ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
*Vol. 2, Issue 7, July 2013*

# Study of Blackhole Attack Using Different Routing Protocols in MANET

**Harjeet Kaur [1], Manju Bala [2], Varsha Sahni [3]**

M. Tech Student, Dept of CSE, CTIEMT, Jalandhar, India [1]

HOD, Dept. Of CSE, CTIEMT, Jalandhar, India[2]

Assistant Professor, Dept. Of CSE, CTIEMT, Jalandhar, India[3]

**ABSTRACT:** An ad-hoc network (MANET) is set of different types of mobile node. MANET is mobile so they utilize wireless connection to attach with network. MANET can be deployed at low cost in variety of application. In MANET different types of routing protocols have been recommended. These protocols can be classified into three main categories reactive (on-demand), proactive (table-driven) and hybrid routing protocols namely AODV, OLSR and ZRP [1] [2] [3]. This research effort focused first the comparative investigations of routing protocols under the various types of attack then to create scenario and simulate and investigate the performance metrics viz. Packet delivery ratio, average jitter, average throughput and end to end delay of reactive, proactive and hybrid routing protocols such as AODV and AODV with blackhole attack, OLSR and OLSR with blackhole attack and ZRP and ZRP with blackhole attack for the different scenario under the different conditions.

**Keywords:** MANET, Routing protocols AODV, OLSR, ZRP and Blackhole attack.

## I.INTRODUCTION

In today's fast and rapidly growing world of technologies MANET can turn the dream of networking at any place and at time into reality. We are almost there by the way such as Bluetooth enabled mobile phones such as 3G. MANET provides lots of feature and now more and more businesses understand the advantages of usage of computer networking. Depending on the firm's size and resources it might be a small LAN containing only a few dozen computers; however in large corporations the networks can grow to enormous and complex mixture of computers and servers. A computer network is a system for communication between two system and computers. These networks may be fixed (permanent) or temporary. A mobile ad hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless.

The reminder of paper is organised as follow: In Section 2, describes the routing protocols AODV, OLSR and ZRP. Section 3 describes the black hole attack with single and multiple malicious nodes, Section 4 describes the simulation study and results of routing protocols AODV, OLSR and ZRP with attack and without attack using the different performance metrics and Section 5 describes the concluding remarks.

## II.TYPES OF ROUTING

In Ad-hoc networks require multi-hop routing and all nodes can potentially contribute in the routing protocols. Routing is the moving information from a source to a destination in an in network. At least one intermediate node within the internetwork is encountered during the transfer of information. Mainly two activities are involved in this concept: determining optimal routing paths and transferring the packets through an internetwork. The transferring of packets throughout an internetwork is called as packet switching which is straight forward, and the path determination might be very complex. Routing is mainly classified into static routing and dynamic routing. Static routing is the routing strategy being stated manually or statically, in the router. Static routing maintain a routing table usually written by a networks administrator. And dynamic routing is that routing strategy that is being learnt by an interior or exterior routing protocol. This routing depends on the state of the network i.e., the routing table is affected with the activeness of the destination. Routing protocols are organized as:

- Reactive Routing Protocol (AODV)
- Proactive Routing protocol (OLSR)

- Hybrid routing protocol (ZRP)

### *A. AODV:*

AODV perform both unicast and multicast routing and it preserve a path since needed for communication [4].It used route finding procedure and routing tables for maintaining route information [8]. AODV used HELLO, REEQ AND RREP for communication.

| Source_ Address | Source_ Sequence | Broadcast_ Id | Destination_ Address | Destination_ sequence | Hop_ Count |
|---|---|---|---|---|---|

AODV RREQ field

| Source_ Address | Destination_ Address | Destination_ Sequence | Hop_ Count | Lifetime |
|---|---|---|---|---|

