETs are the future wireless network, that does not need any base station for their communication. While communicating with MANET no infrastructure is needed because it does not need any central established router. Any node can act as a router at the time of communication. So, it's a self-dominant infrastructure less networks established for the communication purpose [1].

In a MANET, nodes among one another's wireless transmission range can communicate directly; but, nodes outside one another's range have to consider another nodes to relay messages. Thus, a multi-hop scenario happens, where many intermediate hosts relay the packets sent by the source host making them reach the destination node [2].

II. ROUTING IN MOBILE AD- HOC NETWORK

Routing is the procedure of selecting paths in a network, the responsibility of a routing protocol incorporates exchanging the route information and discovering a feasible path to a destination on criteria, for example, network lifetime, least power requirement, and hop length. During the process of routing, a source wanting to send a packet to a specific destination sends the packet to a neighboring node with the route information. This node, thus, sends the packet to the next hop on the route, thus on till the destination is reached. A variety of routing protocols for Mobile Ad hoc systems have been proposed in the recent past. There are mainly three types of routing protocols used in Ad hoc network, which are mentioned as below.

- Proactive (Table Driven) Routing Protocols
- Reactive (On Demand) Routing Protocols
- Hybrid Routing Protocols

A. Proactive (Table Driven) Routing Protocols

In proactive routing protocols, all the nodes (routers) periodically exchange routing information with the aim of maintaining a uniform, updated and complete network view. Every node uses the exchanged information to calculate the costs towards all attainable destinations. That way, if a destination is found, there will always be a route available towards it. The main advantage of proactive routing schemes is that there is no initial delay once a route is needed. On the other hand, these are usually related to a bigger overhead and a larger convergence time than for reactive routing techniques, particularly once mobility is high [3].

E.g. Destination sequence distance vector (DSDV), Wireless routing protocol (WRP),Clustered gateway switch routing protocol (CGSR), Source tree adaptive routing (STAR).

B. Reactive (On Demand) Routing Protocols

Reactive routing does not rely, in general, of periodic exchange of routing information or route calculation. Therefore, once a route is needed, the node must begin a route discovery process. This suggests that it must propagate the route request throughout the network and wait for an answer before it can proceed to send packets to the destination. The route is maintained till the destination is unreachable or till the route is no longer necessary. By

following this strategy, reactive routing protocols keep to a minimum the resource consumption by avoiding the other of unused routes. On the opposite hand, the route discovery process causes a significant startup delay and causes a substantial waste of resources. If the network is wide enough, the overhead will be similar or superior to that achieved with proactive routing protocols [3]. E.g. Dynamic source routing (DSR), Ad hoc on demand distance vector (AODV), Associativity Based Routing (ABR). According to the above discussion of two main types of routing protocols it is clear that Proactive routing protocols are the extension of wired network routing protocols and they are beneficial mainly for wired networks. Thus, Reactive routing protocols suits more for Mobile ad hoc Networks.

C. Hybrid Routing Protocols

Hybrid protocols make use of each reactive and proactive approaches. They typically offer means that to switch dynamically between the reactive and proactive elements of the protocol. E.g. Zone Routing Protocol (ZRP).

III. AODV ROUTING PROTOCOL

The advantage of the reactive schemes is that they do not consume a large amount of network bandwidth. In reactive protocols, AODV is chosen because, AODV consumes less memory, compared to DSR and ABR, that consumes additional memory for a route cache.

- AODV are efficient in high mobility networks, however DSR and ABR protocols are efficient solely in networks with less or no mobility.
- Source packet size in DSR and ABR is large due to route cache, compared to AODV.

AODV is an on demand distance vector routing protocol. In on demand routing a route is established between communicating nodes only. There is no fixed existing route as in table driven systems. Whenever a node needs to send data packets it has to initiate route discovery process. Route
discovery consists of two messages: Route Request(RREQ) and Route Reply (RREP) [4].

A. Route Discovery

Route discovery process is initiated whenever a node needs to send data packet to the destination and there is no valid route available in its routing table. The source node then broadcasts a route request (RREQ) packet to all its neighbor nodes, which then forward the request to their neighbor nodes and the process repeats. Each node is assigned a sequence no. and a broadcast ID which is incremented each time the node issues a RREQ packet.

