Improved Performance Analysis of DSDV, AODV, ZRP Under Black Hole Attack in MANETs

[1]S Muzamil Basha, [2]SR Raj Kumar, [3]G N. Vivekananda, [4]Raghu Veer Matam
[1,2,3]Dept. of IT, SVCET
[4]Wipro Technologies

Abstract
MANET consists of mobile hosts equipped with wireless communication devices operating without a central coordinator, self-motivated, rapidly -deployable, self-configuring wireless network. Routing in MANETs has immense challenges due to mobility, limited bandwidth, and battery constraints. Due to this the ad-hoc networks are vulnerable to different attacks one of them is Black Hole attack which occurs in network layer. In this paper We analyze the performance of DSDV (Proactive), AODV (Reactive) and ZRP (Hybrid) both under Black hole attack and without Black hole attack by varying number of nodes. Average End-to-END delay, Packet Delivery Ratio (PDR), Packet Drop Rate (PDRR) and Throughput are measured as performance parameter for estimating the performance of DSDV, AODV and ZRP protocol with and without Black Hole in the Ad-hoc network using NS2 simulator.

Keywords
MANET, AODV, DSDV, ZRP, Black Hole, PDR, PDRR, NS2

I. Introduction

MANET nodes are equipped with wireless transmitters and receivers using Omni-directional (broadcast) antennas. At a given point in time, depending on the parameters like nodes' positions , transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or "ad hoc" network exists between the nodes [1]. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters.

Fig. 1: Mobile Ad-hoc Network

MANET nodes perform the routing among themselves. Therefore, the nodes depend on one another to forward packet to the destination. On behalf of different operating methodologies routing protocols in MANET are classified in to three types [2-3].

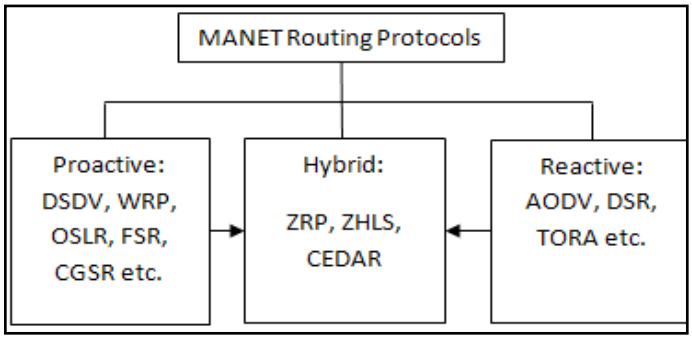


Fig. 2: Categorization of MANET Routing Protocols

The paper is organized as follows: Section 2 gives introduction to Black Hole Attack in MANET. Section 3 gives an idea on related work. Section 4 gives a brief description of three major MANET routing protocols – DSDV, AODV,ZRP that have been used for performance scrutiny of proactive, reactive and hybrid protocols of MANET. Section 5 describes the NS2 Simulation. Section 5 talks about some result and scrutiny and finally section 6 discuss the conclusion of this paper.

A. MANET Characteristics

The routing protocol for ad hoc wireless network should have the following characteristics [3].
It must be fully distributed.
It must be loop free and free from old routes.
Route computation and maintenance must involve a minimum number of nodes.
It must be adaptive to regular topology changes due to mobility of nodes.
It must optimally use scarce resources such as bandwidth, computation power, memory and battery power.

B. MANET Applications

There are many applications of MANET. Some of them are below [3].
1. Military network
2. Sensor network
3. Emergency services
4. Wearable computing

II. Black Hole Attack

Black Hole attack is one of the possible attacks in MANET that occurred at Network Layer. In this attack, a malicious node uses the MANET's routing protocol to sends a fictitious Route REPLY (RREP) packet to a source node that initiates the route discovery in order to make believe itself to be a destination node (or) advertise itself as having the shortest path to the destination node whose packets it wants to interrupt. In fig. 3, source node S wants to send data packets to a destination node D in the network. Source S initiates' the route discovery process. Let node M is a malicious node which behaves as a Black Hole. The malicious node doesn't checks it's routing table as in fig .4, and immediately responds with

a RREP as in fig. 5, even if it not have a valid route to the destination node D, In RREP message Hop Count value is set to lowest value and Sequence number is set to highest value [1]. The malicious node reply reaches the node before the reception of reply from the actual node D. Here after the node S starts discarding the RREP packets coming from the other nodes as the active route discovery process is completed. In this way the Source chooses the path provided by the malicious node and all the data packets are sent to a point where they are not forwarded anywhere and all the data packets will be lost [4-5]. The malicious node M forms a Black Hole in the network and this attack is called Black Hole attack.