AODV RREP field

### *B. OLSR:*

Being a proactive protocol, routes to all destinations within the network are known and maintain before using it. Having the routes available within the standard routing table can be useful for some systems and network applications as there is no route discovery delay associated with finding a new route. The routing operating cost generates, although commonly greater than that of a reactive protocol and does not increase with the number of routes being created. Being a link-state protocol, OLSR requires a reasonably large amount of bandwidth and CPU power to compute optimal paths inside the network. OLSR is a hop by hop table driven or proactive routing protocol. The routes are always all the time at once presented when required suitable to its proactive nature [10]. OLSR used multipoint relay (MPR). MPR are responsible for generating and forwarding topology information. OLSR always need to maintain routing tables. OLSR have three types of control messages, Hello, Topology Control (TC), and Multiple Interface Declaration (MID) [11].

### *C. ZRP:*

ZRP based on the Zone. ZRP was planned to decrease the control overhead of proactive routing protocols and discovery in reactive routing protocols and also decrease the latency caused by route. ZRP is adaptive in nature and it depends on the present organization of network. As the name infer ZRP is base on idea of the zone. A routing zone is different for all nodes, and the zones of closest nodes partially cover one by one [12]. ZRP can be considered like a flat protocol. Zone Routing Protocol consists of various components, which simply jointly offer the full routing advantage of ZRP is that each component work by itself. Components of ZRP are IARP Intra zone Routing Protocol; IERP Inter zone Routing Protocol and BRP Border casts Resolution Protocols.

## III BLACKHOLE ATTACK

Black hole attack is denial of service (DOS) attack in which malicious node send fake information by claiming that it has a fresh or shortest route to destination node and hence source nodes select this shortest path and go through this malicious node and result data misuse or discarded [8]. Once the route is set up, at the moment it’s up to the node whether to drop all the packet or familiar it to the nameless address. This special node, which disappears the data packet, is named as malicious nodes. Black hole attack be an active insider attack. Black hole has two main properties. First the node announces itself when having a suitable route to a destination node and second one the node consumes the intercepted packets.

## IV. SIMULATION AND RESULTS

We have used Network Simulator Qualnet5.1 in our evaluation. In our scenario we simulate 50 nodes and it distributes over 1500*1500 Terrain areas in Qualnet5.1 Simulator using CBR traffic and by applying 30 sec simulation duration in MAC Layer 802.11. Random way point is random based model used for communication. Random way point model is designed to describe the movement pattern of mobile users which includes their location, acceleration and mobility change over time. Under the blackhole attack different performance parameter like Packet Delivery Ratio, Average Jitter, Average Throughput and Average End to End Delay, In this part we discussed the scenario of

routing protocol AODV with blackhole attack, OLSR with blackhole attack and ZRP with the blackhole attack and using the performance metrics packet delivery ratio, average jitter, average throughput and end to end delay.
TABLE 1

TABLE 1 SIMULATION PARAMETERS

| **Parameters** | **Values** |
|---|---|
| Routing Protocols | AODV, OLSR, ZRP |
| MAC Layer | 802.11 |
| Packet Size | 512 Bytes |
| Terrain Size | 1500*1500 |
| Nodes | 50 |
| Mobility Model | Random Waypoint Model |
| Data Traffic Rate | CBR |
| No. of Source | 5,10,15,20,25,30 |
| Simulation duration | 30 sec |
| CBR Traffic Rate | 8 packet/sec |
| Maximum Speed | 0-20 m/sec (30 sec pause time) |
| Attack Type | Blackhole Attack |

**A Case 1 Comparative analysis of performance of AODV and AODV with blackhole attack**

**A.1 Packet Delivery Ratio of AODV and AODV with blackhole attack** In AODV protocol if many nodes are sending and receiving data traffic simultaneously placing more malicious node uniformly causes severe damage because it increases the probability of route affected malicious node. As show in fig 1, when there is no malicious node packet delivery ratio is more, there is very less probability that any route involve malicious node and Packet Delivery Ratio decreases as the malicious node added to the scenario. So AODV without attack has more packet delivery ratio than AODV with blackhole attack.

