Performance Evaluation of DSR and GRP under Black Hole Attack

Amritbir Singh
Punjabi University Regional Center for Information Technology and Management Mohali

ABSTRACT

Mobile Ad Hoc Network is a dynamic network which formed by collection of wireless nodes without any centralized support. Due its features mobile ad hoc network is more prone to security attacks.Black Hole Attack is one of them.Back hole attack is type of security attack in which all data packets routed towards node which not actually exist it drop all data packets.This research paper evaluate the performance of two mobile ad hoc network routing protocols DSR and GRP under black hole attack on certain parameters like end-to-end delay, network load and throughput.OPNET Modeler 14.5 is used as simulation tool. On the basis of observation it found GRP performs better as compared to DSR under black hole attack.

General Terms

Mobile Ad Hoc Network, Routing Protocols, Black Hole Attack

Keywords

MANET, DSR, GRP, OPNET

1. INTRODUCTION

Security is an important element for every network.The availability of network services,confidentially and integrity depends upon security of network.Mobile Ad Hoc Network is type of network which is formed by collection of nodes.Each node in mobile ad hoc network is connected with other nodes over wireless links to form a network in the absence of pre-defined infrastructure. Due to its characteristics like dynamic topology, wireless links, cooperative algorithms,lack of defense mechanism,limited resources mobile ad hoc network is more prone to security attacks.In mobile ad hoc network nodes communicate among each other with blind mutual trust if node become malicious it not easily recognize, it allows attacker to exploit network resources.Wireless links of mobile ad hoc network helps attacker to easily intrude in the network and get access ongoing communication.The attacker takes benefit of these weak points of MANET.Different type of security attacks prevail in mobile ad hoc network.One of them is black hole attack in which attacker node falsely claims itself shortest path to the destination,it receive the data packets from source node and discard it instead of forwarding it to destination node.Thus it slowdown the performance of network and whole network become paralyzed.

The rest of paper is organized as follows Section 2 gives brief description about work done previously.Section 3 gives description about routing protocols.Section 4 gives description about different types of attacks in mobile ad hoc network.Section 5 gives description about black hole attack.Section 6 gives description about simulation tool used for getting and analyzed the results. Section 7 gives description about performance metrics on its basis behavior of routing protocols is analyzed.Section 8 gives the description about how simulation is formed.Section 9 represents the conclusion.

2. RELATED WORK

Many researchers shown their keen interest in evaluation of mobile ad hoc network routing protocols under black hole attack some of them discuss below:

Harjeet Kaur et al [7] presents performance evaluation of three routing protocols AODV, OLSR and ZRP under black hole attack with 50 nodes and varying number of source nodes 5, 10, 15,20,25,30 on the basis of different parameters like packet delivery ratio, average jitter, throughput and end-to- end delay. The CBR traffic pattern was used and results collecting and analyzing by Qualnet 5.1.At the end author concluded that AODV performs better as compared to other two routing protocols.

Irshad Ullah et al [8] presented performance evaluation of AODV and OLSR under black hole attack on the basis of different parameters such as end-to-end delay, network load, throughput with 16 and 30 nodes by using OPNET Modeler 14.5.Author compared the working of both routing protocols under normal operation and black hole attack at end he concluded that AODV is more vulnerable as compared to OLSR under black hole attack.

Najiya Sultana et al [11] presents performance evaluation of two routing protocols with 16 and 30 nodes under black hole attack. The performance of these routing protocols are evaluated on the basis of end-to-end delay, network load and throughput by using OPNET Modeler 14.5.At the end author concluded that AODV is more vulnerable as compared to OLSR under black hole attack.

Vandna Dahiya [14] presented performance evaluation of two routing protocols AODV and OLSR with 21 nodes under black hole attack The evaluation is drawn on the basis of different parameters like end-to-end delay,network load and throughput. Network Simulator 2.35 is used as simulation tool.At the end author concluded that OLSR performs better as compared to AODV.

3. ROUTING PROTOCOLS

Routing protocols in mobile ad hoc network mainly categorized as follows:

A. Proactive Routing Protocols

It is type of routing protocol in which each node has their own set of routing tables and it has stored information about other nodes on network in its routing tables. The main advantage of this type of routing protocols are nodes can get route information immediately for establish a link.