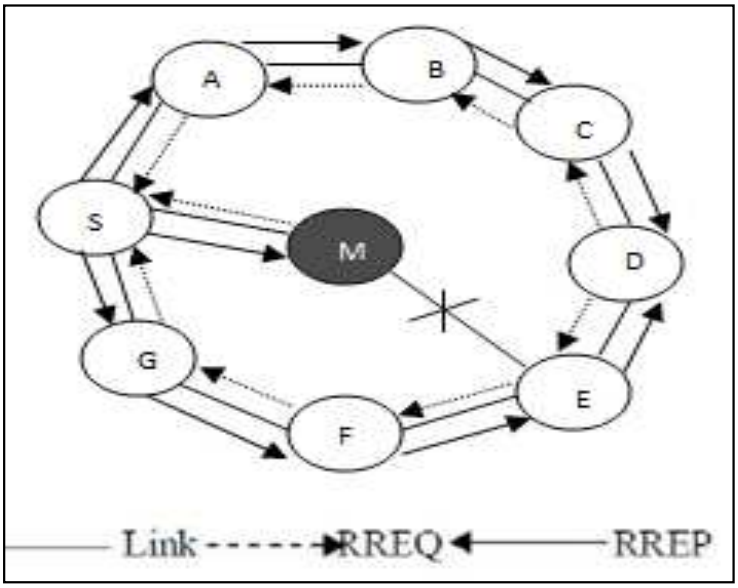


Fig. 3: Black Hole Attack

III. Related Work

The Work done by the researchers on MANETs Routing Protocols as Table 1, some of researchers have done a comparative study on reactive, proactive and Hybrid protocols with and without Black Hole node in MANET.

Table 1: Related Work

Author Name Reference	Protocols Used	**Simulator**	**Performance Metrics**	**Variable Parameters**
S.R. Shirke et al. [2]	AODV	NS2	Packet delivery ratio (PDR), Packet Drop Ratio (PDRR), Throughput.	Number of Malicious Nodes.
Harmandeep Singh et al.[4]	AODV, OLSR, ZRP	NS2	PDR, Throughput, Average end-to-end delay.	Number of Malicious Nodes.
Amin Mohebi et al.[5]	AODV, DSR	NS2	Throughput, Network Load, End-to-End Delay.	Number of Malicious Nodes.
Vidyapathi et al.[6]	AODV	NS2	Packets received, End-to-End delay, Throughput, PDR.	Number of nodes.
Jaspal kumar et al.[7]	AODV,IAODV	NS2	Packet delivery fraction ratio, Throughput, Average end-to-end delay.	Number of nodes.
Tarunpreet Bhatia et al.[8]	AODV	NS2	Average Throughput, PDR, Normalize Routing Load (NRL), Dropped Packets, Jitter.	Pause Time, Number of nodes, Speed, Number of Malicious Nodes
Ashutosh Lanjewar et al.[9]	AODV	NS2	Power Consumption, End-to-End delay, Network Load.	Number of Data Transfers.
Ashok M. Kanthe et al.[10]	AODV	NS2	Throughput, PDRR, End-to-End delay.	Number of Malicious Nodes.
Zaid Ahmad et al.[11]	AODV, idsAODV, HDAODV, EAODV	NS2	Throughput, Delay, PDR, Energy usage, NRL-Protocol Overhead.	Number of Malicious Nodes.
Mahmood Salehi et al.[12]	DSR,OLSR	NS2.34	Packet Drop Ratio, End-to-End delay, Number of Routing Packets	Number of Malicious Nodes.

IV. MANETs Routing Protocols

A. DSDV (Destination Sequence Distance Vector)

Destination-Sequenced Distance Vector (DSDV) routing protocol is a pro-active, table-driven routing protocol for MANETs. Every node will maintain a table listing all the other nodes it has known either directly or through some neighbors. Every node has a single entry in the routing table as shown in Fig .4. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node. Along with these details the table also keeps track of the Next-Hop neighbor to reach the destination node, the timestamp of the last update received for that node [14].

Destination	Next Hop	Number of Hops	Sequence Number	Install Time
A	A	0	A 46	1000
B	B	1	B 36	1200
C	B	2	C 28	1500

Fig. 4: Routing Table in DSDV Protocol

B. AODV (Ad-hoc On-Demand Distance Vector)

AODV routing protocols is another reactive routing protocol, which consists of the following procedures [3]:

1. Path/Route Discovery
2. Path/Route Maintenance

AODV succeed to the concepts of Sequence number from DSDV protocols in order to retain the freshest route in the network. A RREQ (Route Request) [7] is broadcast throughout the network with a search ring technique. Upon receiving RREQ by a node which can be either destination node or an intermediate node with a fresh route to destination reacts with a RREP (Route Reply) uni-cast packet to the source node. As the RREP is routed back along the reverse path, the RREP has reach source node, a route is said to be established between source and destination node [6-7].