The broadcast ID together with the node_s IP address, exclusively identifies a RREQ [5] which is unique in nature. The RREQ packet contains following fields:

- Sequence number of RREQ
- Broadcast ID

The most recent sequence number of the destination Upon receiving RREQ by a node which is either destination node or an intermediate node with a fresh route to destination, it replies by unicasting a route reply (RREP) message to the source node. As the RREP is routed back along the reverse path, intermediate nodes along this path set up forward path entries to the destination in their routing tables. When the RREP reaches source node, a route from source to destination node is established [6].

B. Route Maintenance

Once a route is established between source and destination, it needs maintenance usually at the source end. When any link break or failure is detected, it is declared as invalid and a route error (RERR) message is flooded to all the nodes in the network. These
nodes in turn broadcast the RERR to their ancestor nodes and so on till the influenced source node. Then it is the source node who may decide whether to stop sending data or restart the route discovery process for that particular destination by sending out a fresh RREQ message to its neighbor nodes [7].

IV. BLACK HOLE ATTACK

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. A basic attack that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place. In blackhole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from

other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all objects; data packets. Fig. 1 Blackhole attacks in MANETs In figure 1, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a blackhole. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D [8].

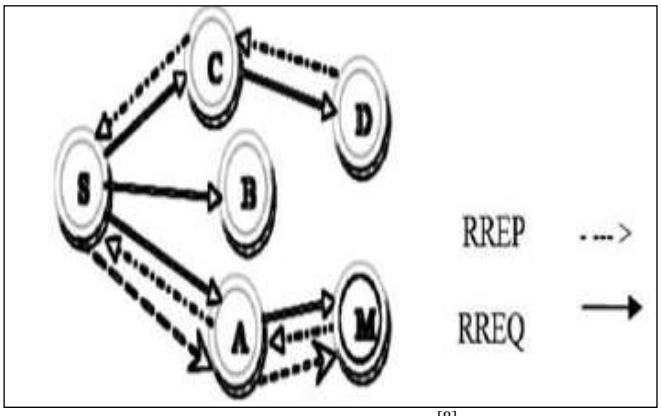


Figure 1: Black hole Attack [8]