B. Reactive Routing Protocols

It is type of routing protocol in which route can establish when it needed by source node for forwarding data packets to destination node.The reactive routing protocols used flooding technique for discovery of routes.Once route will discover it stored and maintained in route cache.The main advantage of this type of routing protocols is it will save the precious bandwidth of ad hoc network.

C. Hybrid Routing Protocols

It is type of routing protocol which acquires the features of both reactive and proactive routing protocols.In hybrid routing protocols whole network divided into different zones and each zone assign Zone ID.These Zone ID helps to easily recognize the physical location of node on network.The main advantage of hybrid routing protocol is it uses minimum network bandwidth as compared to other types of protocols in forwarding of packets from source node to destination node.The different routing protocols in MANET are depicted in Figure 1

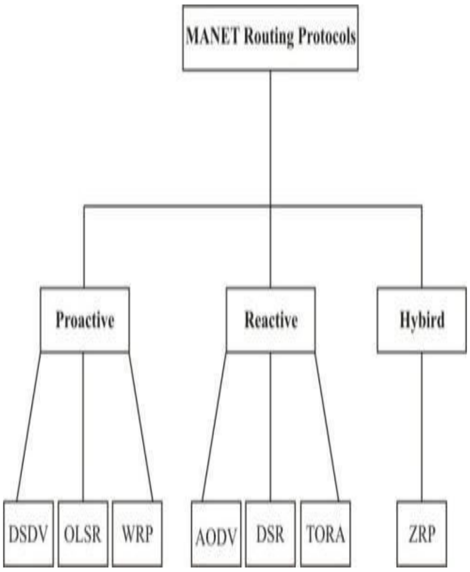

Figure 1: Diagrammatic Representation of Routing Protocols

3.1 Dynamic Source Routing (DSR)

Dynamic Source Routing protocol is on demand routing protocol which used source routing approach for forwarding data packets from source node to destination node. Source routing is an approach in which data packet header contains complete list of nodes from which data have to pass.This help to source node it has complete knowledge of path to the destination before forwarding data packets and no need to forward periodic messages therefore it uses minimum bandwidth.DSR performs two types of functions:Route Discovery and Route Maintainence.When source node wants to establish a connection it transmits RREQ(Route Request) message to each intermediate node when each intermediate node received this message it retransmit it, until it either reach to the destination node or intermediate node has information about route to destination node in its route cache.Once destination node received RREQ(Route Request) message it transmits REP(Route Reply) message towards source node and stored information about route in its route cache for future use.When RREP(Route Reply) message traverses backward to source node all intermediate nodes know that route is established between source and destination nodes.Route information stored in their route cache.If the link fails the destination node transmits RERR(Route Error) message to source node.The RERR (Route Error) message is generated by destination node to inform source node that link is failed and no longer valid. If links failed the source node removed its information from it route cache. If information about new route to destination is available in route cache it is replaced with previous one.If no such link available in route cache route discovery is reinitiated [4].

3.2 Geographical Routing Protocol(GRP)

Geographical Routing Protocol is a position based routing protocol.Geographical Routing Protocol assumes two assumptions that nodes are aware about their own and their immediate neighbor’s geographical positions.The source node is already known the geographical position of destination node. In geographical routing protocol each node periodically updates positions of its immediate neighbors by beaconing. Beaconing is type of approach which is used to collect the link-state information of neighboring nodes.In beaconing each node send beacon or packet to inform neighboring nodes about its existence.After that neighboring node responds the beacon or packet sent by node and the positions of neighboring nodes updated.The routing table is not used geographical routing protocol for routing of data to destination it depends upon the information available with each node about its immediate neighbors. Global Positioning System(GSP) helps in easy delivery of messages.Under the assumption of bidirectional connectivity geographical routing protocol efficiently implemented on planner graph.Two types of routing algorithm are used:Greedy Routing and Face Routing Algorithm.In greedy routing data packets brought closer to destination node in each step by selecting suitable neighbor. The suit able neighbor is one who reduces distance between sources to destination in each step. The face routing is type of routing in which considered that each regions is separated by edges of planner graph. The routing algorithm takes way around the face it begins from the point closest to the destination and explores next face closest to destination.Face routing always find path to the destination .Greedy routing is failed if there is no next hop closest to destination find among neighbor nodes. Then greedy routing switches over to perimeter mode forwarding and then it continues t o explore next closest point to destination [1].