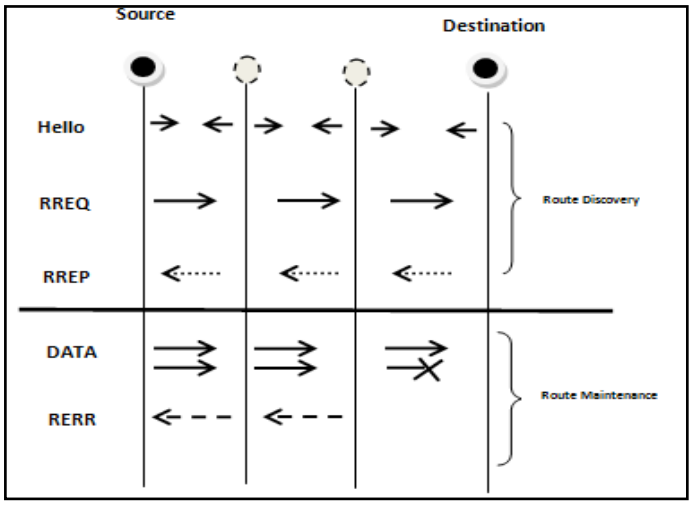


Fig. 5: Basic AODV Operations

C. ZRP (Zone Routing Protocol)

In ZRP neighbor discovery may be implemented through a separate Neighbor Discovery Protocol (NDP). Such a protocol typically operates through the periodic broadcasting of "hello" beacons. The reception of a "hello" beacon can be used to indicate the status of a connection to the beaconing neighbor [15]. Neighbor discovery information is used as a basis for the Intra-zone Routing Protocol (IARP). IARP can be derived from globally proactive link state routing protocols that provide a complete view of network connectivity. Route discovery in the Zone Routing framework is distinguished from standard broadcast-based route discovery through a message distribution service known as the Border-cast Resolution Protocol (BRP) [18]. On availability of BRP, the operation of Zone Routing's global reactive Inter-zone Routing Protocol (IERP) is quite similar to standard route discovery protocols. An IERP route discovery is initiated when no route is locally available to the destination of an outgoing data packet.

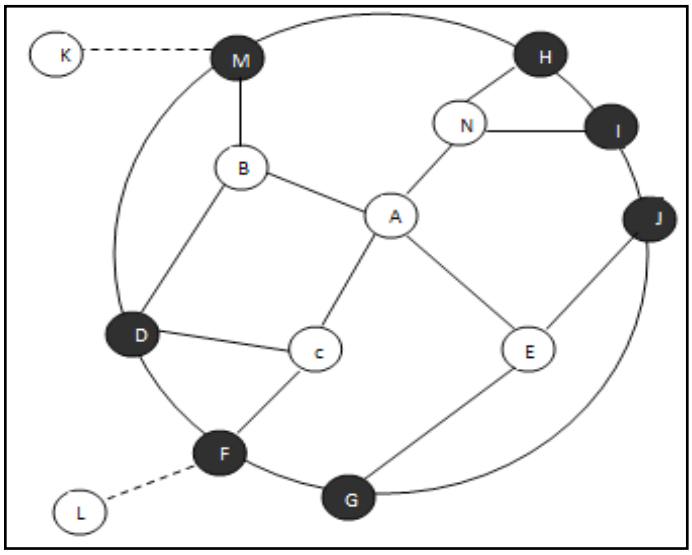


Fig. 6: Routing Zone of Node A with r=2.

Characteristics summary of DSDV, AODV and ZRP routing protocols are as shown Table 2 [7-8].

Table 2: Comparison of DSDV, AODV and ZRP

Metrics	DSDV	AODV	ZRP
Loop free	yes	yes	yes
Multicasting	NO	yes	yes
Large Network size	NO	yes	yes

V. NS2 Simulation

Ns2 is most widely used simulator by researchers; it is event driven object oriented simulator, developed in C++ as backend and OTcl as front end. If we want to deploy a network then both TCL (Tool Command Language) as scripting language with C++ to be used [14].

A. Performance Metrics

The following the performance metrics that are considered for evaluation of MANETs routing protocols.

1. Average End-to-End Delay

There are possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission

delays at the MAC, and propagation and transfer times. It is calculated by time taken for a data packet to be transmitted across an MANET from source to destination gives the average end-to-end delay for the received packets. This metric describes the packet delivery time: the lower the end-to-end delay the better the application performance [7].

$$D = (Tr - Ts)$$

Tr = Receiver Time and Ts = Sender Time (1)

2. Packet Delivery Ratio (PDR)

The ratio of the data packets delivered to the destinations to those generated by the CBR sources. The PDR shows how successful a protocol performs delivering packets from source to destination. The higher the PDR better the result. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness. To improve the performance of the network system the PDR must be high as feasible [6].

$$PDR = \frac{\text{Total no. of. Packets received}}{\text{Total no. of. Packets send}} \quad (2)$$

3. Packet Drop Rate (PDRR)

It is the ratio of the data lost at destination to those generated by the CBR sources. The packets are dropped when the node is not able to find the valid route to the node specified as an intermediate node in the route to reach the destination node [10].

$$PDRR = \frac{\text{Total no. of. Packets Dropped at destination}}{\text{Total no. of. Packets created by CBR source}} \quad (3)$$