V. PROPOSED METHODOLOGY

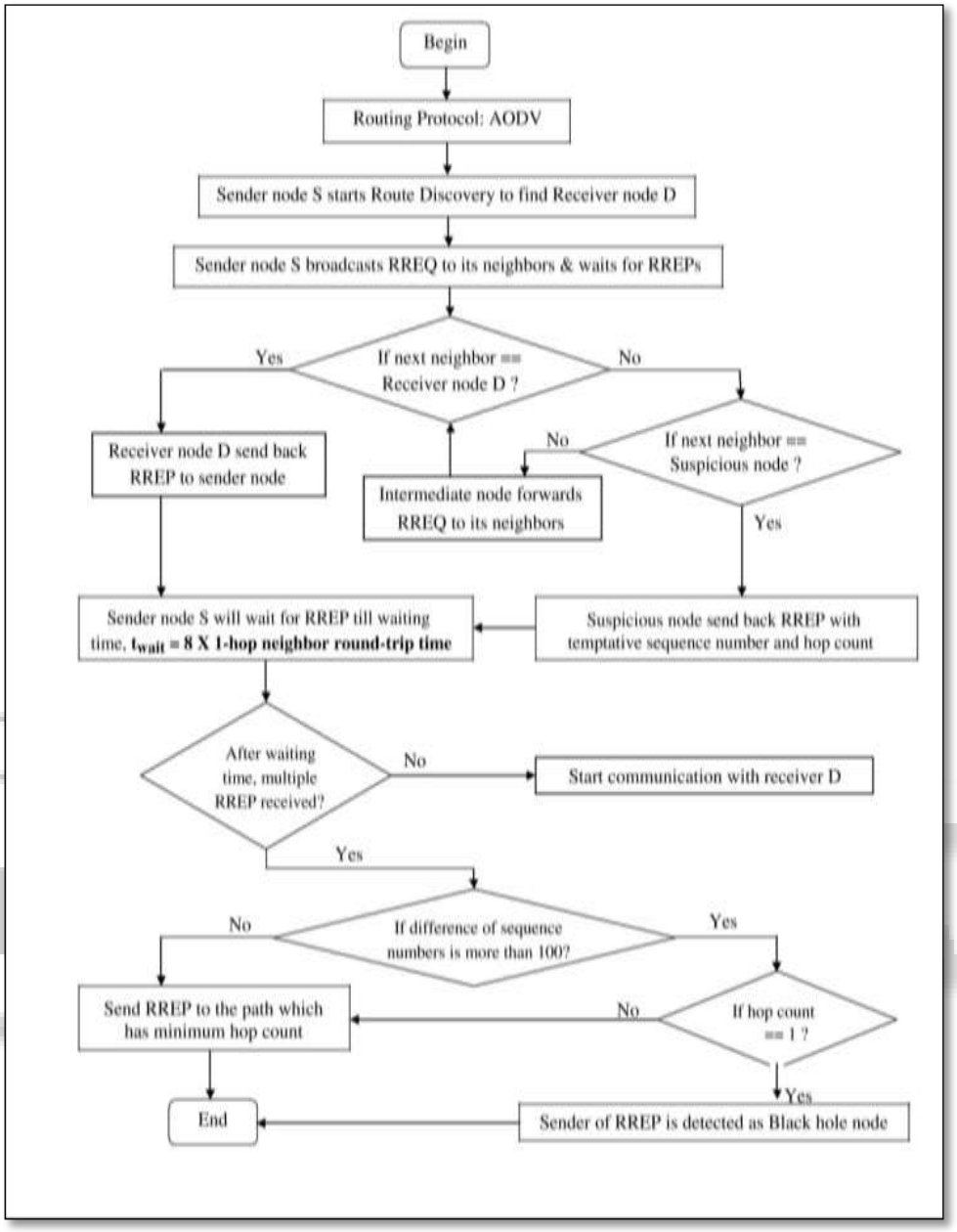


Figure 2: Proposed Algorithm

VI. SIMULATION RESULTS AND ANALYSIS

The simulation tool used is NS2 (v-2.34) network simulator. The NS2 is an event-driven simulator tool that is specifically designed to study the dynamic nature of wireless communication networks.

Here, in this work i have taken different node scenario that means 25,35,50 and 60 nodes in a wireless network. The simulation environment is taken 700 by 700 square meter space. In a simulation 5 black hole nodes are implemented in a wireless network. The simulation time is 100 seconds. The packets were generated using CBR with a packet size 512 bytes. Here, i have also taken waiting time for sender node, a time for which a sender node will wait for route reply from different nodes. The value of which is, t_{wait} = 8 X 1-hop neighbor round-trip time.

Parameters	**Value**
Simulator	NS-2(Version 2.34)
Channel type	Wireless
Simulation Time	100 seconds
Number of mobile nodes	25, 35, 50, 60
Number of malicious nodes	5
Packet Size	512 bytes
Traffic Type	CBR
Routing Protocols	AODV

