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

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 6, June 2013

PERFORMANCE EVALUATION OF AODV, OLSR and ZRP ROUTING PROTOCOLS UNDER THE BLACK HOLE ATTACK 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: The wireless mobile ad-hoc network (MANET) is set of dissimilar types of mobile nodes. These nodes in MANET communicate with each other without any fixed infrastructure. Because of MANET's infrastructure network is unprotected from the attacks of malicious nodes. One of the attacks is called black hole attack. In MANET black hole attack is occurring easily. In the black hole attack node falsie advertises that they have secure path to destination and absorb the data packet. Nodes those drop or misuse the data are called malicious nodes. This paper focus to analyzed the performance of reactive (AODV), proactive (OLSR) and hybrid (ZRP) routing protocols with blackhole attack and without blackhole attack using different performance metrics like Packet Delivery Ratio, Average Jitter, Average Throughput and Average End to End Delay. The simulation study of ad-hoc routing protocols in MANET is done with Qualnet5.1 simulator.

Keywords: Wireless Mobile ad hoc network (MANET), AODV, OLSR, ZRP, Black hole attack and Performance Metrics.

I. INTRODUCTION

MANET is called as wireless ad-hoc network in which nodes are free to move anywhere and be capable of transmit and receive traffic and communication link broken at any moment [1]. MANET has some attributes like simplicity of use, continually changing topology, wireless connection and distributed operations [2]. MANET was planned only for military use in the beginning, but now the MANET used in several areas like electronic payments, virtual classrooms, video conferences, meetings, rescue systems, automated battlefields, voting systems, offices and vehicular computing [1,3]. Mobile nodes use radio transmits medium for message sending. It is a self-organized network. Mobile nodes in wireless network can communicate with one other in specific range [1]. MANET has some feature like Mesh network, dynamic topology, highly adaptable and rapidly deploy-able network. The most important objective of these networks in real-life networks to carry the idea of mobility is interested [2].

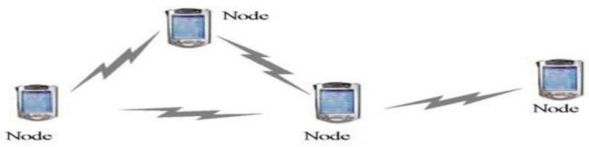

Fig 1 MANET [2]

The reminder of paper is organised as follow: In Section 2, describes the routing protocols Reactive (AODV), Proactive (OLSR) and Hybrid (ZRP) routing protocols. Section 3 describes the black hole attack with single and multiple malicious nodes, Section 4 describes simulation 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. ROUTING IN MANET

The process of sending and receiving data from one node to another is done with the help of routing protocols [4]. In MANET each node works as router. Sender and receiver be capable of communicate, if and only if they are inside the communicate range beside sender has sent the message through the nodes [5]. The chief goal in ad-hoc network is to create an accurate and capable route among couples of nodes and to make sure that the proper and timely release of packets [4]. The routing protocols for MANET can be categorized into three types according to procedure used for route discovery and route maintenance [2]: reactive or on-demand, proactive or table driven and hybrid routing protocols combination of both reactive and proactive routing protocols [4].

A.REACTIVE ROUTING PROTOCOLS

Reactive Routing protocols are on demand routing protocols in which route is required, when its demand for the data packets [6]. At any time, if source wants to send message to receiver, then the protocol create a path as soon as when demand for the route. Ad hoc On-Demand Distance Vector Routing (AODV), Cluster based Routing Protocols (CBRP) and Dynamic Source Routing Protocol (DSRP) are On-Demand Routing protocols [2].

1. AODV

AODV have some combine properties of DSR and DSDV. It is based on Bellman-ford Distance Algorithm. AODV always discover a route source to destination only on-demand [7]. It used route finding procedure and routing tables for maintaining route information [8]. AODV used REEQ AND RREP for communication. A RREQ holds the senders' address, the address of the wanted node and the last sequence number inward starting that node, if there is present one. The receipt node checks if it has a route to the particular node, if there exists a route and the sequence-number to set up a fresh route. The node response to the requesting by transfer a route replies (RREP). But on the other hand supply a route does not stay alive the receipt node sends a RREQ itself to attempt to discover a route for the request node [9]. AODV perform both unicast and multicast routing and it preserve a path while needed for communication [4].