4. ATTACKS IN MANET

Attacks in mobile a d hoc network mainly categorized as follows:

4.1 Internal Attacks

It is those type of attacks in which attacker wants to cause congestion transmit fake routing information or not allow nodes to provide services.

4.2 External Attacks

It is those type of attacks in which attacker wants to access the network and participate in network activities.

4.3 Active Attacks

It is those type of attack in which attacker tried to destroy or alter the data exchanged on network. The active attacks can be external or internal.In external active attacks attacker or malicious node from outside the network. But in internal active attacks attacker or malicious node from inside the network.

Active Attacks further classified into following types:

4.3.1 Dropping Attack

It is type of attack in which malicious node dropped all the data packets which forward towards for transmission.It prevents end-to-end communications between nodes thus whole network become stun. If malicious node reached its critical point it starts transmitting data packets to new destinations. Thus network performance decreases.

4.3.2 Modification Attacks

It is type of attack in which attacker modifies the data packets and disturb the network communication. Sinkhole Attack is an example of modification attacks in this attack attacker tried to attract network traffic with the help of malicious node. This attack mostly affects the routing protocols which used advertised information of such as nearest node to destination in route discovery process.

4.3.3 Fabrication Attacks

It is type of attack in which attacker falsely send route reply message when it receive route request message from source node and falsely claims fresh route to destination.

4.3.4 Timing Attacks

It is type of attack in which attacker attract other nodes by claiming itself node closer to actual node.DoS attacks rushing attacks and hello flooding attacks use this technique.

4.4 Passive Attacks

It is those type of attacks in which attacker node gets the information about the transmitted on network instead of alter or change it.This attacks are major risk to the security of network and very hard to detect. One solution for this problem is data can be encrypted by using powerful encryption techniques.

Passive Attacks further classified into following types:

4.4.1 Eavesdropping

It is type of attack in which attacker wants to collect confidential information such as location of node, public key, private key which kept secret during communication.

4.4.2 Traffic Analysis

It is type of attack in which attacker monitor network traffic to get information about source and destination node.The different network layers attacks in MANET are depicted in Table 1

Table 1 Different Network Layers Attacks

Network Layers	**Attacks Types**
Application	Malicious Code, Data Corruption,Viruses and Worms
Transport	Session Hijacking Attack, SYN Flooding Attack
Network	Black hole, Wormhole, Sinkhole, Link Spoofing, Rushing Attack, Reply Attack Link Withholding, Resource Consumption Attack, Sybil Attack
Data Link	Selfish Misbehavior, Malicious Behaviour,Traffic Analysis
Physical	Eavesdropping, Jamming Active Interference

5. BLACK HOLE ATTACK IN MANET

Black Hole is type of attack in which malicious node uses its routing protocol falsely claims it have a shortest path towards destination node and advertises its availability of fresh route towards destination node without checking its routing tables.Therefore malicious node is always available to reply route request of source node.The flooding technique is used by malicious node for transmit route reply message in response of source node route request message before actual node respond. Thus forged route is created, now it is up to the node whether it drops the data packets or forwarding it on unknown address.Black Hole Attack explained in Figure 2 in which node “A” wants to send data packets towards node “D” and it initiate route discovery process but node “C” is malicious node it falsely claims itself active route towards specified destination node as soon it receive route request message than it send route reply message to node “A” before any other node.Node “A” consider it as active route and active route discovery is complete.Node “A” will ignore other node requests and starts sending data packets towards node “C” thus all data packets will lost or send to unknown destination.Due to this network overhead will increased and precious bandwidth of network is wasted.