Throughput (Tp):

It is the average rate of successful transmitted data packets in bytes per second within runtime [11].

$$Tp = \frac{\text{no.of.bytes received} * 8}{\text{simulation time} * 1000} \text{ kbps} \quad (4)$$

VI. Implementation

Table 3: Simulation Parameters

Parameter Name	DSDV	AODV	ZRP
NS Version	NS 2.35	NS 2.35	NS 2.35
channel type	Wireless Channel	Wireless Channel	Wireless Channel
netif	Phy/WirelessPhy	Phy/WirelessPhy	Phy/WirelessPhy/802_15_4
mac protocol	Mac/802_11	Mac/802_11	Mac/802_15_4
Radio propagation	Two Ray Ground	Two Ray Ground	Two Ray Ground
Antenna Type	Omni Antenna	Omni Antenna	Omni Antenna
Mobility Model	Random waypoint	Random waypoint	Random waypoint
Mobility	40 m/s	40 m/s	40 m/s
ifq	Queue/DropTail/PriQueue	CMUPriQueue	Queue/DropTail/PriQueue
ifqlen	100	100	100
Packet size	256 Bytes	256 Bytes	256 Bytes
number of nodes	15 and 200	15 and 200	15 and 200
routing protocol	DSDV	AODV	ZRP
Zone Radius	-	-	4
Area	1024×800 m	1024×800 m	1024×800 m
Transmission range	200 m	200 m	200 m
simulation time	2000 sec	2000 sec	2000 sec
Topology	Random	Random	Random
Traffic type	CBR(UDP)	CBR(UDP)	CBR(UDP)

VII. Results

Table 4: Simulation Result of DSDV With and Without Black Hole Attack

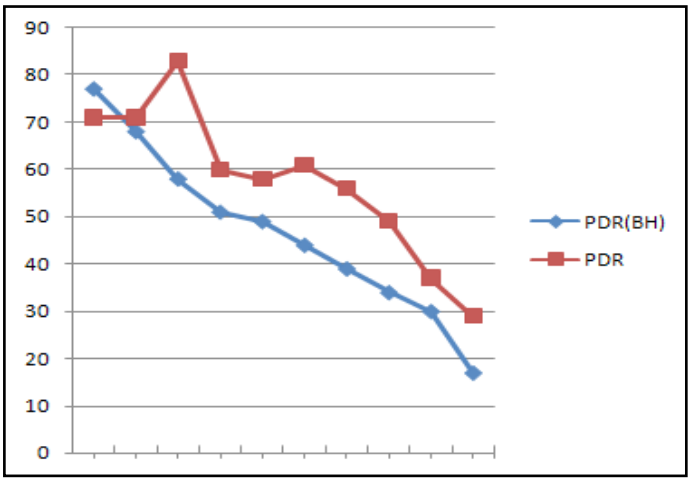
protocol	No. of. nodes	PDR(BH)	PDR	PDRR(BH)	PDRR	Delay(BH)	Delay	Throughput(BH)	Throughput
DSDV	10	77	71	35	29	0.12	0.2	78	109
	20	68	71	36	30	0.16	0.16	64	210
	30	58	83	53	51	0.20	0.17	55	210
	40	51	60	46	40	0.15	0.13	49	250
	50	49	58	48	43	0.33	0.18	46	270
	60	44	61	49	47	0.27	0.22	45	290
	70	39	56	52	51	0.41	0.27	41	305
	80	34	49	58	56	0.39	0.31	38	315
	90	30	37	61	59	0.52	0.37	33	329
	100	17	29	64	62	0.43	0.43	27	344

Table 5: Simulation Result of AODV With and Without Black Hole Attack

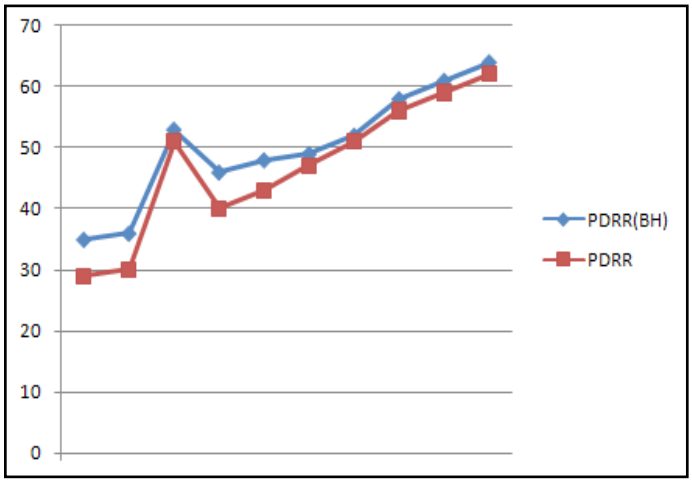
protocol	No. of. nodes	PDR(BH)	PDR	PDRR(BH)	PDRR	Delay(BH)	Delay	Throughput(BH)	Throughput
AODV	10	68	95	25	5	0.04	0.28	64	89
	20	61	99	27	13	0.14	0.45	46	93
	30	52	99	50	15	0.16	0.5	45	93
	40	39	99	45	24	0.15	0.52	38	93
	50	34	99	46	25	0.23	0.65	34	93
	60	30	98	45	27	0.14	0.61	30	91
	70	26	97	46	27	0.24	0.60	27	90
	80	21	95	46	26	0.13	0.58	23	89
	90	19	94	46	26	0.26	0.55	19	87
	100	15	90	45	27	0.16	0.49	14	84

