Effect Analysis of Black Hole Attack of AODV Protocol in MANET using Table Driven Approach

Richa Kudesia
Department of CS&E
IFTM University
Moradabad, U.P., India

Ankur Jain
Department of CS&E
IFTM University
Moradabad, U.P., India

Bharti Jain
Department of E&CE
IFTM University
Moradabad, U.P., India

ABSTRACT

MANET is a wireless network that allows user to communicate and transfer information without using any infrastructure and irrespective of their location. They are very useful for home uses, for military uses etc. Though they are very useful in day to day life, major threats are also there to attack over it; some of them are wormhole attack, denial of service, eavesdropping etc. Black Hole attack is one of the major attacks on MANET. In this research paper, the effect of black hole over the network is evaluated by varying certain values of the network like number of nodes, pause time, area and speed. This paper shows that despite of presence of black hole in the network, the increament and decrement of certain values also affect the performance of MANET. For this, a table has been used which stores all the values of the parameters with and without black hole in the network obtaining by variations among the several values. Before and after values are stored which are afterwards will use for the analysis of the performance of the protocol. The protocol used in this paper is AODV (Ad-Hoc on Demand Distance Vector) protocol.

General Terms

Wireless Computer Network, MANET, Ad-Hoc on Demand Distance Vector Protocol.

Keywords

Black Hole Attack, Malicious nodes, AODV protocol, Routing Protocols.

1. INTRODUCTION

Wireless networks are its extreme popularity today because all users want to operate and to get their work done instantly irrespective of their geographic positions, and wireless network is able to perform this task as it enables users to communicate and transfer data with each other without any wired medium between them. The ad-hoc network comes under the wireless network where no infrastructure is needed to communicate with each other. Ad-hoc network is the network where there is no infrastructure and nodes are able to join and leave the network. This network is also known as infrastructure less network because nodes serve as router to forward data to neighbours nodes.

Most important networking operations include network management and routing. Routing protocols are classifies into three categories based on their functionality:

1. Reactive protocols - also known as on demand routing protocol as they do not maintain routing information, until they are requested, e.g. Dynamic Source Routing (DSR).
2. Proactive protocols - also known as table driven protocols as it requires each node to maintain one or more tables to store routing information, e.g. Destination Sequenced Distance Vector (DSDV).
3. Hybrid protocols - exploit the strengths of both reactive and proactive protocols, and combine them together to get better results, e.g. Zone Routing Protocol (ZSR).

Security is the major issue of MANET as the working and performance totally depends on the attacks and threats and thus it is necessary to minimize and remove the vulnerability of attacks.

2. AD-HOC ON DEMAND DISTANCE VECTOR (AODV) PROTOCOL

AODV is a reactive protocol. In AODV, network is silent until a connection is needed. When a node wishes to start transmission from another node in a network to which it has no route, AODV provides topology information for the node. There is a procedure which is followed by the protocol in order to provide a path to the nodes. AODV uses control messages in order to find a route to the destination node. Three control messages are used by AODV are route request message (RREQ) which is send by the source node, route reply message (RREP) send by the other nodes about the route and route error message (RERR) which are used when the connections are no more present and nodes keep moving around.

Whenever a node wants to send a data packet to another node, it scans its routing table. If it has a fresh route to the destination node then it sends the packet along with that route. If it does not have a route then it starts route discovery process. In route discovery process, it sends the RREQ message to its neighbours. The intermediate node checks that whether it is the destination node or it has a fresh route to the destination node. If it is the destination node then it sends back the RREP message to the source node, otherwise it forwards the message to its neighbours. This process continues until the destination node is found or a node that has the fresh route to the destination is found. After the route discovery process is over, the source node and the destination node communicate with each other and send the packets between them.

AODV provides no security measures thus it is very easy for a malicious node to perform any kind of attack by simply following the rules provided by the AODV. This research paper provides a security measure to prevent the network with the Black Hole Attack.