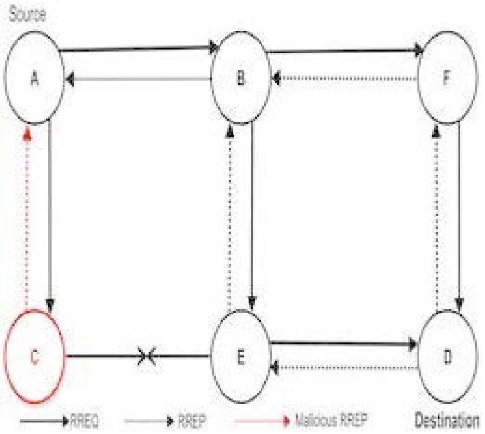

Figure 2: Black Hole Problem

6. SIMULATION TOOL

In this research collection and analysis of results are performed on OPNET Modeler 14.5.OPNET is widely used commercial network simulator to simulate heterogeneous network like ad hoc networks.It has huge library of network models and protocols which help in designing and modeling of communication networks efficiently.OPNET is used graphical user interface so it easy to simulate networks in OPNET as compared to other network simulators.OPNET incorporates number of features to support an increase stability and mobility in the mobile ad -hoc network.A number of routing parameters of MANET are supported by OPNET Modeler and it is easy to design network in OPNET Modeler and to evaluate the performance of these routing protocols.These parameters are known as performance metrics.The specific application and transport layer protocols demand their own set of performance metrics to evaluate the network efficiency.In this study, the performance of these routing protocols is evaluated on the basis of three parameters which are end-to-end delay,network load and throughput. Performance of these routing protocols are evaluated for the selection of efficient routing protocol for the network.

7. PERFORMANCE METRICS

1. End-To-End Delay

End-To-End Delay represents average time that taken by a data packet to reach its destination. This metric is calculated by subtracting time taken by first data packet to traverse the network from time at which first data packet arrived to destination.

2. Network Load

Network load represents the bit/sec load submitted by all higher layers in all WLAN nodes of the network to wireless LAN layers. When more traffic is coming on the network it is difficult for network to cope up with this heavy load of traffic it is called network load. Heavy load on network may affect the performance of network. The performance of network is decreases. In heavy load data packets may collide this may cause congestion on the network and makes the routing process slow.

3. Throughput

It is ratio of total amount of data transfer from sender to receiver and time taken by receiver to receive last packet of data from sender. In other words we can say that it calculates how constantly data is provided by network to receiver. Throughput is the number of data packets arriving at receiver per milliseconds.

8. SIMULATION AND PERFORMANCE ANALYSIS

Simulation process is divided into different scenarios. All nodes are randomly deployed under static linear fashion in campus network environment of 4000X4000 square meters.FTP with high load traffic is used as traffic pattern. The file size is 50,000 bytes .Every node moves with constant speed of 10 m/s with 80 seconds pause time.All nodes are defined as manet stations with one WLAN server.WLAN connection speed is 11 Mbps.The simulation time is 10 minutes.The parameters used in this study are summarized in Table 2:

Table 2: Parameters of Simulation

Parameters	**Value**
Simulator	OPNET 14.5
Number of Nodes	10 and 20
Maximum Speed	10 m/s
Simulation Time	10 minutes
Pause Time	80 sec
Environment Size	4000X4000
Packet Inter Arrival Time	exponential(1)
Packet Size	exponential(1024)
Traffic Type	FTP
Mobility Model	Random Waypoint
Data Rate	11 Mbps
Addressing Mode	IPv4