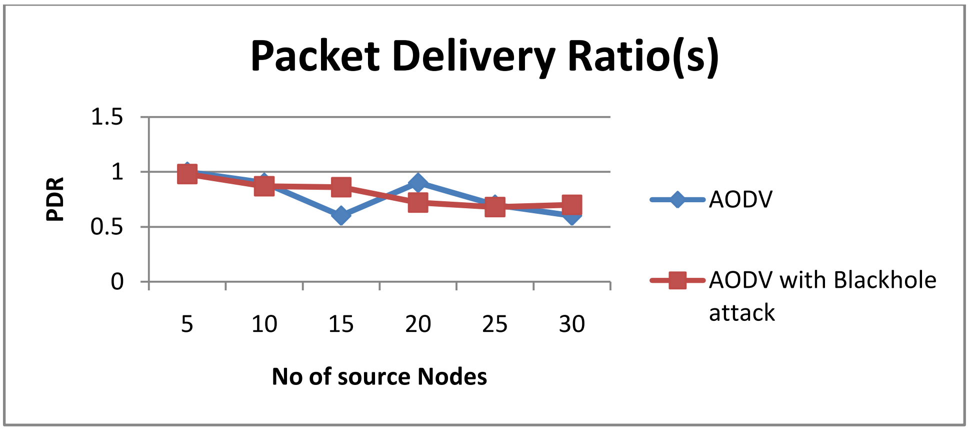

Fig 1 Packet Delivery Ratio of AODV and AODV with blackhole attack

**A.2 Average Jitter of AODV and AODV with blackhole attack** Jitter is another significant application layer parameter in ad hoc network especially in case where quality of service is required. Study of blackhole attack effect on jitter in AODV protocol in fig 2 shows that when the malicious node added, Jitter increase as compare to network without any malicious node. This is because when there is no malicious node than there is no route affected by this malicious node which causes less delay. Another important characteristic can be seen from this fig 2 that in case of no malicious nodes in network jitter increases as node mobility speed increases. When we increase number of malicious node from 3 to 4 there is a significant increase in jitter as compared to AODV without malicious node. So it clearly observed that AODV with blackhole attack has more jitter as compared to AODV.

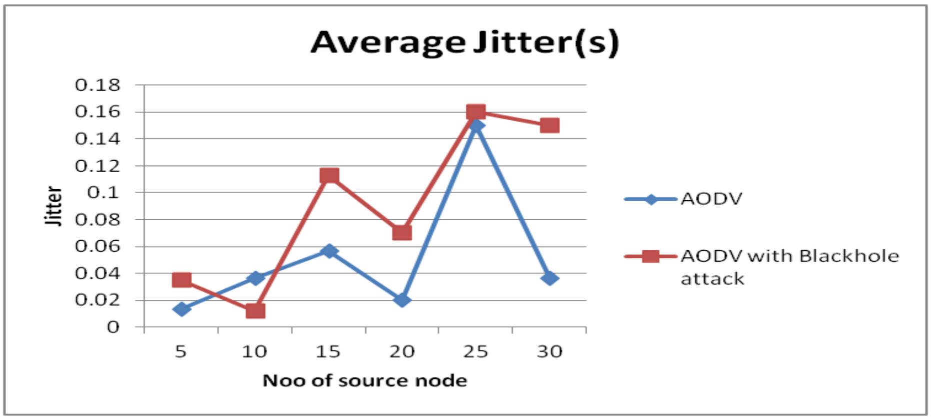

Fig 2 Average Jitter of AODV and AODV with blackhole attack

**A.3 Average Throughput of AODV and AODV with blackhole attack** fig 3 shows that AODV outperform AODV with blackhole attack when we compare throughput. In case of AODV with blackhole attack there is no significant difference in average throughput as the number of source nodes increases, when no malicious nodes are placed in network. When we add the number of malicious nodes in the network throughput in the presence of these malicious nodes or attack is decreases suddenly. Fig 3 shows that AODV has more throughput than AODV with blackhole attack.

