Performance Analysis of Routing Protocols under Security Issues through Use of NS2 Simulator

Akanksha Bali
Assistant Professor, Dept. of Computer Engineering
YCET, Jammu, India

Malvika Ashok
Assistant Professor, Dept. of Computer Engineering
YCET, Jammu, India

Megha Mahajan
Lecturer, Dept. of Computer Engineering
YCET, Jammu, India

ABSTRACT
Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. Unlike the wired networks, the unique characteristics of MANET pose a number of non-trivial challenges to security design. In MANETs, routing protocols are necessary to find specific paths between the source and the destination. MANET routing protocols are categorized into three types named as proactive, reactive, hybrid. To Provide Connectivity, Wireless MANETs take the help of multi-hop peer to peer routing. The MANETs topology change with time. MANETs have applications in several military and civilian areas. This paper contains comparison related to five different types of routing protocols named as AODV, DSDV, DSR, ZRP and OLSR. In MANET, these protocols are used for active routing under the several scenarios which plays a complex role in places where wired networks neither present nor economical to play. My objective was to implement Five routing protocols named above by using NS2 and compared their performances under different Parameters and metrics by using Attack and without attack.

Keywords
MANETs, DSR, DSDV, ZRP, AODV, OLSR, NS2, Routing Protocols, Black Hole Attack, AODV-BH, DSDV-BH, DSR-BH, ZRP-BH, OLSR-BH

1. INTRODUCTION
A MANET uses multiple hops routing that have uses in several domains like military, civilian and computing areas. The MANETs topology continuously manipulate with time. The traditional routing protocols are not superior for MANETs due to this fresh challenge faced by protocols of routing. Not all the protocols can handle change in topology as well as the proved assumptions used by these protocols. Mobile Ad-hoc network can be divided into Table Driven, on demand, hybrid (ZRP), hierarchical, geographical due to several techniques of routing. A mobile ad-hoc network is a union of mobile nodes forming an ad-hoc network without centralized infrastructure. These networks did well in environment without any infrastructure and deploy an infrastructure is not very cost effective. MANET is famous because of broad area of present wireless services providing pervasive computing at low cost. The main objective of such type of network is to give quick process of communication arrangement and computing. The Behavior of protocols of routing in this changing world topology environment is important. DSDV, DSR, ZRP, OLSR, AODV are some of the protocols of routing have been suggested on the last two decades. This changing environment and framework not only provides big dare to improve the role of ad-hoc network routing protocols. Nodes differing speed leads to failure of link. Congestion leads by size of networks and load of traffic. Limited range of transmission, power and high frequency also causes reasonable impacts over scalability of networks. MANETS is a sovereign system of mobile nodes affiliated by wireless links, every nodes works as a router for the remaining nodes in the networks otherwise nodes works as an end system. Electronically, wireless network is an upgraded fresh automaton that will permit users to connect to information and services without regard of their geographic locations. Infra-structured network and infrastructure-less networks are the two categories of wireless networks. Infra-structured networks are those networks where fixed and wired gateways exist. In this network, mobile communicate with a bridge in its communication radius. A MANET is a union of nodes that are wireless which communicate/interact by forwarding packets to permit them to collaborate with foreign domain of explicit wireless transmission.

2. ROUTING PROTOCOLS
MANETs are multi-hop ad-hoc wireless networks in which structure of the networks manipulates vigorously due to the motion of nodes. Nodes in these networks make use of the similar random access in wireless channel, collaborating in a friendly manner to involving themselves in forwarding the network nodes that only behave as hosts but also behave as routers that shift data from one node to other node. There is a need of routing procedures to get a path, so as to send the packets accurately between the transmitters of a destination. [10]

2.1 AODV
Reactive routing protocol/ source initiated routing protocol/ reactive gateway discovery is called by Adhoc on demand vector routing protocol. This is due to AODV only finds the way to the destination when source desires to send data. Route discovery mechanism of AODV depends upon route request, route reply and route fault message. In AODV, when there is a desire to discover path, source node sends so many RREQ messages to all nearby immediate nodes. The sequence number of destination is contained by this RREQ message. This sequence number guides in assuring route effectiveness availability and protect from loop in routing. For sending node, a node having highest sequence number is preferred first. The format of RREQ is [2]

Source Address	Broadcast ID	Source Sequence no	Destination Address	Destination Sequence No	Hop Count

Figure 1: - Format of RREQ

The < Sender Address/ Source Address, Distributed ID/Broadcast ID> recognize a RREQ