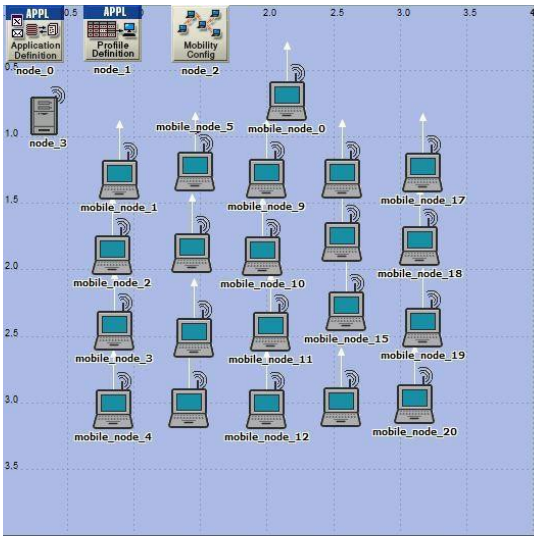

Figure 3: Simulation Scenario Having 20 Nodes

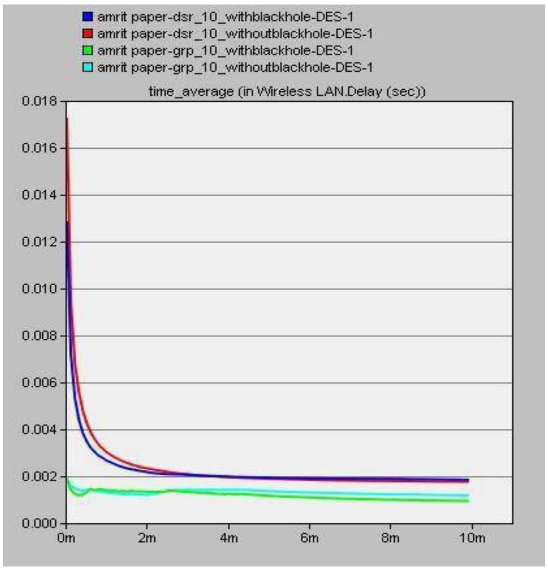

Figure 4: End-To-End Delay for 10 Nodes

In end-to-end delay the behavior of attack is depends upon protocol type, routing procedure and number of nodes. In figure 4 evaluation of two routing protocols namely DSR and GRP in terms of end-to-end delay for 10 nodes under normal operation and under black hole attack is presented. The results of black hole attack are compared with results of normal operation to analyze the overall effect of black hole attack on whole network. It is evident from the graph that end-to-end delay is higher in DSR and GRP under normal operation as compared to DSR and GRP under black hole attack because in black hole attack route request and route reply is not needed the malicious node send its route reply to source before destination node and establish link with destination node and starts sending data packets it exhibits less end-to-end delay. The end-to-end delay is higher in DSR as compared to GRP due its reactive nature.

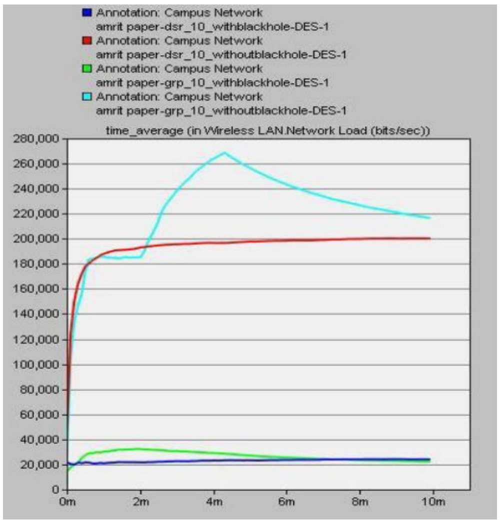

Figure 5: Network Load for 10 Nodes

In figure 5 evaluation of two routing protocols namely DSR and GRP in terms of network load for 10 nodes under normal operation and under black hole attack is presented. It is evident from graph network load is minimum in DSR and GRP under black hole attack because malicious node discard all data packets instead of forwarding it within network it affects on network load it decreases.When comparison drawn between both routing protocols it found that network load is higher in GRP under black hole attack as compared to DSR.

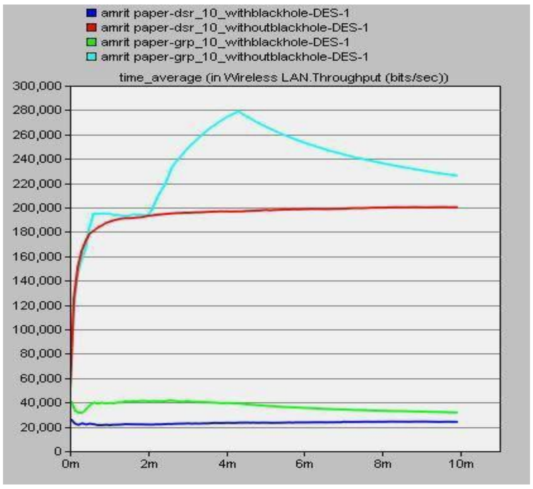

Figure 6: Throughput for 10 Nodes

In figure 6 evaluation of two routing protocols namely DSR and GRP in the terms of throughput for 10 nodes under normal operation and under black hole attack is presented. Due to discarding of data packets by malicious instead of forwarding it within network it affects the throughput. It is also evident from graph that throughput in DSR and GRP under normal operation is higher as compared to DSR and GRP under black hole attack. The throughput is higher in GRP under black hole attack as compared to DSR.