Table 1: Simulation Parameters

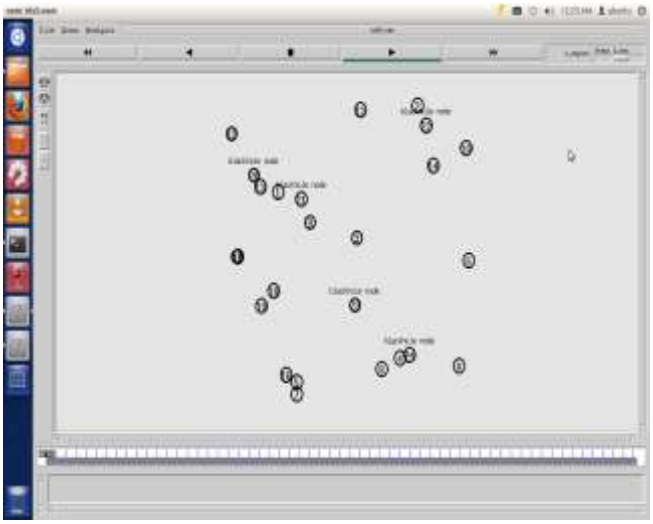


Figure 3: NAM of proposed AODV Output File for 25 nodes with 5 black hole nodes

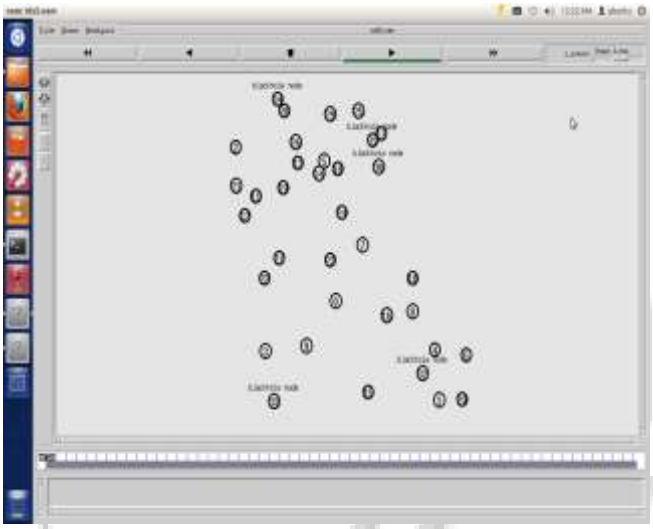


Figure 4: NAM of proposed AODV Output File for 35 nodes with 5 black hole nodes

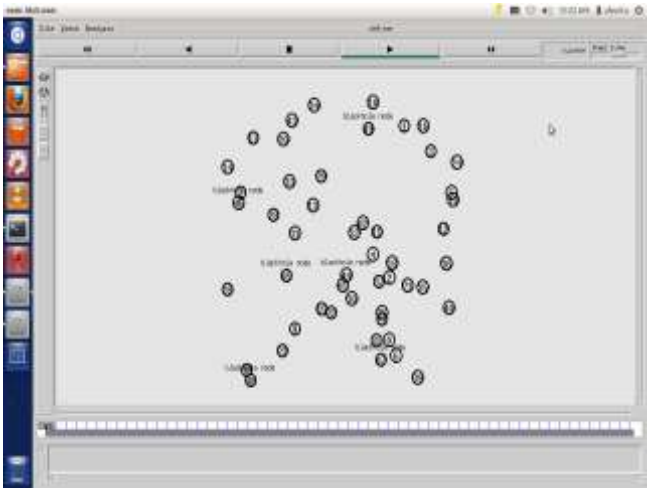


Figure 5: NAM of proposed AODV Output File for 50 nodes with 5 black hole nodes

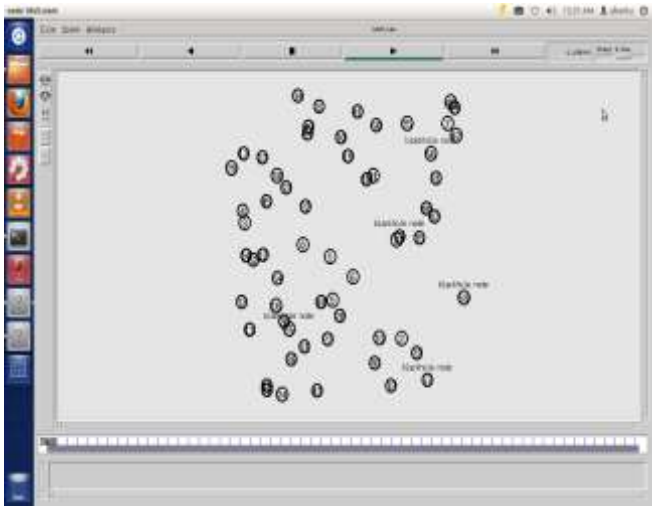
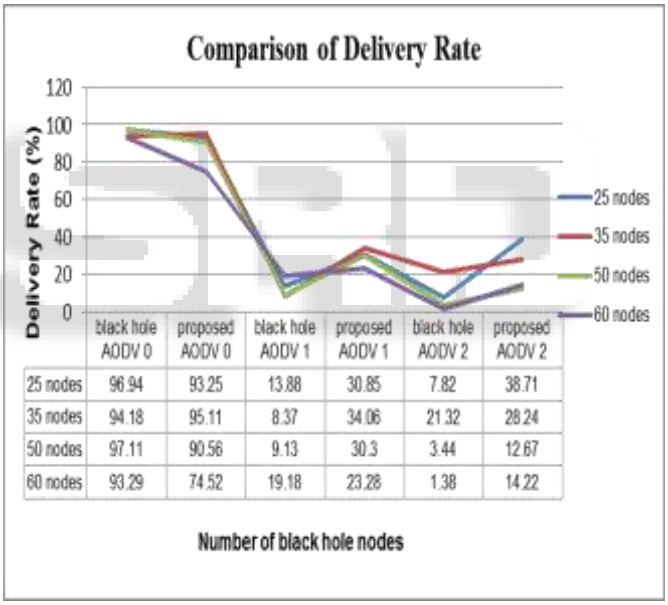