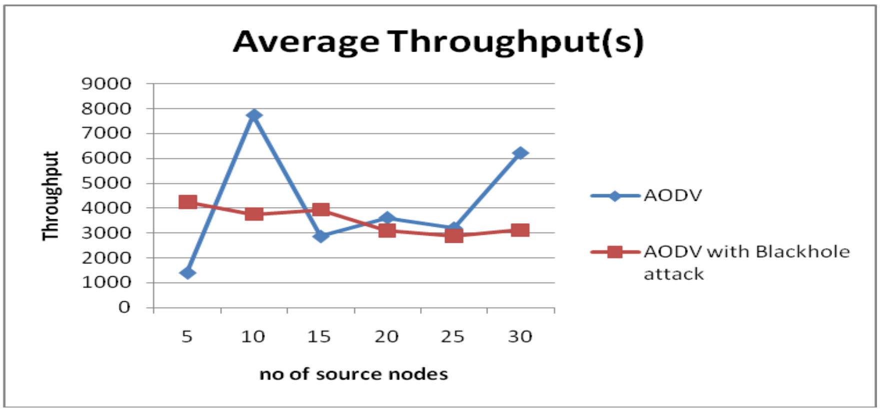

Fig 3 Average Throughput of AODV and AODV with blackhole attack

**A.4 End to End Delay of AODV and AODV with blackhole attack** fig 4 shows that Average End to End Delay does not get affected by the attack much when number of malicious nodes is less also there is small change in End to End Delay. However there is a significant increase in average End to End Delay when number malicious node are high and there is a negative relationship between End to End Delay and number of source nodes. So when we compare the AODV and AODV with blackhole attack with respect to end to end delay AODV with blackhole attack has more delay than AODV.

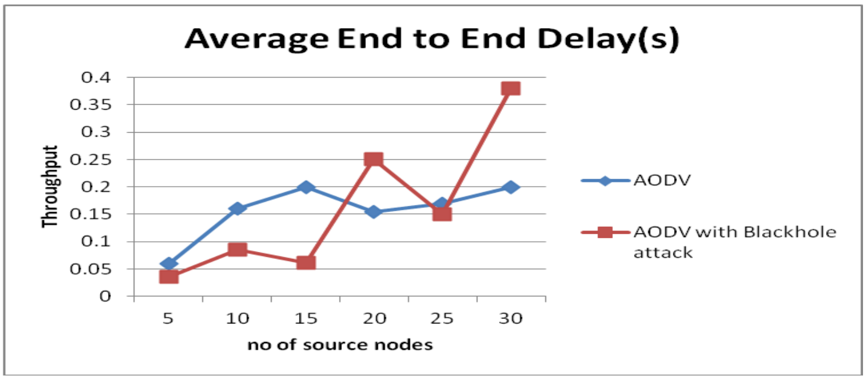

Fig. 4 End to End Delay of AODV and AODV with blackhole attack

**B Case 2 Comparative analysis of performance of OLSR and OLSR with blackhole attack**

**B.1 Packet Delivery Ratio of OLSR and OLSR with blackhole attack** Fig 5 shows that, when there is no malicious node packet delivery ratio is more, there is very less probability that any route involve malicious node and Packet Delivery Ratio decreases as the malicious node added to the network. But once the number of malicious node increases a particular level and it placed uniformly all over network effect of attack become severe. So OLSR without attack has more packet delivery ratio than OLSR with blackhole attack, as the number of source nodes increases OLSR decreases and OLSR with blackhole attack increases.