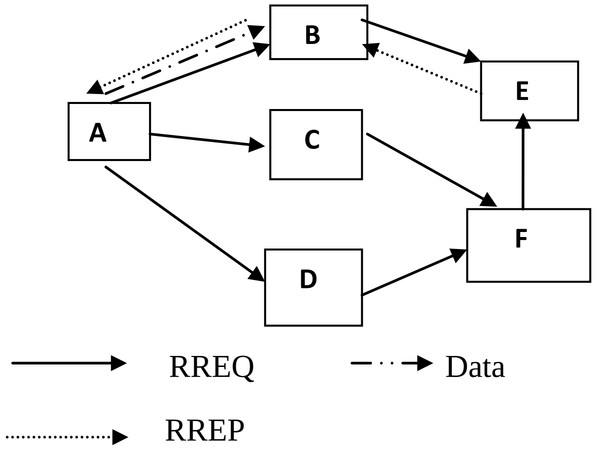

Fig. 1 Propagation of RREQ and RREP from A to E

3. BLACK HOLE ATTACK

In this attack, the malicious node advertise itself to have the shortest route for the communication and transferring of packets, and thus drops the packets without forwarding them to the neighbouring nodes. Black hole attack is one of the possible attack and most common attack in MANET. It can be said as the Denial of Service. In this attack, a node generates a RREQ message and passes it to its neighbours; a malicious node advertises that it has the best path to the destination node during the process of route discovery. As soon as it receives the RREQ message from the source node, it immediately sends back a fake RREP message to it. The source node receives the RREP message and starts sending the packet to it. When source node starts sending packets to the destination by using this route, the malicious node drops all packets instead of forwarding it. In other words it can be said that it "swallows" the data packet.

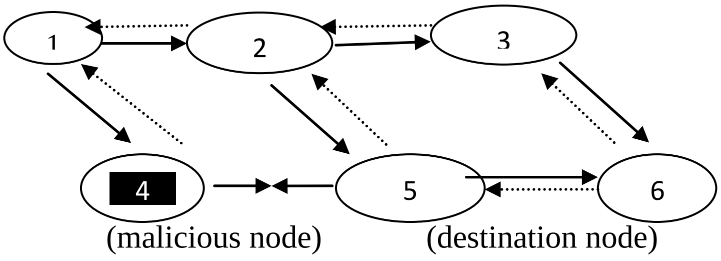

Fig. 2 Black Hole Attack

For instance, let's have a look over the above figure

In the above figure, there are 6 nodes out of which node 1 is the source node which generates the RREQ message in order to find the fresh route to send a packet to the destination node i.e. node 6. The intermediate nodes of node 1 are node 2 and node 4. Both the nodes get the RREQ message generated by the node 1. Node 4, being the malicious node, sends the RREP message back to the node 1 advertising that it has the best path to the destination node, node 6. After receiving the RREP message from node 4, node 1 started sending the packet to the node 4. But node 4 will not forward it; it discards all the messages just making it the denial of service.

In this:

- Source node: Node 1.
- Destination node: Node 6
- Malicious Node: Node 4

4. RELATED WORK

Previously, a lot of work has been done to eliminate the Black Hole Attack. Many researchers presented different procedures and algorithm over this. Some of them are given below.

Many researchers have given the solution to find out and eliminate a single black hole node, but no one has proposed a solution for multiple nodes acting in coordination. For example, if there are two black nodes in the network, n1 and n2,and by the solution provided by the researchers if n1 is considered as malicious node, then the source node will send the RREP to other nodes including n2 eliminating the n1. As n1 is coordinating with n2, n2 will give a positive reply to source node saying that it has the shortest route to the destination node and source node will start sending packets through n2. But as n2 is in coordination with n1, the packets will be consumed by n1 and security will be compromised. In [1] Ravinder Kaur used the digital signature to detect the malicious node. Digital signature is one of the verification techniques. All nodes are provided with a digital signature. This method was very effective but applying digital signature to every node is a bit difficult task. In [2] T.Manikandan proposes a method of activating the immoral node and hence further data packet loss is prevented. They analyze the performance of the nodes after the inclusion of immoral node. The immoral node is applied only for nodes that were attacked rather for applying for all the nodes. Jaspinder Kaur in her paper detects and isolate malicious node from the network by using fake route request packets [3]. This confuses the malicious node and thus detection become easy. Some work has been done by analyzing different protocols with and without Black hole attack by Manju Bala [4]. It has been concluded that AODV protocol with malicious nodes and without malicious nodes performs better in all the cases. In [5] Akshat Jain presented that every node is maintained an authentication table of their neighbours and digital signature is used. Light-weight packet is used by the source node to destination node encrypted by its own private key KPRs and public key of destination KPUd. They concluded that as the solution contains a LWP so not much of routing overhead increases in the network. Santosh Kumar evaluated the performance of AODV protocol in presence of malicious nodes which causes the black hole attack and without them with cbr traffic under different scalable network mobility and for this they used the RWP model [6]. They checked the working of AODV protocol one by one first checking it without the malicious nodes and then with malicious nodes. It was concluded that when a node became a malicious node, it affected the performance of the AODV protocol. In some paper, they studied the problem of black hole attack in inter cluster MANET routing and proposed a feasible solution for it on the top of AODV protocol to avoid the black hole attack, and also prevent the network from further malicious behaviour by Ira Nath [7]. Ekta Barkhodia evaluated the performance of AODV protocol with respect to throughput and end to end delay using OPNET modeller [8]. They checked the performance under the presence of malicious nodes. The average end to end delay increases with the increasing number of malicious nodes while throughput varied with the increasing number of malicious nodes, i.e. throughput also increases with the increased number of malicious nodes. The effect of black hole attack has been studied in both proactive (OLSR) and reactive (AODV) protocols and a comparison is done between them [9] by Irshad Ullah. The impact of Black Hole attack is evaluated by finding out which protocol is more dangerous towards the attack. Payal N. Raj [10] proposed a DPRAODV (Detection, Prevention and Reactive AODV) to secure attacks of black hole by reporting other nodes in the network. The parameters used by her were packet delivery ratio, end to end delay and routing overhead. But in case of other parameters, this solution is not so feasible. Detection of a malicious node is done by introducing a fidelity table in the network Latha tamilselvan [11]. It has been analyzed that the percentage of packets received through is more than that in AODV in presence of co-operative Black Hole attack. Topology Graph based Anomaly Detection (TOGBAD) is introduced by Marko Jahnke [12]. They created a topology graph and the number of nodes according to the topology graph is calculated. The number of neighbours that a node says to have in its HELLO messages is determined. For each HELLO message, the sender's number of neighbours according to the message is checked for possibility against the number of neighbours according to the topology graph. A significant difference between the two values will trigger an alarm. In this he considered a node that is generating unreal routing information is a malicious node. It would trigger an alarm if the check fails. The detection of malicious node has been carried out by introducing a new black hole node in the route [13] by Semih Dokurer. Conclusion was that introducing a new node in the network reduces the black hole attack effects by some percentage. The characteristic changes in the node also doubts over the nature of a node. This is concluded by Nikayama [14]. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a selective black hole node, otherwise, the data of the latest observation is added into dataset for dynamic updating purposes. The characteristics observed in this method include the number of sent RREQs, the number of received RREPs and the mean destination sequence number of the observed RREQs and RREPs. However, it does not involve a detection mode, such as revising the AODV protocol or deploying IDS nodes, thus it does not isolate selective black hole nodes. Bo Sun [15] tried to eliminate the Black hole attack effect in routing control office. Cryptography based method is used by them to evaluate the effect of black hole attack.