2.2 DSR

It depends on bellman ford algorithm. Few extreme extensive modifications have been done in bellman ford algorithm so that it is well suited for environment and suffer with CI (count to infinity) problem. Modifications are transmitted due to manipulation in topology which causes overhead. A complete dump and incremental manipulation are the two categories of updating that are used to overcome the drawback. In complete dump, whole routing table is sent to neighbors as far as full topology change. In incremental manipulation, modification in the route is set. Each node maintains a number of all destinations and list of hops to every destination. To reduce network jam/traffic created by route update, DSDV uses incremental manipulation or complete dump. Routing information can be always available with this improvement when there is a link addition/removal occurs, i.e. manipulation occurs. The format of DSDV is [3]

Destination IP Address	Destination Sequence Number	Hop Count

Figure 2: - Format of DSDV

2.3 DSDV

The routing protocols designed basically for used in multiple hops ad-hoc wireless networks. DSR make the network self learned with any consolidated infrastructure. DSR appears under reactive routing access that raises route discovery and route maintenance process. It uses the source routing means source needs to know the full hop sequence to the destination. The main loss is that every packet has to carry the overhead. Finding a route is high priced in case of time, energy and high frequency. Advantage is that it avoids routing loops due to determination of complete route by a single node. Another advantage is that avoidance of the need for update routing information in the in-between node due to all the needed routing information. It establishes the way with less delay. It easily repaired the broken link in active/ working routes. Sequence numbers are used for loop free activity and trace accuracy of information. It removes the requirement to continuously traffic the network with update message like in an AODV. The in-between node makes use of information of route cache efficiently to overcome the control overhead. [4]

2.4 ZRP

ZRP is outline to direct the problem related with proactive and reactive routing. Extreme bandwidth usage due to flooding of update packets and high delay in request of route discovery are two major problems of proactive and reactive routing protocol. ZRP arise/occur with the idea of zones. Route maintenance is smoother and less no of routing updates due to limited zone. Border node performs the task of reactive routing when the node is external to the zone can communicate. Hence ZRP gathers the characteristics of both proactive and reactive protocol. MAC level functions intra zone routing protocol, broadcast routing protocol are the four components contained by the ZRP structure/architecture. When the nodes are inside/within the zone, proactive routing is used. When the nodes are outside the zone, reactive routing is neighbor finding and function of maintenance is done by MAC level. Packets routed by an IARP protocol within a defined zone. IARP holds information in the routing table about all the nodes. If the nodes are outside the zone, IERP protocols help to search best path. Accurate routes are maintained by the IERP outside the zone. If the routes in its table are not present in IERP, then it transmits query to BRP that restricts traffic/flood within network. It sends route query request to nodes lie in border which transmit and receive packets only. [5]

2.5 OLSR

Putta et al. determines the behavior analysis of reactive protocols like AODV, DSR and proactive protocol Like OLSR, DSDV. Distinguishable analysis represented with sum of consideration of networking context. Data and voice are the combo of communication will be presented by the accurate routing protocols. All analyzed routing protocols behave same. OLSR is best in performance than all in terms of increasing load of traffic. OLSR continuously transmits routing packets to maintain the updated routing table to increase the routing load. When DSR generates large delay then it gives large sum of data packets for use in ftp sources. AODV and DSR give less performance for CBR than OLSR. Due to similar nature of both delay and routing load, we can't say who is winner between DBR and AODV. [9]

3. NS2 SIMULATOR

NS2 is a disconnected event simulator directed at networking research. It gives generous means for TCP routing and Multicast protocols by wired and wireless Networks. Imitation results can be shown as graphical interpretation by x-graph. The flavor used is UBUNTU 12.04 in platform of LINUX operating system. NS2 deciphers OTCL scripts illustrated by user. A user explained several elements of system of connections in OTCL like scheduler objects. These simulators are reproduced with the NS2. The broad understanding of NS2 in research and thesis sector is due to free dissemination and open source. It is appropriate for distinguishing several protocols, jam and builds fresh protocols. It is a union of C++ and OTCL. Object oriented imitator is also known as ns2 because it uses C++. OTCL works as an interpreter. On one hand, constituent imitations of protocols need a system programming language which can usefully packet header. The time it takes to deal with is less and run time speed is more important for the tasks. C++ is quick to learn but change slowly. In NS2 two languages are used one of two is TCL which is the front end language removes the disadvantage of C++. It changes quickly but slow to run. Second of two is called backend language written in C++. DSDV, DSR, ZRP, OLSR and AODV programming are done in TCL program. When it is compiled, a trace and a NAM file are generated, which gives information about the motion pattern of nodes, sum of hops among nodes and type of linking. A scenario file is originated which describe mobile nodes destination along with their speed. CBR file s also generated illustrates the connection arrangement, topography and packets type that is useful to obtain the trace file and NAM files used by the imitator to reproduce the network. [7]