B. PROACTIVE ROUTING PROTOCOLS

Proactive Routing protocols are table driven and there is require retaining regular up-to-date routing information about the every node inside the network and it stores the entire information within route table in the type of cache [6]. Destination Sequenced Distance Vector (DSDV) routing protocol, Global State Routing (GSR), Wireless Routing Protocol (WRP), Zone Based Hierarchical Link State Routing Protocol (ZHLS) and Clustered Gateway Switch Routing Protocol (CGSR) are table driven routing protocols [7].

1. OLSR

OLSR is a hop by hop proactive routing protocol. It is optimizations of clean connections state algorithm in ad hoc networks. 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 has three types of control messages, Hello, Topology Control (TC), and Multiple Interface Declaration (MID) [11].

1. a. Hello: OLSR makes use of "Hello" messages to find it is one hop neighbours and it is two hop neighbours through their responses. This control message is transmitted for sense the neighbour and used for MPR calculation.

1. b. Topology Control: OLSR uses topology control (TC) messages along with MPR forwarding to disseminate neighbour information throughout the network.

1. c. Multiple Interface Declaration: MID message includes the record of every IP addresses use by every node in the network. Every single nodes running on OLSR broadcast messages on extra than single interface.

1. d. Multi Point Relaying: MPR are used nodes to transmit route message. The choice of MPR is base on HELLO communication send between the neighbour nodes.

C. HYBRID ROUTING PROTOCOLS

Hybrid routing protocol have both the combines feature of Reactive and Proactive Routing protocols [6]. It decreased the latency in reactive protocol and reduce the control overhead of proactive routing protocols. This protocol is based on hierarchical or layered system structure. Temporally ordered routing algorithm (TORA) and Zone routing protocol (ZRP) are Hybrid routing protocols [7].

1. ZRP

The Zone Routing protocols combine the feature of both reactive and proactive protocol into Hybrid Routing Protocol [13]. 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 distinct for all nodes, and the zones of adjacent nodes partially cover one by one [12]. ZRP can be considered like a flat protocol. Zone Routing Protocol consists of numerous components, which simply jointly offer the full routing advantage of ZRP, each's component work by itself. Components of ZRP are: IARP, IERP and BRP.

1. a. ARP: The first protocol of ZRP is the IARP (Intra zone Routing Protocol). This protocol is used to communicate through the inner nodes of its zone and is partial by the zones radius suitable to differ in topology, limited neighbourhood of a node can modify rapidly. This node always desires to update the routing information [13]. IARP protocol is use indoor routing zones [14].

1. b. IERP: Inter zone Routing Protocol is global reactive routing component of the ZRP, the Inter zone Routing Protocol takes gain of the well-known local topology of a node's zone and using a reactive move towards enables communication using nodes in previous zones [13]. In Reactive routing protocol IERP is used among routing zones [14].

1. c. BRP: The Border casts Resolution Protocol is used in the ZRP to nonstop the route requests start with the global reactive IERP to the minor nodes and removing disused queries and maximize effectiveness [13]. It uses the Intra zone routing information provided by IARP to create a border cast tree.

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 disappear the data packet, is named as malicious nodes. Black hole attack be an active insider attack. Black hole has two properties. First the node announces itself when having a suitable route to a destination node and second one the node consumes the intercepted packets [15].

Black hole Attacks are categories as:-

- Single Blackhole Attack
- Collaborative Blackhole Attack

A. Single Blackhole Attack [12]

Single Blackhole Attack in which one node acts as malicious node which drops all the data. Single black hole attack is also known as Black Hole Attack with single malicious node.

B. Collaborative Blackhole Attack [12]

Collaborative Blackhole Attack in which many nodes in a group's act as malicious nodes and these nodes misuses or destroys the data traffic. Collaborative black hole attack is also known as Black Hole Attack by multiple malicious nodes.

IV. SIMULATION AND RESULTS

In our scenario we simulate 50 nodes and it distributes over 1500*1500 Terrain areas in Qualnet5.1 Simulator using CBR traffic and MAC Layer 802.11 and by applying 30 sec simulation duration. Random way point is random based model used for communication. This designed to describe the movement pattern of mobile users which includes their location, acceleration and mobility change over time.