5. PROBLEM STATEMENT

MANET is the most successful and widely used network today, as there is no need of any infrastructure to exchange message with one another or from one device to another device. There are three kinds of routing protocols over which the MANET works. They are reactive protocols, proactive protocols and hybrid protocols. The basic difference between these protocols is that in reactive protocol the route is discovered whenever it is demanded by a node and in proactive protocols, they have the information about the destinations in the network. Hybrid protocol carries the functionality of both the reactive and proactive protocols. MANET is in high demand today but it also has many security issues. It is vulnerable to many attacks like wormhole attack, denial of service, eavesdropping etc. Black Hole Attack is one of the major attack to which MANET is vulnerable. In this attack, a node presents itself as it has the shortest path to convey the message to the desired node and thus the source node starts sending the packets to the destination node via that node. But as it was the malicious node, it instead of sending the packets further in the network starts dropping them and thus compromises the security. Much of the work has been done before by other writers over Black Hole attack in MANET using different procedures. Some made use of digital signature; some introduced a new node in the network. In this thesis, the detection of malicious node will be carried out by using a table in the network.

6. SIMULATION ENVIRONMENT

For simulation, we have used ns2 (v-2.35) network simulator. Ns is a discrete event simulator targeted at networking research [6]. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks [4]. The simulation is done to analyze the performance of the network's various parameters. The metrics used for the performances are given below:

6.1.1 Throughput: It is the ratio between the total amount of data and the time taken to the receiver to receive the packet.

6.1.2 Packet end to end delay: It is the average time taken by the packet to travel in the network.

6.1.3 Network Load: It is the total traffic of the whole network from the higher layer of MAC that is received and chained for transmission.

The simulation tool used for this study is ns-2. Ns-2 is one of the discrete-event network simulator used in research and training. Ns-2 works at packet level and also provides considerable support to simulate many protocols like DSR, TCP, FTP, UDP and HTTP. It simulated both wired and wireless networks. It is primarily UNIX based and its scripting language is TCL. Ns-2 is said to be standard experiment environment in research community. It is a discrete event scheduler. The goals of ns-2 are to support networking research and education like protocol design, traffic studies etc. It also supports protocol comparison, new architecture designs. It provides collaborative environment.

Scripts are written in TCL language. TCL is the short form of Tool Command Language. It is a programming language which is very dynamic. It is widely used in desktop and web applications, testing, networking etc. It is highly extensible and easily deployed. TCL language is compatible with C language and the libraries of TCL can be easily operated in C language. This is the most significant feature of TCL language.

7. RESULTS

Ns-2 simulator is used to analyze the effect of Black hole on the network. Parameters used for this purpose are packet delivery ratio (PDR), throughput, pause time and end to end delay. First the performance is checked of the network without any black hole and then with black hole. Comparison is done to evaluate the loss suffered by the network due to the presence of black hole.