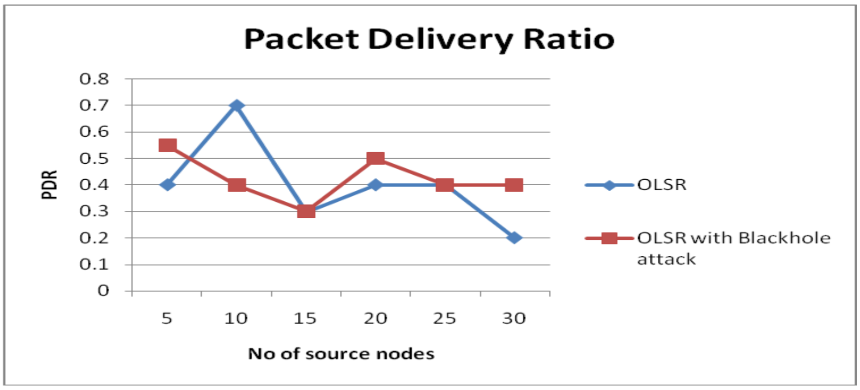

Fig. 5 Packet Delivery Ratio of OLSR and OLSR with blackhole attack

**B.2 Average Jitter of OLSR and OLSR with blackhole attack** fig 6 shows that, Study of blackhole attack effect on jitter in OLSR protocol when the malicious node added, Jitter increase as compare to network without any malicious node. this is because when number of malicious nodes are less than number of route affected by these malicious node are also low which cause less delay. Another important characteristic can be seen from this fig 6 that in case of malicious nodes in network jitter increases as the number of source nodes increases. When we increase number of malicious node increases 3 or 4 there is a significant increase in jitter as compared to OLSR without malicious node. So it clearly observed that OLSR with blackhole attack has more jitter as compared to OLSR.

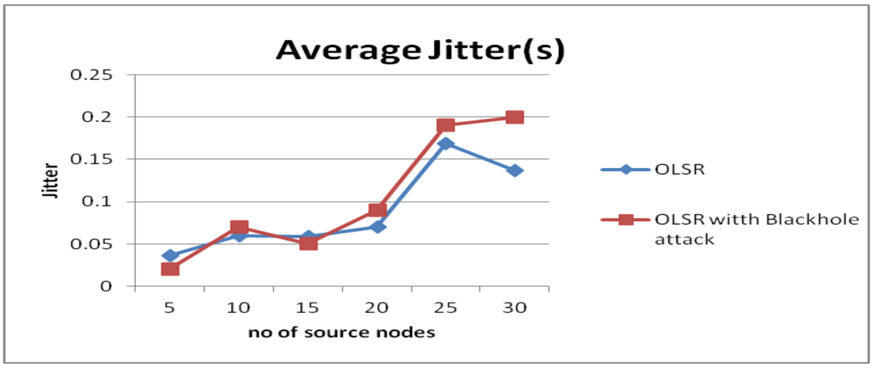

Fig. 6 Average Jitter of OLSR and OLSR with blackhole attack

**B.3 Average Throughput of OLSR and OLSR with blackhole attack** fig 7 shows that, OLSR perform better OLSR with blackhole attack when we compare throughput. In case of OLSR with blackhole attack there is no significant difference in average throughput as the number of source nodes increases, when no malicious nodes are placed in network but as the malicious nodes are added in the network throughput decreases gradually as compared to the OLSR without malicious nodes. Figure shows that OLSR has more throughput than OLSR with blackhole attack.