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
Attack Type	Blackhole Attack

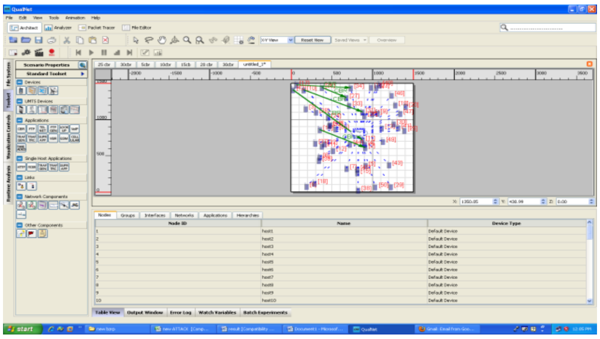

Fig 2 Scenarios in Qualnet5.1 Simulator

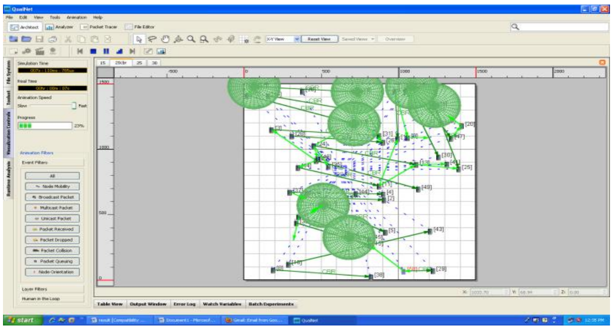

Fig 3: Running Simulation in QualNet5.1 Simulator

A. Performance Metrics: We have used the Packet Delivery Ratio, Jitter, Throughput and End to End Delay for measuring the performance of Reactive (AODV), Proactive (OLSR) and Hybrid (ZRP) Routing protocols.

1. Packet Delivery Ratio (PDR): PDR is determined by dividing the number of packets received by the destination through the number of packets originates by the application layer of the source [15].

PDR = (Total Packet received / Total Packet sent)*100

2. Average Jitter (bits/sec): It Signifies the Packets from the source will reach the destination with dissimilar delays. A packet's wait varies with its location in the queues of the routers along the path between source and destination and this position can varies unpredictably [15].

3. Throughput: It is calculated by number of packets successfully transmitted to their final destination per unit time [15].

4. Average End to End Delay: It signifies the average time has taken by packets to reach one end to another end (Source to Destination).

D = (Tr –Ts) Where Tr is received Time and Ts is sent Time [15].

B Case 1: COMPARISON OF AODV, OLSR AND ZRP

First we compare the performance of AODV, OLSR and ZRP using the performance metrics Packet Delivery Ratio, Average Jitter, Average Throughput and End to End Delay are shown in fig 4, fig 5, fig 6 and fig 7.

1. Packet Delivery Ratio: Fig 4 shows the Packet Delivery Ratio of AODV, OLSR and ZRP. In case of low traffic 5-30 no. Of source nodes and by placing 50 nodes AODV perform better, but Packet Delivery Ratio starts decreases as the number of source nodes increases. OLSR and ZRP perform less efficiently. Both OLSR and ZRP have similar values of Packet Delivery Ratio with small variation.

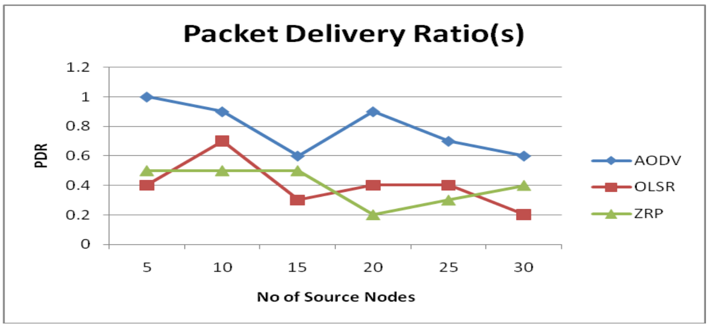

Fig 4: Packet Delivery Ratio Vs No. of source nodes

2. Average Jitter: Fig 5 shows the Average Jitter of ZRP is always high because of framework of ZRP. OLSR has more jitter as compared to AODV. AODV has less jitter, but as the number of source nodes increases 20-25 delay is also increases, but AODV has less jitter than both another protocols.