Initial points used are given below:

Number of nodes	: 15
Pause time	: 0.0
Area	: 1000 x 1000
Speed	: 10.0

The routing protocol used is AODV.

7.1 Packet Delivery Ratio (PDR):

For evaluation of PDR, some variations are done.

a. **Variations in number of nodes**: By varying the number of nodes and keeping other parameters constant, it is checked that whether the effect on PDR increases or decreases. Variation in number of nodes is done first without introducing any black hole in the network and after that by introducing the black hole in the network. The result is that first by varying the number of nodes the PDR also fluctuates but not with a high difference. On comparing PDR with and without black hole, it is analyzed that PDR decreases with a noticeable difference in case of with black hole in the network. It can be easily understand by the following graph.

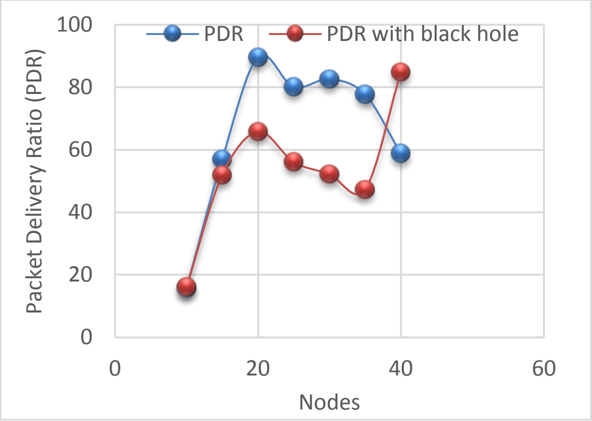

Fig. 3 Packet Delivery Ratio by varying number of nodes

b. **Variation in speed:** some analysis is done by keeping in mind that what affect the PDR will have if speed changes. So in this case, speed keeps on change while other variables remain constant. The difference in the performance of PDR is clearly showed in the given graph. It is showed that PDR decreases when the black hole is present but if the comparison is done between the performance when the black hole is present and it is absent, and then the difference is not too much. Minute drop is there in PDR when the black hole is present in the network.

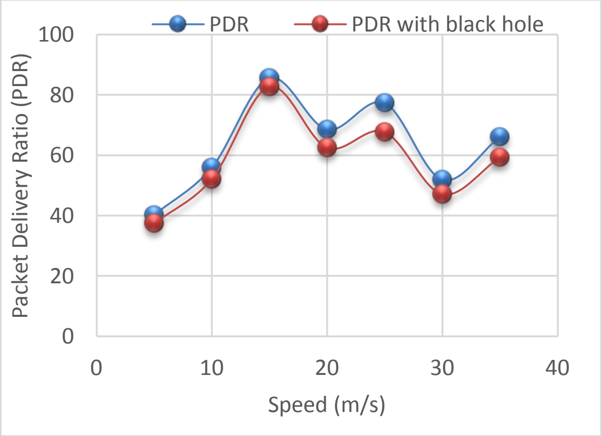

Fig. 4 Packet Delivery Ratio by varying speed

c. **Variation in pause time:** the effect of variation in pause time also matters while comparing the PDR. It has been evaluated that PDR in case of absence of black hole performs better than in the presence of black hole. However, the difference is not on a large scale, but yet the performance of PDR is better in the network having no black hole. The performance can be seen in the following graph.

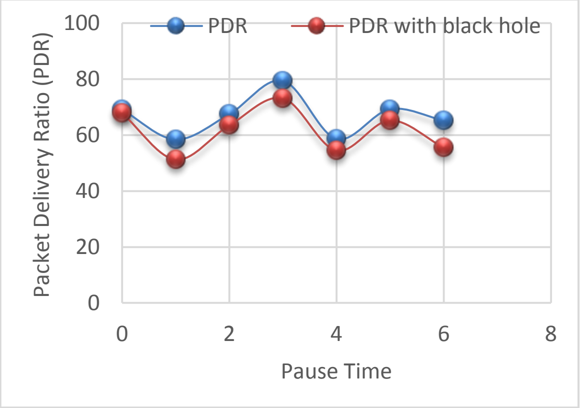

Fig. 5 Packet Delivery Ratio by varying the pause time

d. **Variation in Area:** variation in area does not have that much effect in the performance of PDR. Almost no difference is analyzed while evaluating the PDR with and without black hole as shown in the graph below.