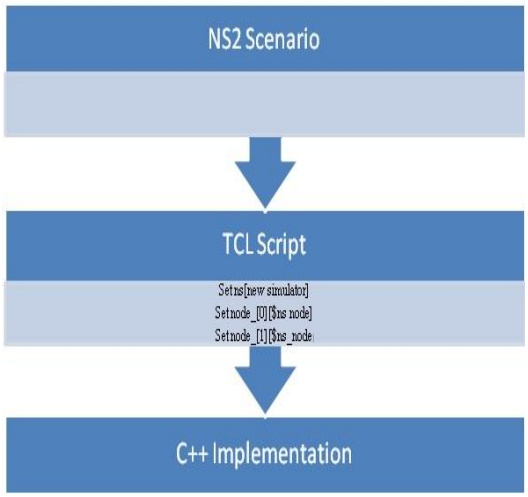

Figure 3: - Basic steps of NS2

3.1 Use of NS2

It is used in TCP, routing in ad-hoc networks like DSDV, DSR, ZRP, AODV and the remaining protocols too, MAC like TDMA, multiple casting protocols, used in satellite like spacecraft protocols.

3.2 Architecture of NS2

In TCL basic architecture, first TCL imitation script is written in TCL file and its expansion is .TCL then it is operate by NS2 shell executable command which involves both C++ and TCL language. The connection within two languages is provided through TCLCL associating. Shell originates two outputs one of two is NAM which hoard the output as activity. Advanced architecture differ from basic architecture of NS2 because in advance architecture, C++ imitation objects is exchanged with C++, OTCL simulation objects is regained with OTCL interpreter and NAM and Trace file is replaced with simulation results. [8]

3.3 Metrics of Routing Protocol

- PDR: - It is also known as packet delivery ratio which is defined as division of packets of data arrived at receiver to the originated/total packets of data. It only computes the sum of packets reached in the destination.
- Delay: - The subtraction of arrived data packet time to the originated data packet time through sender. This is also called as latency. The application that is used in Delay that is sensitive is voice. It is inversely proportional to behavior of protocols.
- NRL: - The sum of control message of routing is divided to the sum of arrived messages at the destination.
- Throughput: - The sum of messages arrives at receiver is followed by size of packet multiplied by 8 is divided to the total time of simulation. Mathematical calculations can be used to determine throughput.
- Packet Sent: - The sums of packets assigned to the destination.
- Packet Receiving Count: - The sum of packets reached in the destination.

3.4 Performance parameters

The several parameters used in DSDV, DSR, ZRP, OLSR and AODV are given below:

Parameters	Value
Operating System	Ubuntu 12.04
NS2	2.35
Routing Protocol	AODV, DSDV, DSR, ZRP and OLSR
Channel Type	Wireless Channel
Radio Propogation Model	Two Way Round
Network Interface Type	Wireless Physical
Mac Type	802.11
Queue/Drop Tail	Priority Queue
Antenna	Omni Antenna
Max Packet in NT	50
no of Mobile Nodes	30
X Dimension of Topography	1000
Y Dimension of Topography	1000
Simulation Time	"./comm."
Initial Energy	1000
Transmission Power	0.025
Range	3.65262e-10
Frequency	914e+6
Agent	UDP
Application	CBR
Packet Size	512
Maximum Packets	1000
Speed	3,5,7

Figure 4: Performance Parameters

4. RELATED WORK

A comparison will be organized to search which routing protocol is adequate in terms of security issues, PDR, delay, NRL, Packet sent, throughput, Packet received.