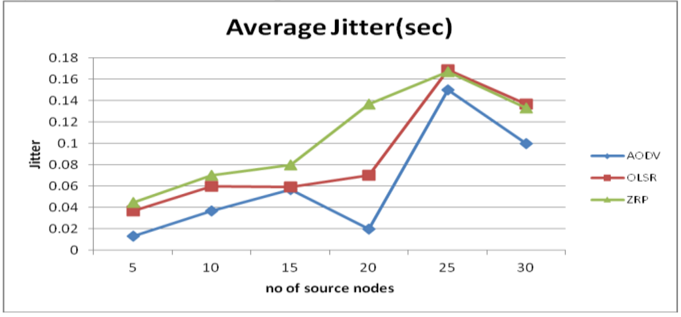

Fig 5: Average Jitter Vs No. of source nodes

3. Average Throughput: Fig 6 shows that throughput of AODV is greater than another routing protocol. OLSR and ZRP have almost similar throughput with small variations. AODV has less overhead comparison to OLSR and ZRP routing protocols. AODV performed better than OLSR and ZRP.

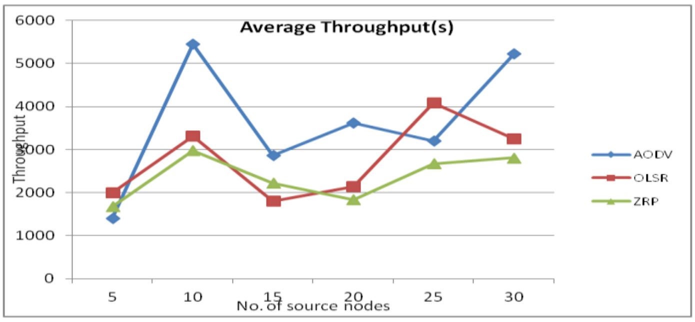

Fig 6: Average Throughput Vs No. of source nodes

4. Average End to End Delay: Fig 7 shows that both OLSR and ZRP have more delay. Because of nature of AODV, it has less connection setup delay than both OLSR and ZRP. As the number of source nodes increases end to end delay is also increases in AODV, OLSR and ZRP routing protocols. But AODV has less end to end delay than OLSR and ZRP.

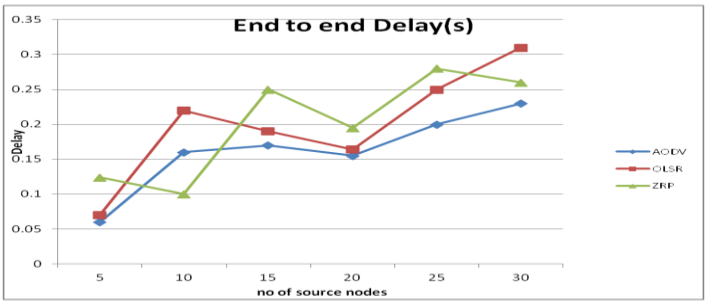

Fig 7: Average End to End Delay Vs No. of source nodes

C Case II: COMPARISON OF AODV with blackhole attack, OLSR with blackhole attack and ZRP with blackhole attack

We compare the performance of AODV with blackhole attack, OLSR with blackhole attack and ZRP with blackhole attack using the Blackhole attack with performance metrics packet delivery ratio, average jitter, average throughput and end to end delay are shown in fig 8, fig 9, fig 10 and fig 11.

1. Packet Delivery Ratio with blackhole attack: Fig 8 shows that Packet Delivery Ratio of AODV with blackhole attack is less than AODV without attack in the presence of malicious node, OLSR with blackhole attack than OLSR without attack and ZRP with blackhole attack than ZRP without attack. So it observes that blackhole attack decrease the performance of routing protocols because these malicious nodes drop the data packets.