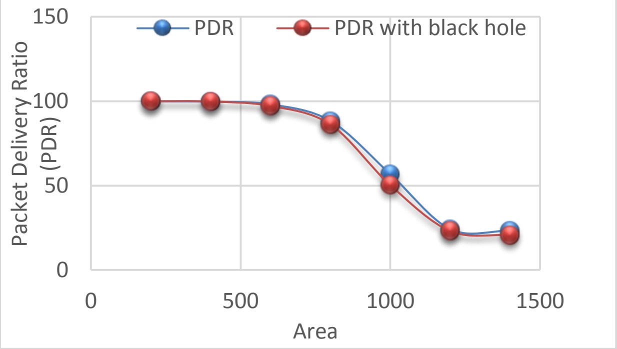

Fig. 6 Packet Delivery Ratio by varying the area

7.2 Throughput:

Throughput is also evaluated by varying different variables of the network.

a. Variation in number of nodes: Figure 7 shows the throughput after number of nodes is varied. To evaluate the throughput, no. of nodes is varied and on each varied number of nodes, throughput is checked in the presence of malicious node and in the absence of malicious node.

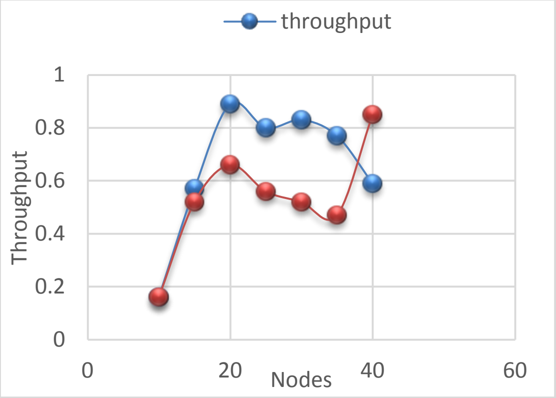

Fig. 7 Throughput by varying number of nodes

It can be observed by seeing the above graph that as the number of nodes increases, throughput first gets increase and after that keeps on decreasing in the case of testing without malicious node. On the other hand, while evaluating throughput in the presence of black hole, it can be seen that throughput first increases, then decreases and after that again increases.

B.Variation in speed: By varying the speed, it can be easily observed by seeing the figure 8 that there is a minute difference in the working of the protocol with and without malicious node.

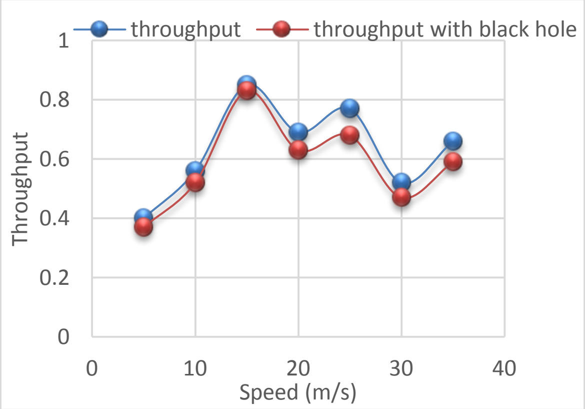

Fig. 8 Throughput by varying the speed

c. Variation in Pause time: Throughput is then evaluated by changing the pause time. Again the throughput is analyzed both with and without the malicious node as shown in fig.9.

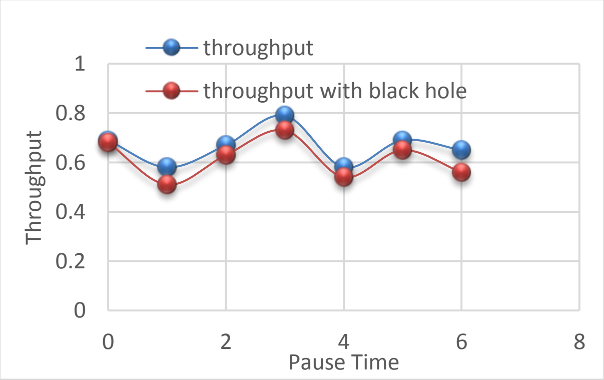

Fig. 9 Throughput by varying the Pause Time

It is clearly showed in the graph that throughput decreases in the presence of a black hole but the difference is negligible. Performance of the throughput affected but not that much.

d.Variation in Area: What effect will be there on throughput if area changes, this is shown in fig.10.

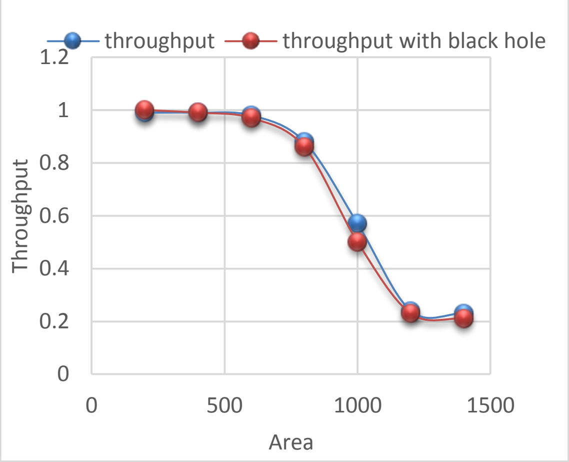

Fig. 10 Throughput by varying the Area

After seeing the above graph, it is evaluated that there is almost negligible difference when the performance is analyzed with and without malicious node.