This paper contains issues related to four different types of routing protocols named as AODV, DSDV, DSR, ZRP and OLSR. First we installed OS UBUNTU by virtual box. The package used in our thesis is NS2 because it contains all AODV, DSDV, DSR protocols. As per our objective, we have to compare the performance of DSDV, DSR, ZRP, AODV and OLSR. But ZRP and OLSR are not under ns2.35, so for ZRP and OLSR, we need to integrate both separately with NS2 and make the patch file of them. Now we will have to design a network as per required for all- AODV, DSR, DSDV, ZRP, OLSR. For analysis of Performance we can take any script like Shell, Perl, and AWK and so on. After getting performance of multiple protocols we can do next step. For checking performance we will have to apply an attack so we are going to apply black hole attack on all routing protocol named as AODV-BH, DSDV-BH, DSR-BH, ZRP-BH and OLSR-BH and then we will check the performance. BH is black-hole. Make, make depend, SUDO make install are the commands used to run all protocols. The performance metrics that we consider for comparing performances are named as throughput, PDR, NRL, end to end delay, loss of packet, routing overhead. This is done by using AWK script. This analysis is done by way of Graph and AWK script file. We Enter the values comes through AWK script file is entered in EXCEL sheet and make a chart by way of the entries as represented in figure given below

4.1 Analysis of comparison between AODV and AODV-BH (AODV with Black hole)

From the below table and graph we analyzed that AODV is better in delay than AODV-BH attack. AODV is superior in PDR, NRL and throughput than AODV-BH. The Receiving packet count values of AODV table is less than receiving packet count values of AODV-BH table. The sum of packets lost values in AODV table is less than AODV-BH table [10].

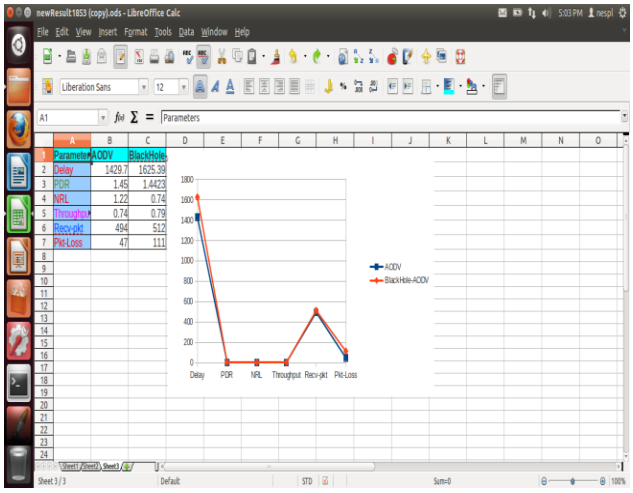

Figure 5: Comparison of analysis of AODV and AODV-BH (AODV with Black Hole Attack)

4.2 Analysis of comparison between DSDV and DSDV-BH (DSDV with Black hole)

From the below table and graph we analyzed that DSDV is very much better in delay than DSDV-BH attack. DSDV is superior in PDR and throughput than DSDV-BH. The Receiving packet count values of DSDV table is inferior than receiving packet count values of DSDV-BH table. The sum of packets lost values in DSDV table is inferior to DSDV-BH table. The NRL (Normalized Routing Load) of DSDV is superior to DSDV-BH. The graph and Table of DSDV with Black Hole Attack and Without Attack is shown below [10]:

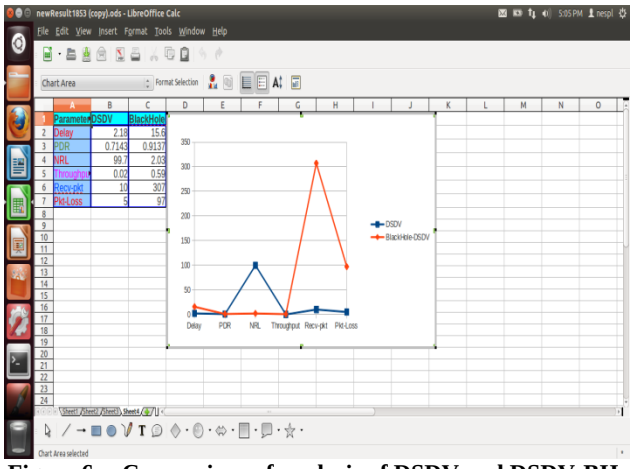

Figure 6: - Comparison of analysis of DSDV and DSDV-BH (DSDV with Black Hole Attack)

4.3 Analysis of comparison between DSR and DSR-BH (DSR with Black hole):

From the below table and graph we analyzed that the values of delay, NRL and packet lost in DSR table is very lower than DSR-BH table that means DSR is superior in delay, NRL and Packet lost than DSR-BH attack. The values of PDR in DSR table are very less than DSR-BH table hence DSR is inferior in PDR than DSR-BH. The throughput in DSR is extremely higher than DSR-BH. The graph and Table of DSR with Black Hole Attack and Without Attack is shown below [10]:

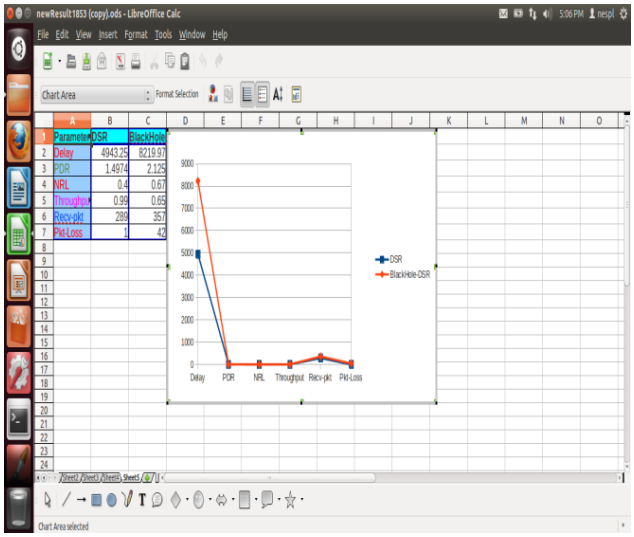

Figure 7: Comparison of analysis of DSR and DSR-BH (DSR with Black Hole Attack)

4.4 Analysis of comparison between ZRP and ZRP-BH (ZRP with Black hole)

From the below table and graph we analyzed that ZRP is superior in delay, PDR, Receiving Packet Count, Throughput and Packet lost than ZRP-BH attack. The values of NRL in ZRP table is extremely higher than ZRP-BH table hence ZRP is inferior in NRL than ZRP-BH [10].

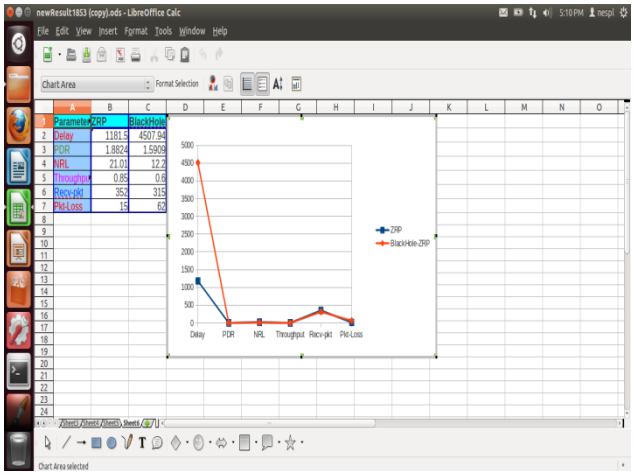

Figure 8: Comparison of analysis of ZRP and ZRP-BH (ZRP with Black Hole Attack)

4.5 Analysis of comparison between OLSR and OLSR-BH (OLSR with Black hole):

From the below table and graph, we analyzed that the values of delay, NRL and packet lost in OLSR is extremely more than OLSR-BH table that means OLSR-BH is superior delay, NRL and Packet lost than DSDV. The value of PDR in OLSR table is extremely more than OLSR-BH table hence OLSR is superior in PDR than OLSR-BH. The throughput values in OLSR table are less than OLSR-BH table. The values of receiving packet count in OLSR table are less than OLSR-BH table.

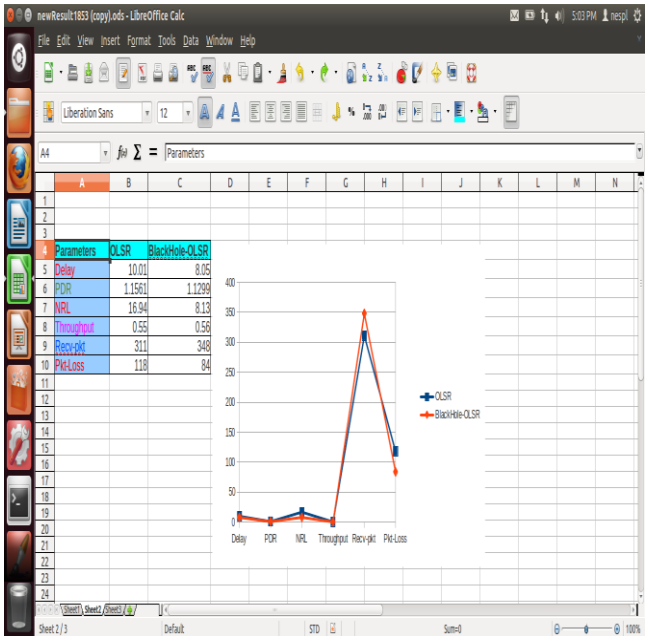

Figure 9: - Comparison of analysis of OLSR and OLSR-BH (OLSR with Black Hole Attack)