Table 6: Simulation Result of ZRP With and Without Black Hole Attack

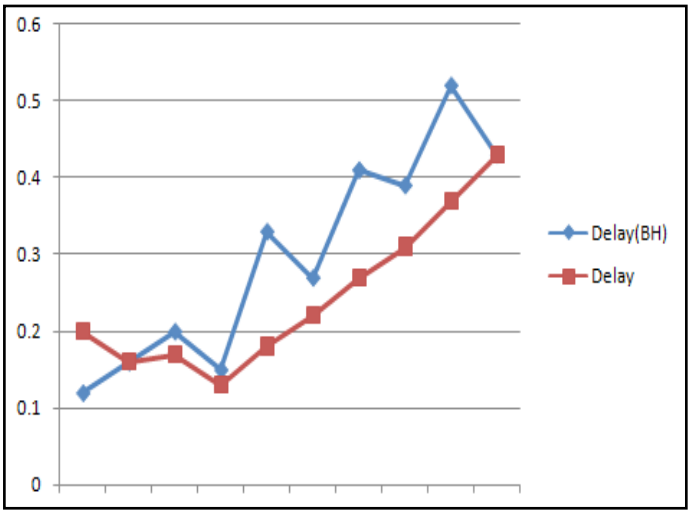
protocol	No. of. nodes	PDR(BH)	PDR	PDRR(BH)	PDRR	Delay(BH)	Delay	Throughput(BH)	Throughput
ZRP	10	95	85	26	5	0.031	0.38	95	156
	20	88	70	27	13	0.132	0.48	85	230
	30	75	60	49	15	0.128	0.53	73	210
	40	72	44	43	24	0.184	0.62	71	175
	50	70	34	44	37	0.121	0.73	68	110
	60	65	29	45	45	0.153	0.69	65	95
	70	59	25	45	47	0.091	0.83	60	97
	80	55	19	47	49	0.132	0.79	54	85
	90	51	17	47	54	0.045	0.64	49	80
	100	49	14	44	61	0.119	0.51	42	76



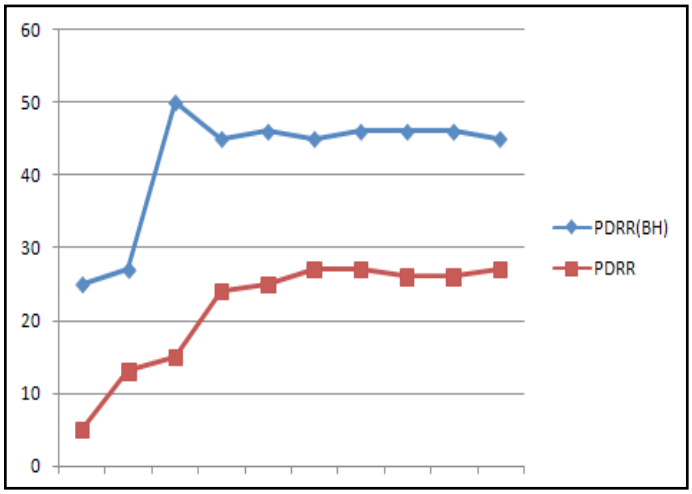
Graph 1.1 DSDV_ PDR and PDR (BH) Vs Varying Number of nodes



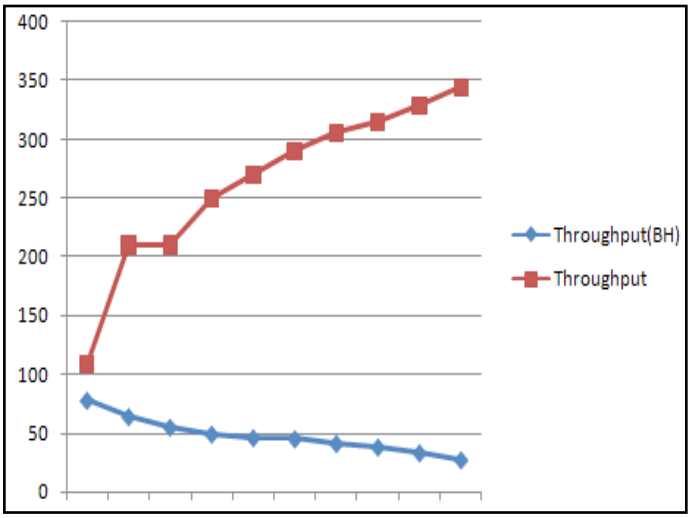
Graph 1.2 DSDV_ PDRR and PDRR (BH) Vs Varying Number of nodes