Figure 6: NAM of proposed AODV Output File for 60 nodes with 5 black hole nodes

1) Delivery Rate

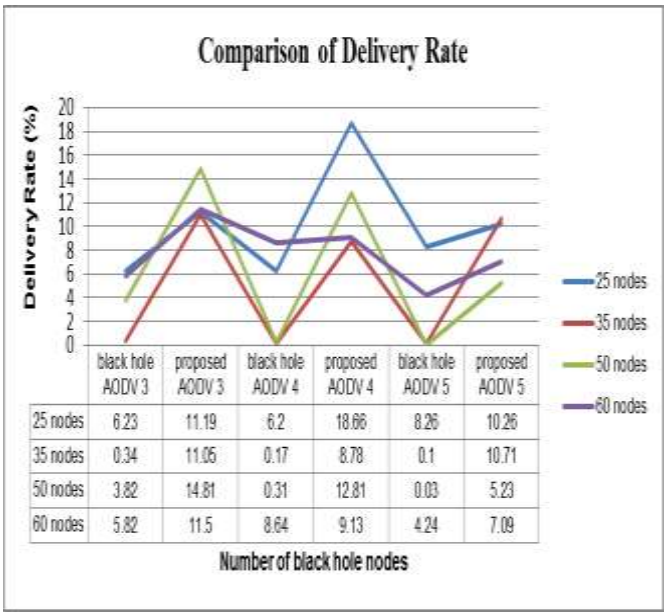
The percentage of the ratio between the data packets delivered to destination with respect to the number of packets sent. The graph in figure 7 shows the comparison of delivery rate without a black hole node, and with one and two number of black ole nodes.



	black hole AODV 0	proposed AODV 0	black hole AODV 1	proposed AODV 1	black hole AODV 2	proposed AODV 2
25 nodes	96.94	93.25	13.88	30.85	7.82	38.71
35 nodes	94.18	95.11	8.37	34.06	21.32	28.24
50 nodes	97.11	90.56	9.13	30.3	3.44	12.67
60 nodes	93.29	74.52	19.18	23.28	1.38	14.22

Figure 7: Delivery Rate comparison for different node scenario with 0,1,2 no. of black hole nodes

Here, the graph in figure 8 shows the comparison of delivery rate with three, four and five numbers of black hole nodes.

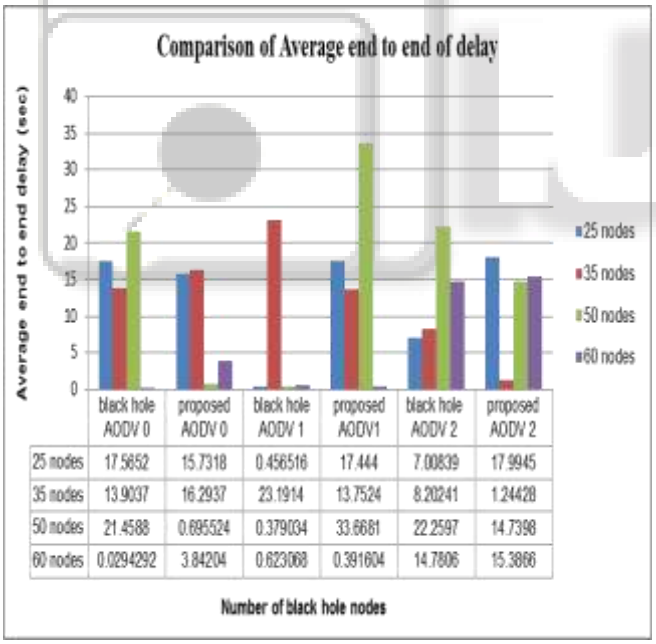


	black hole AODV 3	proposed AODV 3	black hole AODV 4	proposed AODV 4	black hole AODV 5	proposed AODV 5
25 nodes	6.23	11.19	6.2	18.66	8.26	10.26
35 nodes	0.34	11.05	0.17	8.78	0.1	10.71
50 nodes	3.82	14.81	0.31	12.81	0.03	5.23
60 nodes	5.82	11.5	8.64	9.13	4.24	7.09