7.3 Dropped Packets:

Dropped packets indicate the number of packets that are dropped or do not transfer to the destination node in the network. The effects over the dropped packets are checked out by varying the number of nodes, speed, pause time and area.

a. Variation in number of nodes: When the nodes increases, then the effect will be as shown in the below figure.

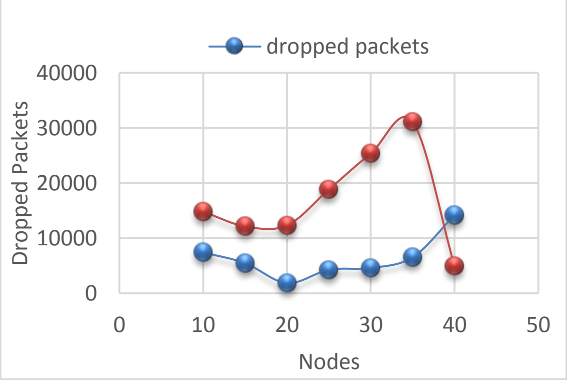

Fig. 11 Dropped Packets by varying the nodes

A huge difference can be seen in the graph. When it is checked that without black hole and with black hole too, how many packets will drop, it is observed that with black hole the number of dropped packets increased with a high margin. As the nodes increase, the value of dropped packets also increases. So it is clear that increasing number of nodes affect a lot to the dropped packets.

b. Varying the speed: Next the evaluation is done to find out how the varying speed affects the dropped packet when the network is available without black hole and after introducing a black hole in the network. The result is shown in the fig. 12.

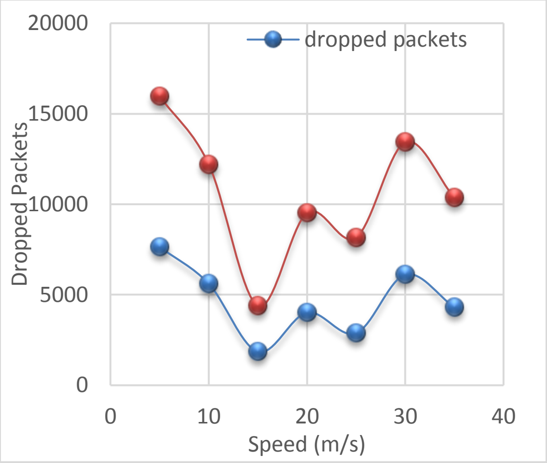

Fig. 12 Dropped Packets by varying the speed

When the comparison is done between the dropped packets without having a black hole in the network and with black hole in the network, the difference is major. The number of dropped packets also varies as the speed varies in both the cases. But the varying value of dropped packets still is more in the network having black hole. Thus it is analyzed that introducing a black hole in the network disturbs the value of dropped packets also.

c. Varying the Pause Time: As like in the case of variation in nodes and speed, the variation in pause time also has a major effect over the dropped packets and it can be easily analyzed by seeing the below given figure.

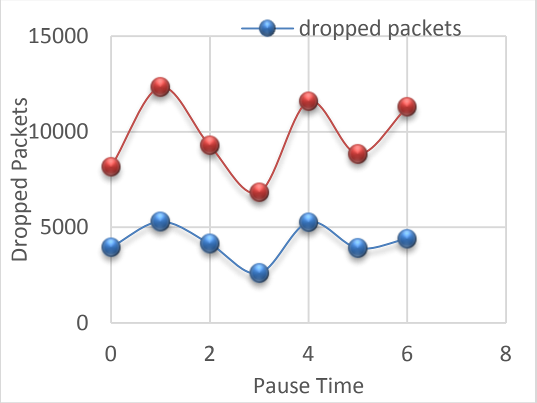

Fig. 13 Dropped Packets by varying the Pause time

As the pause time increases, the number of dropped packets also increases, both in the case of without black hole and with black hole. But as it is shown by the graph, the value increases with a high number when there is a black hole in the network. So when there is a black hole in the network, the dropped packets increases as the pause time increases.

d. Varying the Area: Area also affects the dropped packets but not in that much extent. At the initial level, there is no much difference between without black hole and with black hole. But as the area increases, the value also get differ with a major number as it is shown in the fig.14.