4.6 Performance without Attack

From the below table and graph we analyzed that the value of delay in DSR table is higher than all values of delay in the remaining tables of protocols. DSDV is superior in delay without Black hole attack due to less value of delay in its own table. ZRP is superior in PDR but DSDV is inferior in PDR due to less value of PDR in its own table. The value of NRL is extremely high in DSDV table and less in DSR table. The value of Throughput is extremely high in DSR table and less in DSDV table. The value of receiving packet count is extremely high in AODV and less in DSDV table. The value of packet loss is less in DSR but high in OLSR.

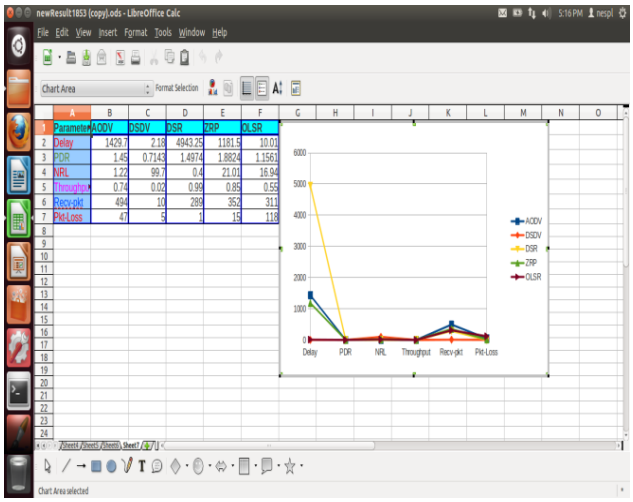

Figure 10: - Performance of DSDV, DSR, OLSR, ZRP and AODV without Black Hole Attack

4.7 Performance with Black Hole Attack

From the below table and graph represented in the figure, we analyzed that the DSR-BH is inferior in delay due to extreme high values of delay in its own table and superior in packet loss due to less packet loss value in DSR-BH table. DSDV-BH is superior in Delay. The values of Receiving Packet Count are high in AODV-BH table. The values of through put are high in DSR-BH table. The values of NRL are high in ZRP table. DSR-BH is superior in PDR.