Figure 8: Delivery Rate comparison for different node scenario with 3,4,5 no. of black hole nodes

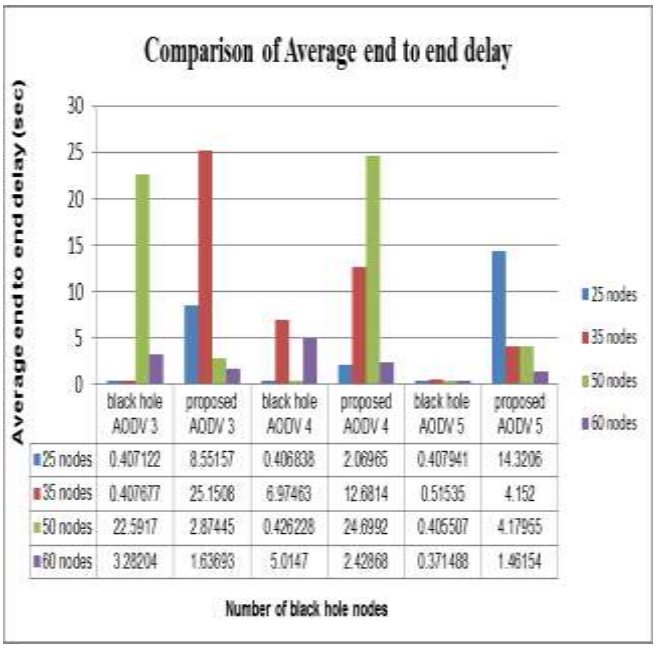
2) Average end to end Delay

The time taken for a packet to be transmitted across a network from source to destination. Here, also the graph shown below indicates the comparison of the average end to end delay without black hole attack and with 1,2,3,4 and 5 numbers of black hole nodes.



	black hole AODV 0	proposed AODV 0	black hole AODV 1	proposed AODV1	black hole AODV 2	proposed AODV 2
25 nodes	17.5652	15.7318	0.456516	17.444	7.00839	17.9945
35 nodes	13.9037	16.2937	23.1914	13.7524	8.20241	1.24428
50 nodes	21.4588	0.695524	0.379034	33.6681	22.2597	14.7398
60 nodes	0.0294292	3.84204	0.623068	0.391604	14.7806	15.3866

Figure 9: Average end to end Delay comparison for different node scenario with 0,1,2 no. of black hole nodes

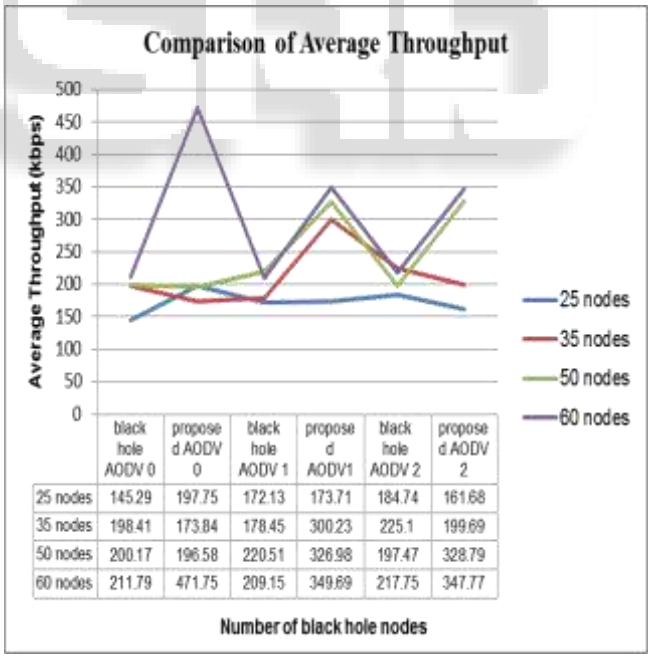


	black hole AODV 3	proposed AODV 3	black hole AODV 4	proposed AODV 4	black hole AODV 5	proposed AODV 5
25 nodes	0.407122	8.55157	0.406838	2.06965	0.407941	14.3206
35 nodes	0.407677	25.1508	6.97463	12.6814	0.51535	4.152
50 nodes	22.5917	2.87445	0.426228	24.6992	0.406507	4.17955
60 nodes	3.28204	1.63693	5.0147	2.42868	0.371488	1.46154