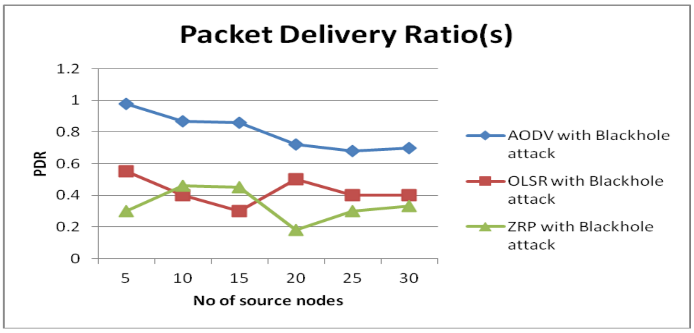

Fig 8: Packet Delivery Ratio Vs No. of source nodes with attack

2. Average jitter with blackhole attack: fig 9 shows the average jitter of AODV with blackhole attack is also less. In terms of delay the performance of OLSR with blackhole attack improves with the fewer number of source nodes because of its nature (table driven). It maintains up-to-date routing information from each node to every other node in the network and ZRP with blackhole attack has more jitter as compared to ZRP without attack.

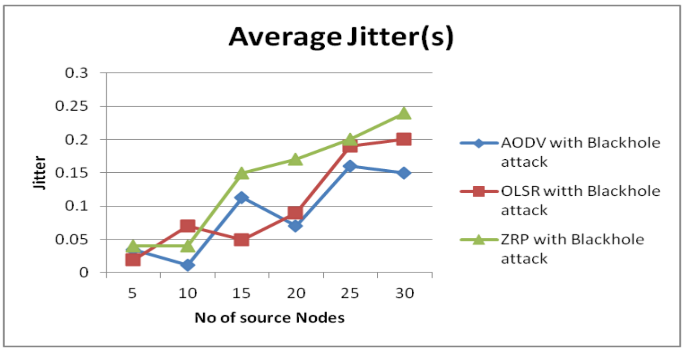

Fig 9: Average Jitter Vs No. of source nodes with attack

3. Average Throughput with blackhole attack: Fig 10 shows it is obvious that the throughput for AODV is high compared to that of OLSR and ZRP, also in AODV, without attack, its throughput is higher than in the case with attack because of the packets discarded by the malicious node, Here the malicious node discards the data rather than forwarding it to the destination, thus effecting throughput. The same is seen in the case with OLSR throughput with no attack is higher than the throughput of OLSR under attack and same is observed in ZRP.

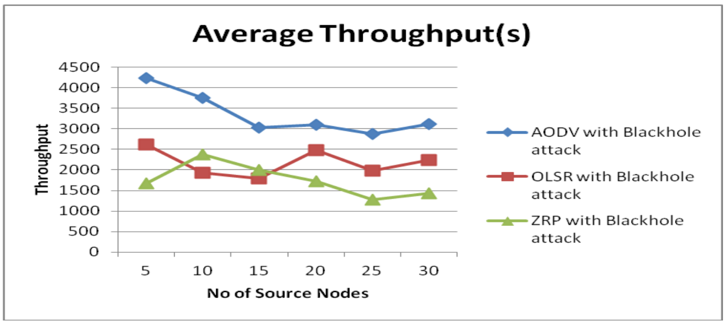

Fig 10: Average Throughput Vs No. of source nodes with attack

4. Average end to end delay with blackhole attack: in case of end to end delay in Fig 11 shows that OLSR with blackhole attack and ZRP with blackhole attack have high end to end delay in presence of a malicious node as compare to that of AODV with blackhole attack. As the routing protocols are able to adjust its changes in it during node restart and node pausing. As the number of source node increases end to end delay is also increases in routing protocols.

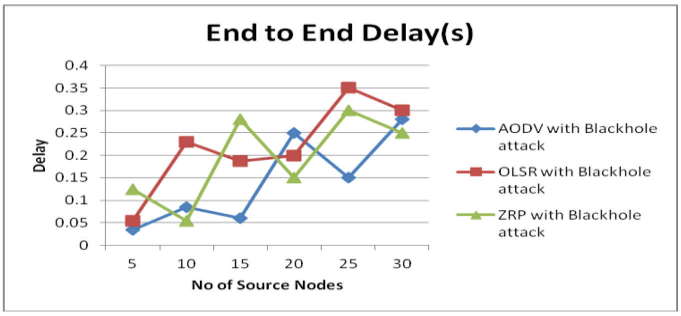

Fig 11: Average End to End Delay Vs No. of source nodes with attack

TABLE 2
Packet Delivery Ratio of AODV and AODV with Blackhole attack, OLSR and OLSR with Blackhole attack and ZRP and ZRP with Blackhole attack