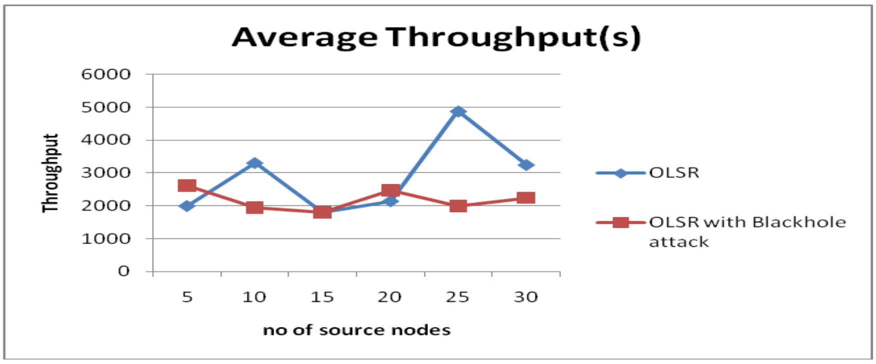

Fig. 7 Average Throughput of OLSR and OLSR with blackhole attack

**B.4 End to End Delay of OLSR and OLSR with blackhole attack** fig 8 shows that, Average End to End Delay does not get affected by the attack much when number of malicious nodes are less also these is small change in End to End Delay. However there is a significant increase in average End to End Delay when number malicious node are high and there is a negative relationship between End to End Delay and number of source nodes. So when we compare the OLSR and OLSR with blackhole attack with respect to end to end delay OLSR with blackhole attack has more delay than OLSR.

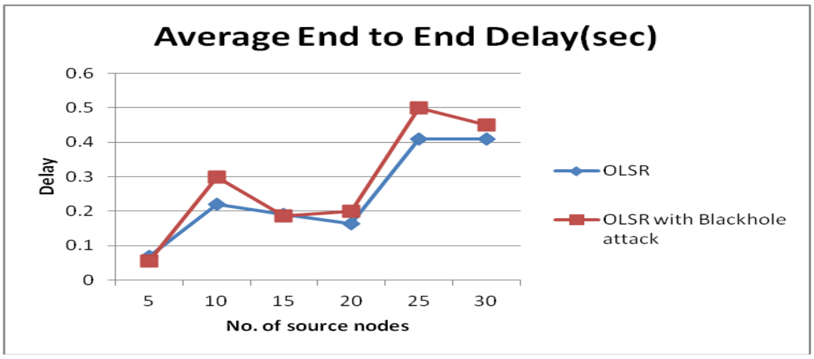

Fig. 8 End to End Delay of OLSR and OLSR with blackhole attack

### C Case 3 Comparative analysis of performance of ZRP and ZRP with blackhole attack

**C.1 Packet Delivery Ratio of ZRP and ZRP with blackhole attack** Fig 9 shows that, when there is no malicious node packet delivery ratio of ZRP is more, there is very less probability that any route involve malicious node and Packet Delivery Ratio decreases as the malicious node added to the network. But once the number of malicious node increases a particular level and it placed uniformly all over network effect of attack become severe. So OLSR without attack has more packet delivery ratio than OLSR with blackhole attack, as the number of source nodes increases OLSR decreases with small variation but at the end again ZRP has more packet delivery ratio than ZRP with blackhole attack.

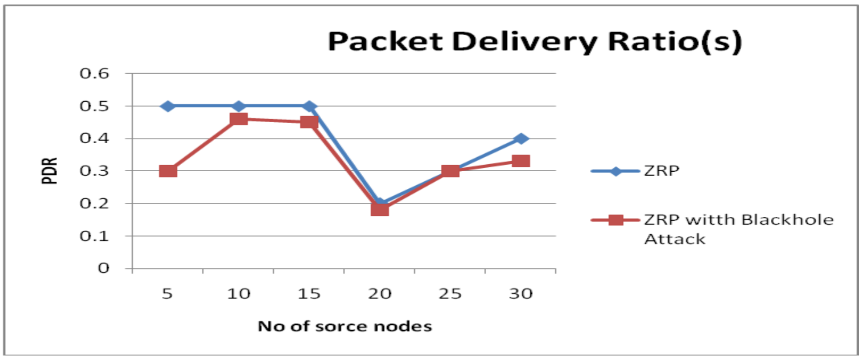

Fig. 9 Packet Delivery Ratio of ZRP and ZRP with blackhole attack

**C.2 Average Jitter of ZRP and ZRP with blackhole attack** Fig 10 shows that, blackhole attack effect on jitter in ZRP protocol when the malicious node added, Jitter increase as compare to network without any malicious node. this is because when number of malicious nodes are less than number of route affected by these malicious node are also low which cause less delay. When we increase number of malicious node increases 3 or 4 there is a significant increase in jitter as compared to ZRP without malicious node. So it clearly observed that ZRP with blackhole attack has more jitter as compared to ZRP.