Figure 10: Avg. End to end Delay comparison for different node scenario with 3,4,5 no. of black hole nodes

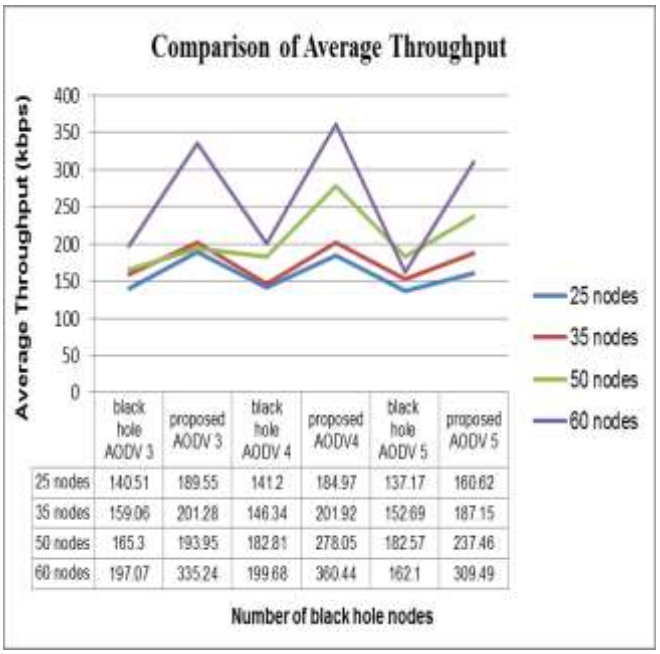
3) Average Throughput

Throughput is the average rate of successful message delivery over a communication channel. The graph shows that the comparison in throughput of network without and with 1,2,3,4 and 5 numbers of black hole nodes. The results of throughput in proposed scheme are good as compared to black hole attack.



	black hole AODV 0	proposed AODV 0	black hole AODV 1	proposed AODV1	black hole AODV 2	proposed AODV 2
25 nodes	145.29	197.75	172.13	173.71	184.74	161.68
35 nodes	198.41	173.84	178.45	300.23	225.1	199.69
50 nodes	200.17	196.58	220.51	326.98	197.47	328.79
60 nodes	211.79	471.75	209.15	349.69	217.75	347.77

Figure 11: Average Throughput comparison for different node scenario with 0,1,2 no. of black hole nodes



	black hole AODV 3	proposed AODV 3	black hole AODV 4	proposed AODV4	black hole AODV 5	proposed AODV 5
25 nodes	140.51	189.55	141.2	184.97	137.17	160.62
35 nodes	159.06	201.28	146.34	201.92	152.69	187.15
50 nodes	165.3	193.95	182.81	278.05	182.57	237.46
60 nodes	197.07	335.24	199.68	360.44	162.1	309.49

Figure 12: Average Throughput comparison for different node scenario with 3,4,5 no. of black hole nodes

VII. CONCLUSION AND FUTURE WORK

We have developed a new black hole prevention and detection mechanism/method to improve the security requirement in AODV. According to the simulation results of various parameters e. g. Delivery Rate, Average end to end Delay, and Average throughput in proposed mechanism is performed better than Black hole AODV. In future, Proposed scheme will be simulated on various mobility models, various traffic conditions, traffic pairs, and pause times.

ACKNOWLEDGMENT

I would like to thank Prof. Vanaraj B. Vaghela sir for his guidelines in making this paper.

REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, 'An Overview of Mobile Ad Hoc Networks: Applications and Challenges', Department of Information Technology (INTEC), Ghent University.

[2] Chaubey, Nirbhaykumar, 'Enhancement of security mechanism in design of mobile ad hoc networks using suitable security algorithm', Department of Computer Science.

[3] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava, ' An Overview of AODV Routing Protocol', International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.3, May-June 2012 pp-728-732.

[4] Ravinder Kaur, Jyoti Kalra, "Detection and Prevention of Black Hole attack with Digital Signature", IJARCSSE volume 4, issue 8, August 2014.

[5] C. E. Perkins; E. M. Belding-Royer; and S. R.Das (2003). Ad hoc on demand distance vector (AODV) routing. RFC 3561. The Internet Engineering Task Force, Network Working Group.

[6] H.L. Nguyen, U.T. Nguyen, ―Study of Different Types of Attacks on Multicast in Mobile Ad- Hoc Networks, International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006