S. No	No. of Source Nodes	AODV	AODV With attack	OLSR	OLSR with attack	ZRP	ZRP with attack
1	5	1	0.98	0.4	0.55	0.5	0.3
2	10	0.9	0.87	0.7	0.4	0.5	0.46
3	15	0.6	0.86	0.3	0.3	0.5	0.45
4	20	0.9	0.72	0.4	0.5	0.2	0.18
5	25	0.7	0.68	0.4	0.4	0.3	0.3
6	30	0.6	0.7	0.2	0.4	0.4	0.33

TABLE 3
Average Jitter of AODV and AODV with Blackhole attack, OLSR and OLSR with Blackhole attack and ZRP and ZRP with Blackhole attack

S.No	No. of Source Nodes	AODV	AODV With attack	OLSR	OLSR with attack	ZRP	ZRP with attack
1	5	0.13	0.03	0.036	0.02	0.044	0.04
2	10	0.03	0.01	0.06	0.07	0.07	0.04
3	15	0.056	0.113	0.059	0.05	0.08	0.15
4	20	0.02	0.07	0.07	0.09	0.137	0.17
5	25	0.15	0.16	0.16	0.19	0.16	0.2
6	30	0.1	0.15	0.13	0.2	0.13	0.24

TABLE 4
Average Throughput of AODV and AODV with Blackhole attack, OLSR and OLSR with Blackhole attack and ZRP and ZRP with Blackhole attack.

S.No	No.of Source nodes	AODV	AODV With attack	OLSR	OLSR with attack	ZRP	ZRP with attack
1	5	1402	4240	1998	2612	1671	1671
2	10	5448	3752	3307	1936	2974	2380
3	15	2865	3029	1798	1798	2225	1998
4	20	3619	3107	2142	2474	1830	1729
5	25	3198	2876	4079	1987	2665	1269
6	30	5227	3114	3247	2240	2807	1439

TABLE 5
Average end to end delay of AODV and AODV with Blackhole attack, OLSR and OLSR with Blackhole attack and ZRP and ZRP with Blackhole attack

S.No	No.of Source nodes	AODV	AODV With attack	OLSR	OLSR with attack	ZRP	ZRP with attack
1	5	0.06	0.035	0.07	0.05	0.124	0.124
2	10	0.16	0.085	0.22	0.23	0.1	0.055
3	15	0.17	0.061	0.19	0.18	0.25	0.28
4	20	0.15	0.17	0.164	0.2	0.195	0.15
5	25	0.2	0.15	0.25	0.35	0.28	0.3
6	30	0.23	0.28	0.31	0.3	0.26	0.25

V. CONCLUSION AND FUTURE WORK

In the comparative analysis of Reactive protocol AODV, Proactive protocol OLSR and Hybrid routing protocol ZRP with attack and without attack using performance metrics packet delivery ratio, Average jitter, Average throughput, Average End to End Delay. The performance of AODV is best in presence of blackhole attack and without attack than OLSR and ZRP with attack and without attack in every case. In future we plan to extend my work on the blackhole detection and prevention scheme using some kind of security algorithm.

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.Shaily Mittal and Prabhjot Kaur "PERFORMANCE COMPARISION OF AODV, DSR and ZRP ROUTING PROTOCOLS IN MANET'S" International Conference on Advances in Computing, Control, and Telecommunication Technologies 978-0-7695-3915-7/09 © 2009 IEEE.

14. Raj Shree, Sanjay Kr. Dwivedi and Ravi Prakash Pandey "Design Enhancements in ZRP for Detecting Multiple Black Hole Nodes in Mobile Ad Hoc Networks" *International Journal of Computer Applications ISSN 0975 – 8887 Volume 18– No.5, March 2011.*

15. Arti Sharma and Satendra Jain"A Behavioral Study of AODV with and without Blackhole Attack in MANET" International Journal of Modern Engineering Research (IJMER) Vol.1, Issue.2, pp-391-395 ISSN: 2249-6645.

16.Vivek Thaper, Bindyia Jain and Varsha Sahni "PERFORMANCE ANALYSIS OF ADHOC ROUTING PROTOCOLS USING RANDOM WAYPOINT MOBILITY MODEL IN WIRELESS SENSOR NETWORKS" (IJCSE)International Journal on Computer Science and Engineering ISSN : 0975-3397 Vol. 3 No. 8 August 2011.