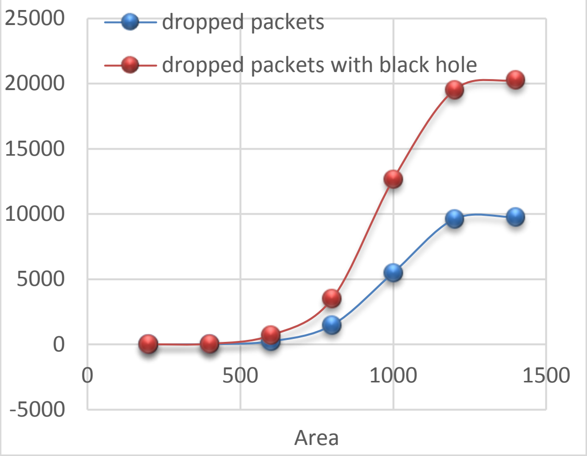

Fig. 14 Dropped Packets by varying Area

The graph shows that when the area is between 200 and 600, the dropped packets level are almost same, but after that when the area increases to 800, the values also increases and when the black hole is introduced in the network, the value increases with a high level. It can be analyzed that increasing the area also increases the number of dropped packets when a black hole is present in the network.

7.4 End to End Delay:

End to End delay is also evaluated by varying various parameters.

a. Varying number of Nodes: By increasing number of nodes, it is evaluated that there is no similarity among the graphs of without black hole and with black hole in the network.

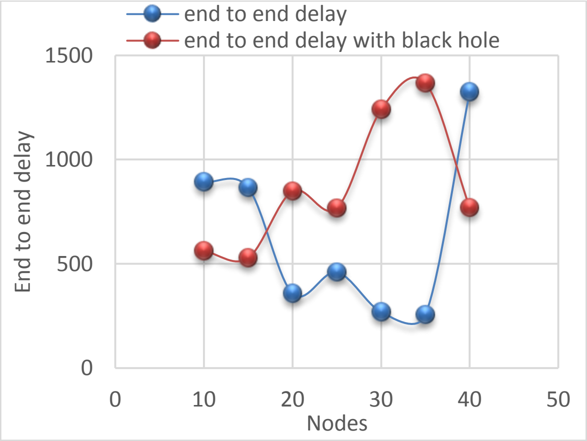

Fig. 15 End to End delay by varying number of nodes

The graph shows that where the delay increases in the network without black hole, at that point it decreases when there is a black hole in the network. Up downs can be seen in the graph. Some time the delay increase and somewhere it decreases in both the cases.

b. <u>Varying the Speed:</u> After varying the speed in the network, the result comes out is as shown below in fig. 16.

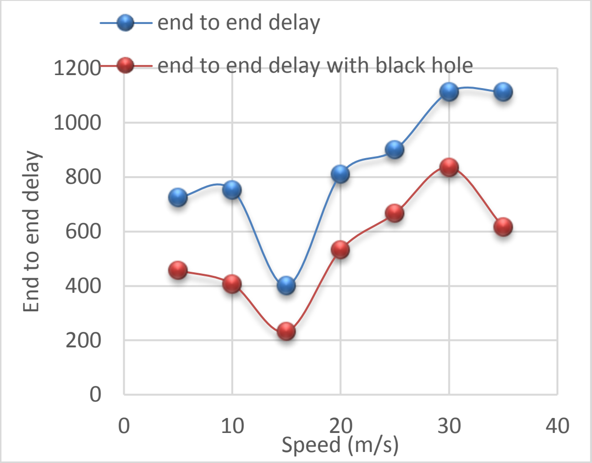

Fig. 16 End to end Delay by varying Speed.

The graph shows that delay goes smooth in both the cases. However it increases when the black hole is present in the network. At on e point, when the speed is about 50, the delay decreases when the black hole is absent in the network and it increases when the black hole is present in the network.

c. <u>Varying the Pause Time:</u> The case is similar as that of varying the speed the difference is given in the fig.17.

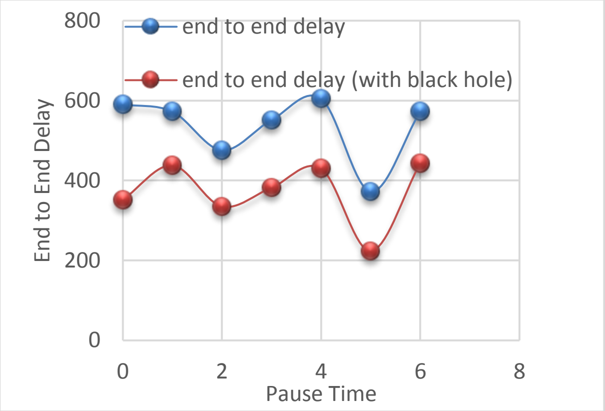

Fig. 17 End to End delay by varying the Pause Time

As it is shown in the figure, the delay goes in the same way in both the parts when black hole is present and when black hole is absent. But the value is high when there is a black hole in the network. There is no overlapping between the two values.

d. <u>Varying the Area:</u> When the area is increased, there is continuous increament and decreamnet in the delay. At some point the delay increases and at some point the delay decreases in both the absence and presence of black hole in the network.