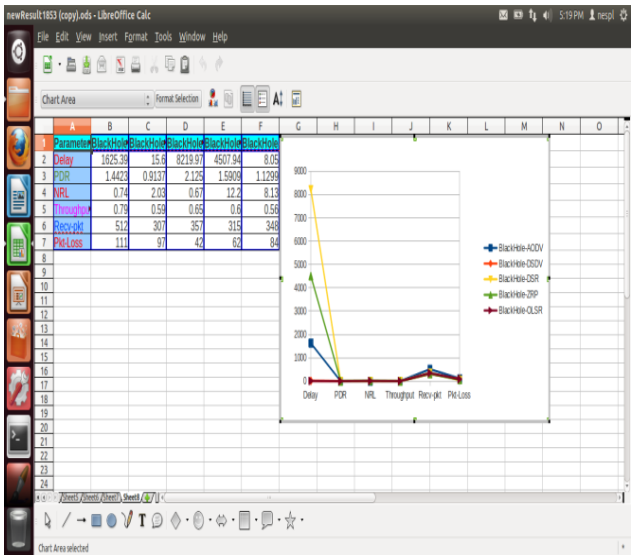

Figure 11: - Performance of DSDV, DSR, OLSR, ZRP and AODV with Black Hole Attack

5. CONCLUSION

The paper concludes that DSDV is superior in delay than all protocols it means that DSDV has good DSR and DSR-BH is superior in PDR than all protocols but DSR-BH is superior in PDR than DSR. Throughput and NRL is superior in DSDV. The value of receiving packet count is more in AODV table and AODV-BH table but the values of receiving packet count in AODV-BH table is more than values of receiving packet count in AODV table. The values of packet loss in DSR and DSR-BH are lesser than all protocols tables. But DSR-BH has more packet loss than DSR. The values of throughput are high in AODV and AODV-BH table, but throughput in AODV-BH is superior in AODV. ZRP is superior in delay, PDR, Receiving Packet Count, Throughput and Packet lost than ZRP-BH attack. The NRL value in ZRP table is more than ZRP-BH table hence ZRP is inferior in NRL than ZRP-BH. The Performance of OLSR is opposite to DSDV. We analyzed that the values of delay, NRL and packet lost in OLSR table is extreme high than OLSR-BH table that means OLSR-BH is superior in delay, NRL and little loss of packet than DSDV. The PDR value in OLSR table is greater than OLSR-BH table hence OLSR is superior in PDR than OLSR-BH.

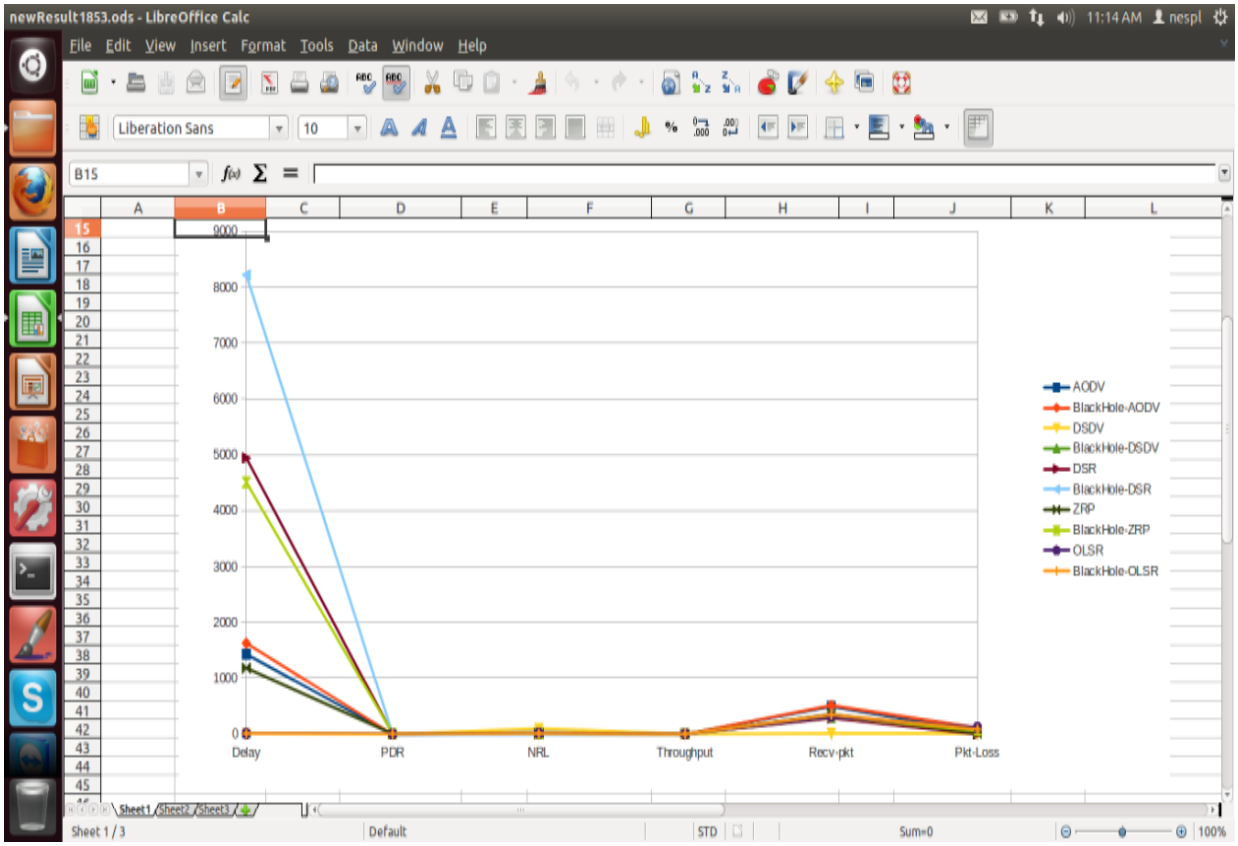

Figure 12: Performance Analysis of Routing Protocols under Security Issues through Use of NS2 Simulator

Table 1: Overall Comparison of all protocols with and without BH based on different parameters