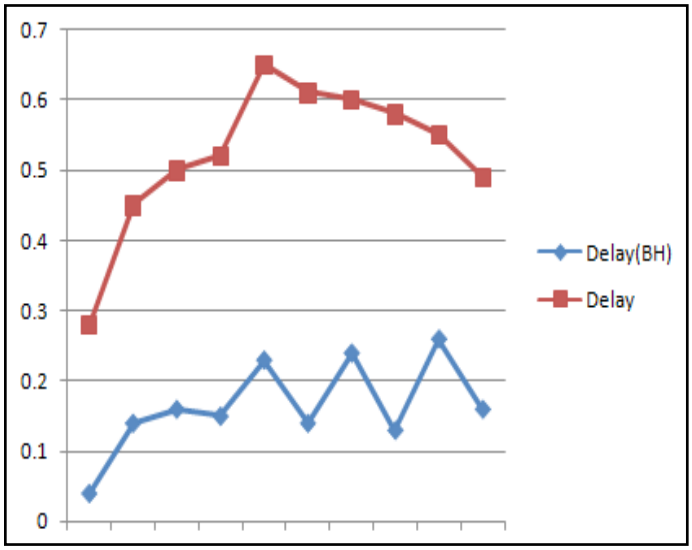
Graph 1.3 DSDV_ Delay and Delay (BH) Vs Varying Number of nodes



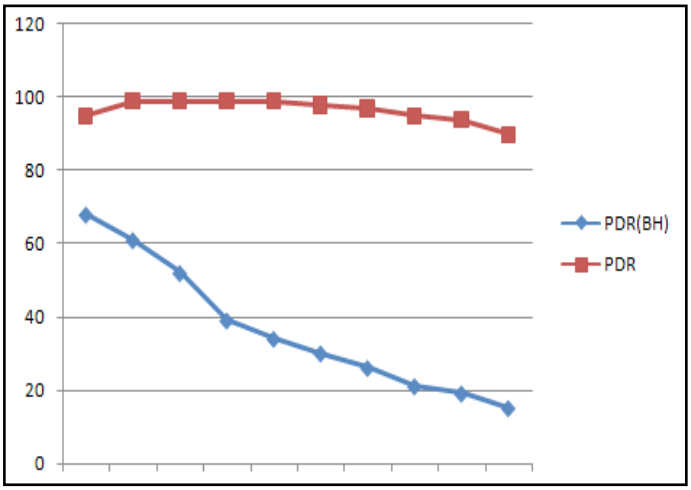
Graph 2.2 AODV_ PDDR and PDDR (BH) Vs Varying Number of nodes



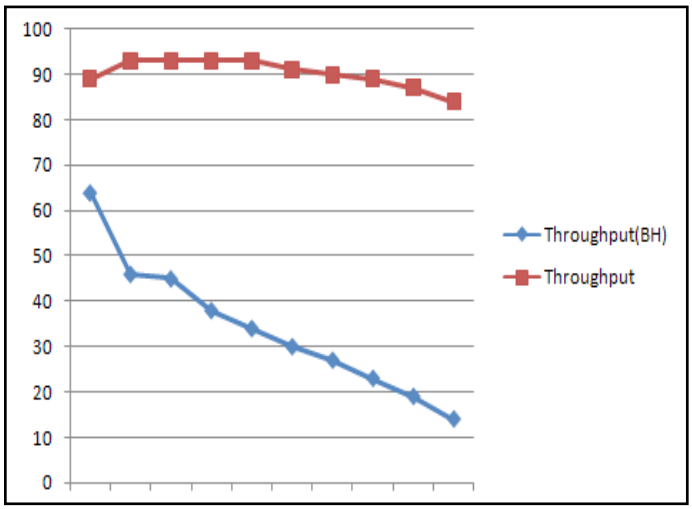
Graph 1.4 DSDV_ Throughput and Throughput (BH) Vs Varying Number of nodes



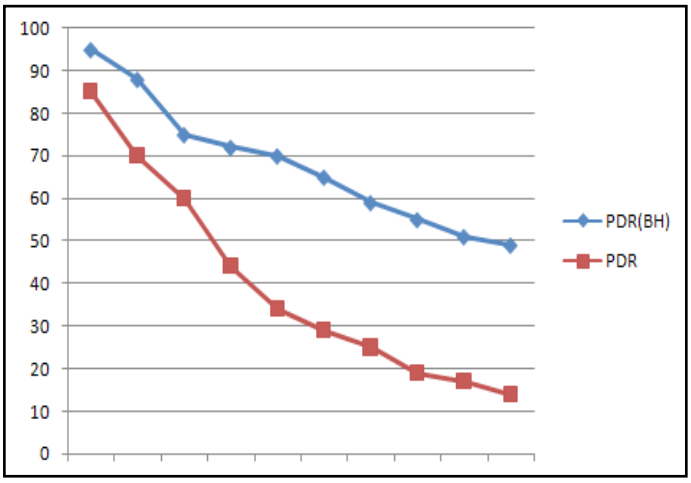
Graph 2.3 AODV_ Delay and Delay (BH) Vs Varying Number of nodes