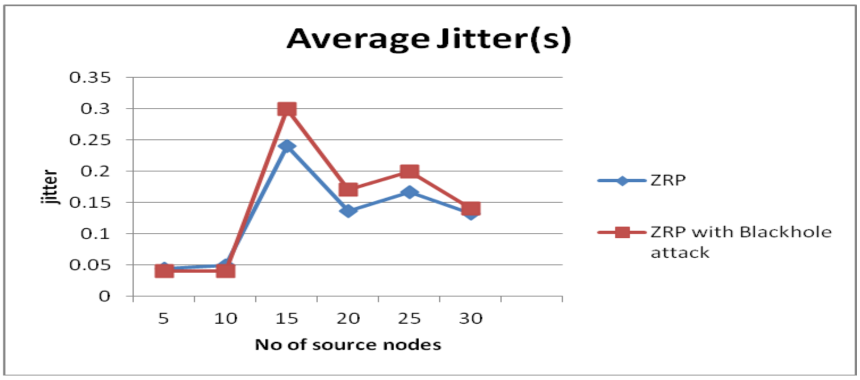

Fig. 10 Average Jitter of ZRP and ZRP with blackhole attack

**C.3 Average Throughput of ZRP and ZRP with blackhole attack** fig 11 shows that, ZRP perform better than ZRP with blackhole attack when we compare Throughput. In case of ZRP with blackhole attack there is only small difference in throughput as the number of source nodes increases, when no malicious nodes are placed in network. As the malicious nodes add in the network throughput of ZRP with blackhole attack is decreases. Figure shows that ZRP has more throughput than ZRP with blackhole attack.

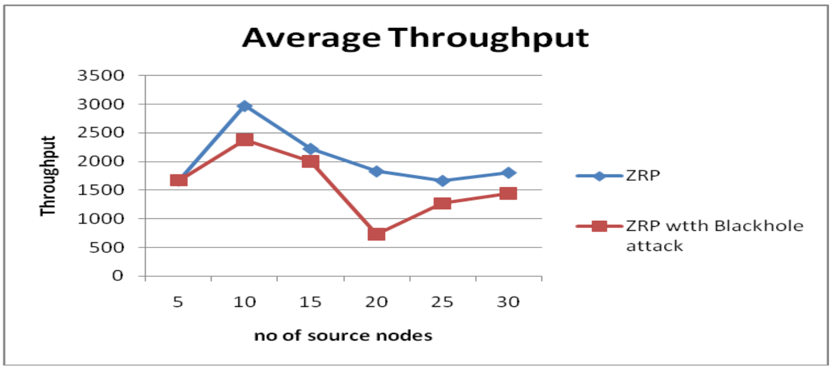

Fig. 11 Average Throughput of ZRP and ZRP with blackhole attack

**C.4 End to End Delay of ZRP and ZRP with blackhole attack** fig 12 shows that, Average End to End Delay does not get affected by the attack much when number of malicious nodes are less also these is small change in End to End Delay. However there is a significant increase in average End to End Delay when number malicious nodes are high. So when we compare the ZRP and ZRP with blackhole attack with respect to end to end delay ZRP with blackhole attack has more delay than ZRP.