Parameters	AODV	DSDV	DSR	ZRP	OLSR
Delay	It has the maximum delay after DSDV and ZRP without black hole and minimum delay after DSDV with black hole	It has the least delay without black hole compared to other routing protocols and minimum delay with Black hole after OLSR	Maximum delay with and without black hole	It has delay less than AODV and DSR but greater than DSDV without black hole and with black hole it has maximum delay after DSDV	It has minimum delay without black hole after DSDV and has the least delay with black hole compared to other routing protocols
PDR	Packet delivery ratio(PDR) is lower in AODV than DSR, ZRP	DSDV has the least Packet delivery ratio	Maximum Packet delivery ratio is recorded in DSR	ZRP gives higher packet delivery ratio after DSR	OLSR has more packet delivery ratio than DSDV but lower than all other protocols
NRL	It comes at fourth place in NRL	It has the maximum normalized routing load (NRL)compared to other protocols	Least Normalized Routing load is calculated in DSR	ZRP has higher NRL after DSDV	Normalized routing load of OLSR is higher than AODV and DSR but lower than DSDV and ZRP
Throughput	AODV gives higher throughput after DSR protocol	DSDV has the least throughput compared to all other protocols	DSR has the best throughput among other protocols	Throughput of ZRP is lower than AODV and DSR	OLSR is on fourth number in throughput
Recv-Pkt	Maximum packets are received under AODV compared	Using DSDV the received packets are minimum	Lower no of packets are received in this protocol	In this the received packets number is higher	After ZRP it has higher no of received packets

	to all other protocols		compared to others	after AODV	
Pkt-loss	It gives the worst performance in packet loss after OLSR	No of packet loss are higher than DSR but less than AODV and ZRP	It gives the best performance in packet loss	It comes second in maximum packet loss after AODV	Maximum packet loss occur in OLSR without black hole

6. FUTURE SCOPE

The performance of various routing protocols are analysed on the basis of different parameters. In the future the work will be done on the security issues in routing protocols to enhance the security and to make the network more secure.

7. REFERENCES

[1] T. Santhamurthy, "A Comparative Study of Multi-hop Wireless Ad-hoc Network Routing Protocols in MANETs", International Journal of Computer Science, pp. 176-184, 2011.

[2] G. S. Tomar, M. Dixit and S. Verma, "AODV Routing Protocol with Selective Flooding", IEEE Internatonal Conference of Soft Computing and Pattern Recognition, pp. 82-686, 2009.

[3] A. Kumar, P. Singh, V. Kumar, Dr. N. Tyagi, "Performance Analysis of AODV, CBRP, DSDV and DSR MANET routing Protocol using NS2 Simulation", International Journal on Computer Network and Information Security, vol. 5, no. 9, pp. 45-50, 2013.

[4] K. U. Rahman, R. Khan and A. V. Reddy, "Performance Comparison of On-Demand and Table Driven Ad-hoc Routing Protocols using NCTU ns", IEEE International Conference on Computer Modeling and Simulation, pp. 336-341, 2008.

[5] S. Dalal, S. Singh, " Comparative Study of Reactive On Demand Routing Protocols for Mobile Ad-hoc Network", International Journal of Computer Science and Engineering Technology, vol. 3, no. 7, pp. 243-250, 2012.

[6] I. Vijaya, P. B. Mishra and A. R. Dash, "Influence of Routing Protocols in Performance of Wireless Mobile Ad-hoc Network", IEEE Second International Conference on Emerging Applications of Information Technology, pp. 340-344, 2011.

[7] S. S. Khushwah and G. S. Tomar, "Investigation of Effects of Mobility on Routing Protocols in MANET", International Journal of Computer Science Issues, vol. 8, no. 5, pp. 176-184, 2011.

[8] D. Dembla and Y. Chaba, "Performance Analysis of on Demand Routing Protocols of Mobile Ad-hoc Networks and Comparative Study", The Journal of Computer Science and Information Technology, vol. 3, pp. 30-34, 2006.

[9] C. Putta, K.B. Prasad, D. Ravilla and M. Chandra, "Performance of Ad-hoc Network Routing Protocols in IEEE 802.11", IEEE International Conference on Computer and Communication Technology, pp. 371-376, 2010.

[10] A.Bali, S.N. Singh," Comparing Performance of AODV, DSR, DSDV, ZRP with Black Hole Attack and without Attack through Use of NS2 Simulator", International Journal of Applied.

[11] Engineering Research ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32741-32755.