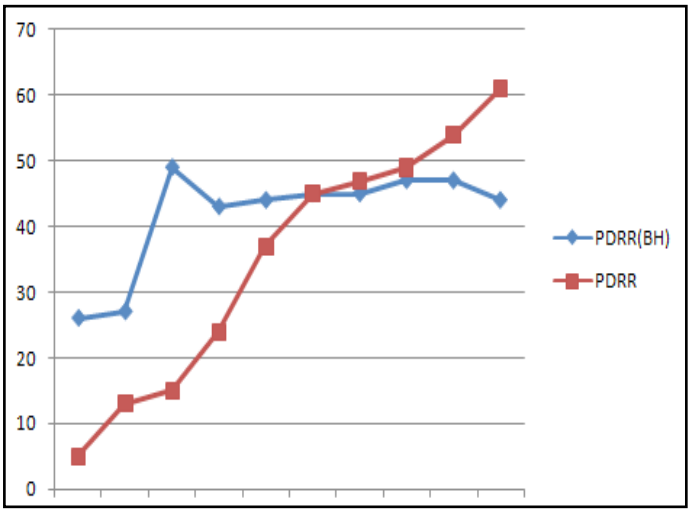
Graph 2.1 AODV_ PDR and PDR (BH) Vs Varying Number of nodes



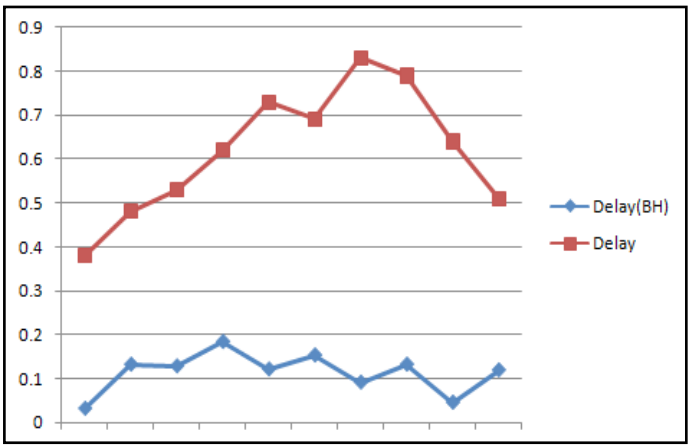
Graph 2.4 AODV_ Throughput and Throughput (BH) Vs Varying Number of nodes



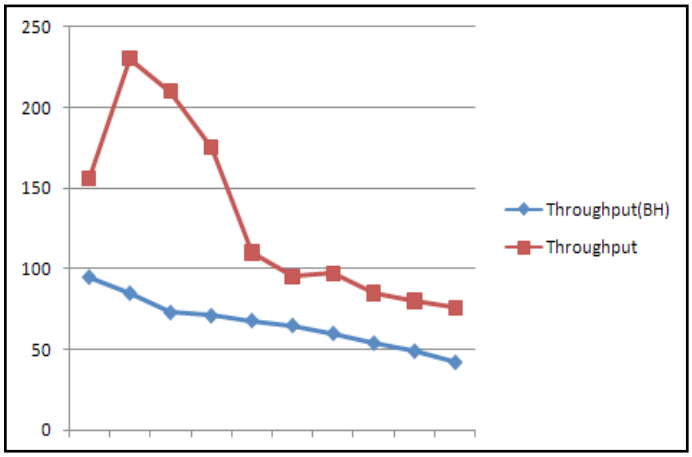
Graph 3.1 ZRP_ PDR and PDR (BH) Vs Varying Number of nodes



Graph 3.2 ZRP_ PDRR and PDRR (BH) Vs Varying Number of nodes



Graph 3.3 ZRP_ Delay and Delay (BH) Vs Varying Number of nodes



Graph 3.4 ZRP_ Throughput and Through (BH) Vs Varying Number of nodes

VIII. Conclusion

In this paper, we have analyzed the performance of MANETS routing protocols like DSDV, AODV and ZRP with respect to different performance metrics like Packet Delivery Ratio (PDR), Packet Drop Ratio (PDRR), Throughput (Th), and End-To-End delay both with and without Black Hole attack in the network. Finally, we conclude the effect of Black Hole is more on AODV protocol as compared to DSDV and ZRP.

IX. Acknowledgments

The authors are thankful to IJECT Journal for the support to develop this document.

Reference

[1] Mobile Ad-Hoc Networks (2013) Working Group [Online] Available: http://www.tools.ietf.org/id/draft-ietf-manet-aodvv2-02.txt dated: 04/11/13.