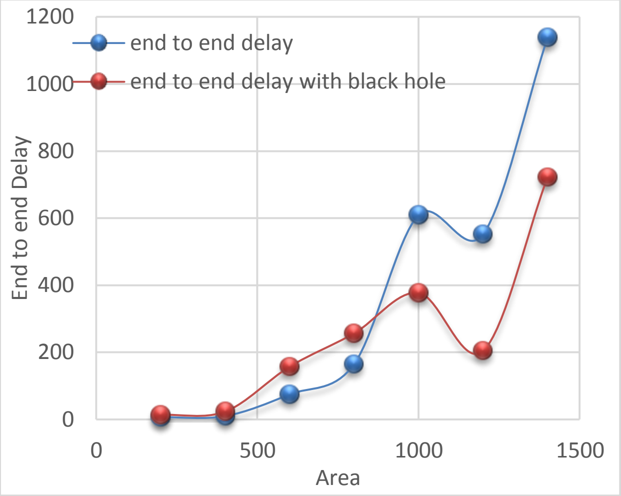

Fig. 18 End to end delay by varying the Area

8. CONCLUSION

In this paper, the analysis of effect of black hole is done in AODV protocol. All the analysis is done by evaluating certain parameters by varying the nodes, pause time, speed and area. The evaluation is done two times; first when there is no black hole in the network and second when there is a black hole in the network, so that the effect of black hole can be easily analyzed. By doing so, the conclusion is made that the variation in speed, nodes and pause time has major effect on the performance of the protocol. However, the increment in area does not have that much effect over the network. Thus it is concluded that not only the presence of black hole but also the variations in certain values also affect the MANET a lot. In future, the prevention from these effects should be done so that variations in nodes, speed and time do not make much effect over the network. In this paper, the comparison is done among various parameters and in future improvement should be done. Future work will consist of the ways to improve it in order to prevent black hole attack to cause much harm to the network and in order to allow the packets to communicate with each other in an attack free environment. After this comparison, the improvement work can be done over it and by this it will become somewhat easy to do work over the improvement of the prevention of the black hole attack in the network.

9. REFERENCES

[1] Ravinder Kaur, Jyoti Kalra, "Detection and Prevention of Black Hole Attack with Digital Signature", Vol.4, Issue 8, August 2014.

[2] T. Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj, "Removal of Selective Black Hole Attack in MANET by AODV Protocol", Vol.3, Issue 3, March 2014.

[3] Jaspinder Kaur, Birinder Singh, "Detect and Isolate Black hole attack in MANET using AODV Protocol", Vol.3, Issue 2, February 2014, IJARCET.

[4] Bala Manju, Kaur Harjeet, SahniVarsha, " Study Of Black Hole Attack using different Routing Protocols in MANET ", Vol. 2, Issue 7 July, 2013.

[5] Akshat Jain, Shekhar Singh Sengar,"Colluding black holes detection in MANET", Vol.2, Issue 1, January 2013, International Journal of Engineering Research & Technology.

[6] Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh rana," Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks", Vol.3, Issue 4, 1395-1399.

[7] Ira Nath, Dr. Rituparna Chaki, "BHAPSC: A new Black Hole Attack Prevention System in clustered MANET", Vol.2, Issue 8, August 2012, International Journal of Advances Research in Computer Science and Software Engineering.

[8] Ekta Barkhodia, Parulpreet Singh, Gurleen kaur walia, "Performance Analysis of AODV using HTTP traffic under Black Hole Attack in MANET ", Vol.2, Issue 3, June 2012

[9] Irshad Ullah, Shoaib Ur Rehman "Analysis of Black Hole attack on MANETs using different MANET Routing Protocols." MEE 10:62, in June, 2010.

[10] Payal N.Raj, Prashant B.Swades, "DPRAODV: A DYNAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET", Vol.2, 2009.

[11] Latha Tamilselvan, Dr. V Sankaranarayanan,"Prevention of co-operative Black Hole Attack in MANET", Vol.3, No.5, May 2008.

[12] Marko Jahnke, Jens Tolle, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", IEEE Computer Society Washington, DC, USA, 2007.

[13] Semih Dokurer "Simulation of Black Hole attack in wireless Ad-hoc Networks" in September 2006.

[14] Hidehisa Nakayama, "Detecting black hole attack on AODV based MANET by dynamic learning method".

[15] Sun, Y. Guan, J. Chen and U.W. Pooch, "Detecting black-hole attack in mobile ad hoc networks", Proc. 5th European Personal Mobile Communications Conference, Apr. 2003, pp. 490-495.