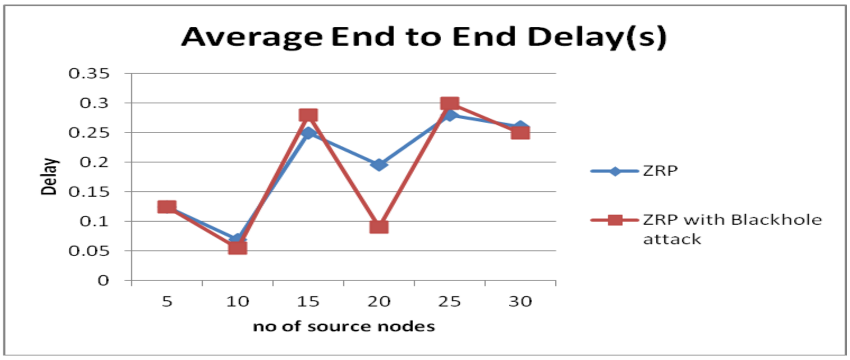

Fig. 12 End to End Delay of ZRP and ZRP with blackhole attack

## V. CONCLUSION AND FUTURE SCOPE

In the performance evaluation of AODV and AODV with blackhole attack, OLSR and OLSR with blackhole attack and ZRP and ZRP with blackhole attack under the performance metrics packet delivery ratio, average jitter, average throughput and end to end delay. From these result it evaluate that AODV with blackhole attack have less impact of the number of malicious nodes, it have high packet delivery ratio and throughput and less jitter and delay in the presence of malicious nodes and absence of the malicious nodes. Another hand OLSR and ZRP also have more impact on the performance in the presence of the malicious nodes as compared to AODV. So it concludes that AODV with malicious nodes and without malicious nodes is performs better in above every case.

## REFRENCES

[1] Pradish Dadhania, Sachin Patel “Performance Evaluation of Routing Protocol like AODV and DSR under Black Hole Attacks” in International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 1, pp.1487-1491, January - February 2013.

[2] Arunima Patel, Sharda Patel, Ashok Verma “A Review of performance Evaluation of AODV Protocol in Manet With and Without Black Hole Attack” International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, Volume 2, Issue 11, November 2012.

[3] Nadia Qasim, Fatin Said, and Hamid Aghvami, “Performance Evaluation of Mobile Ad Hoc Networking Protocols” Chapter 19, pp. 219-229.

[4] Prem Chand and MK Soni “Performance Comparison of AODV and DSR on-Demand Routing Protocols for Mobile Ad-Hoc Networks” International Journal of Computer Applications ISSN 0975 – 8887 Volume 49– No.18, July 2012.

[5] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala “DoS Attacks in Mobile Ad-hoc Networks: A Survey” 2012 Second International Conference on Advanced Computing & Communication Technologies.

[6] Harmandeep Singh, Gurpreet Singh and Manpreet Singh “Performance Evaluation of Mobile Ad Hoc Network Routing Protocols under Black Hole Attack” International Journal of Computer Applications ISSN 0975 – 8887 Volume 42– No.18, March 2012.

[7] Ashok M.Kanthe, Dina Simunic and Ramjee Prasad “Comparison of AODV and DSR On-Demand Routing Protocols in Mobile Ad hoc Networks” Emerging technology Trends in Electronics, communication and networking, © IEEE 2012 First international Conference ISBN 978-1-4673-1628-6.

[8] Vinay P.Virada “Securing And Preventing Aodv Routing Protocol From Black Hole Attack Using Counter Algorithm” International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012 ISSN: 2278-0181.

[9] Ashish Bagwari, Raman Jee,Pankaj Joshi and Sourabh Bisht “ Performance of AODV Routing Protocol with increasing the MANET Nodes and it’s effects on QoS of Mobile Ad hoc Networks ” 2012 International Conference on Communication Systems and Network Technologies 978-0-7695-4692-6/12 © 2012 IEEE.

[10] Naveen Bilandi, Harsh K Verma “Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET” International Journal of Electronics and Computer Science *Engineering* 1660 ISSN- 2277-1956.

[11] Irshad Ullah and Shoaib Ur Rehman “Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols” Master Thesis Electrical Engineering June, 2010 Thesis no: MEE 10:62.

[12] Himani Yadav and Rakesh Kumar “Identification and Removal of Black Hole Attack for Secure Communication in MANETs” *I*nternational *J*ournal of *C*omputer *S*cience and *T*elecommunications [Volume 3, Issue 9, September 2012] ISSN 2047-3338”.

[13] Scalable Network Technologies (SNT). *QualNet*. http://www.qualnet.com/.