[2] S.R. Shirke, V.R. Ghorpade,"Intrusion Dection System for AODV protocol in MANET", International Journal of Engineering Research & Technology, Vol. 2, Issuse 5, 2013.

[3] S. Muzamil Basha, S.R. Raj kumar, M. Raghu veer, "Inclusive performance scrutiny of DSDV, AODV and ZRP MANETs Routing Protocols", Vol. 2, Issuse 5, Oct. 2013.

[4] Harmandeep Singh, Manpreeet Singh,"Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs", International Journal of Advanced Trends in Computer Science and Engineering, Vol. 2, No. 3, May - June 2013.

[5] Amin Mohebi, Ehsan Kamal, Simon Scot,"Simulation and Analysis of AODV and DSR Routing Protocol under Black Hole Attack", I.J. Modern Education and Computer Science", Vol. 10, 2013.

[6] Vidyapathi, Sundar, Harshita, Komal, "Securing MANET From BlackHole And WormHole Attacks", International Journal of Engineering and Technology" Vol. 5, No 3, Jun-Jul, 2013.

[7] Jaspal Kumar, Kulkarni, Daya Gupta,"Effect of Black Hole Attack on MANET Routing Protocols", International Journal of Computer Network and Information Security",Vol. 5, pp. 64 - 72, 2013.

[8] Tarunpreet Bhatia, Verma,"Performance Evalution if AODV under Blackhole Attack", International Journal of Computer Network and Information Security" Vol. 12, pp. 35-44, 2013.

[9] Ashutosh Lanjewar, Neelesh Gupta,"Optimizing Cost, Delay, Packet Loss and Network Load in AODV Routing Protocol", International Journal of Computer Network and Information Security, Vol. 11, No. 4, April, 2013.
[10] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, (2013) "Effects of Malicious Attacks in Mobile Ad-hoc Networks", "IEEE International Conference on Computational Intelligence and Computing Research", 2012.
[11] Zaid Ahmad, Jamalul-lali Ad Manan, Kamarularifin Abd Jalil,"Performance Evaluation on Modified AODV Protocols", IEEE Asia-Pacific Conference on Appiled Electromagnetics, Dec. 11-13, 2012.
[12] Mahmood Salehi, Hamed Samavathi,"DSR Vs OLSR: Simulation based Comparision of Ad-hoc Reactive and Proactive Algorithms Under the Effect of New Routing Attacks", Sixth Intervation Conference on Next Generation Mobile Application, Services and Technologies, IEEE, 2012.
[13] Hon Sun Chiu, King - Shan Lui,"DelPHl: Wormhole Dectection Mechanism for Ad-Hoc Wireless Network", The 1st International Symposium on woreless Pervasive Computing", January, 2006
[14] ns-2: Group [Online] Available: http://www.isi.edu/nsnam/ns/
[15] ZRP, internet draft Group [Online] Available: http:// tools.ietf.org/id/draft-ietf-manet-zone-zrp-04.txt.
[16] ZRP Patch, Group [Online] Available:http://magnet.daiict.ac.in/magnet_member/MTech/2007/patelBrijesh/Simulation.html#Sec_2.
[17] NS Simulator for beginners, Group [Online] Available: http://www-sop.inria.fr/members/Eitan.Altman?COURS-NS/n3.pdf.
[18] Zone Routing Protocol Group [Online] Available: http:// tools.ietf.org/html/draft-ietf manet-zone-zrp-04

S. Muzamil Basha received the B-Tech degree in CSIT form SITAMS, JNTU University, Chittoor, in 2008. He Received M-Tech degree in Information Technology (Networking) from the VIT University, Vellore, Tamil nadu, in 2011 respectively. Currently working as Assistant professor of Information Technology at SVCET, JNTUA University, teaching and research areas include Routing in MANET, IDS in MANET, congestion in MANET, security issues in MANET.

SR Raj Kumar received the B.E degree in ECE form Vellore Engineering college, Vellore, Tamil nadu in 1990. He Received M-Tech degree in Information Technology, Satyabama University, Chennai, Tamil nadu, in 2008. Currently working as Head of the department of Information Technology at SVCET, JNTUA University, teaching and research areas include Routing in MANET, IDS in MANET

G N. Vivekananda received the B-Tech degree in CSE form MITS, Madanapalle in 2010. He Received M-Tech degree in Specialization of software Engineering, SVEC, Tirupathi in 2012 Assistant professor of Information Technology at SVCET, JNTUA University, teaching and research areas include Routing in MANET, IDS in MANET, congestion in MANET, security issues in MANET.

Raghu veer Matam received the B-Tech degree in CSE form GIT, JNTUA University, Gooty, Anathapur , in 2009. He Received M-Tech degree in Information Technology (Networking) from the VIT University, Vellore, Tamil nadu, in 2011 respectively. Currently working as software engineer in Wipro Limited, teaching and research areas include Routing in MANET, IDS in MANET.