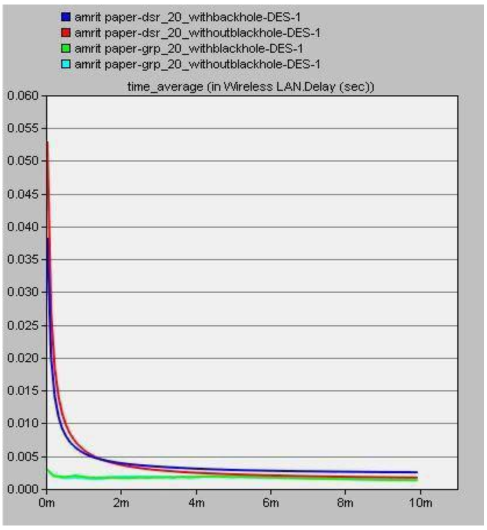

Figure 7: End-To-End Delay for 20 Nodes

The percentage of end-to-end delay slightly increases in figure 7 due to increasing number of nodes.In figure 7 evaluation to two routing protocols namely DSR and GRP in terms of end-to-end delay for 20 nodes under normal operation and under black hole attack is presented.It is evident from graph that end-to-end delay is higher in DSR and GRP under normal operation compared to DSR and GRP under black hole attack.The end-to-end delay is higher in DSR as compared to GRP under black hole attack.

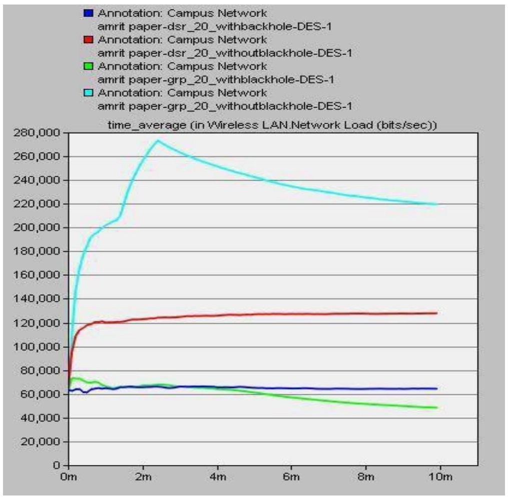

Figure 8: Network Load for 20 Nodes

In figure 8 evaluation of two routing protocols namely DSR and GRP in terms of network load for 20 nodes under normal operation and under black hole attack is presented. It is evident from graph that network load is higher in DSR and GRP under normal operation as compared to DSR and GRP under black hole attack.This is due to discarding of data packets by malicious node under black hole attack instead of forwarding it within network.The network load in GRP under black hole attack is higher as compared to DSR.

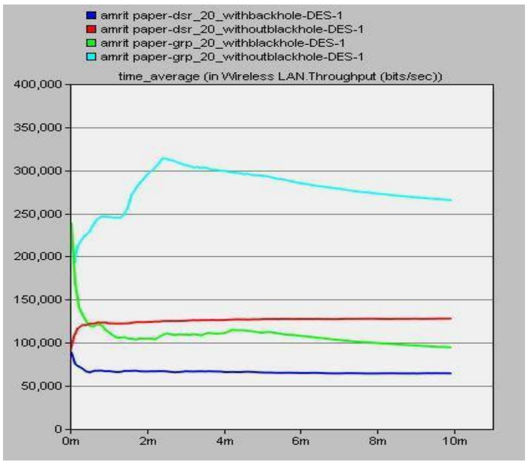

Figure 9: Throughput for 20 Nodes

In figure 9 evaluation of two routing protocols namely DSR and GRP in terms of throughput for 20 nodes under normal operation and under black hole attack is presented. The data packets discarded by malicious node instead of forwarding it within network it affects the throughput. It is also evident from graph that throughput is higher in DSR and GRP under normal operation as compared to DSR and GRP under black hole attack.The throughput in GRP under black hole attack is higher as compared to DSR.The resultant values are depicted in Table 3.

Table 3: Resultant Values

Protocols	Number of Nodes	End-To-End Delay(Sec) Without Attack	End-To-End Delay(Sec) With Attack	Network Load Bit/Sec) Without Attack	Network Load Bit/Sec) With Attack	Throughput Bit/Sec) Without Attack	Throughput Bit/Sec) With Attack
DSR	10	0.01729	0.01289	214089	44868	214016	44868
GRP	10	0.002382	0.002403	432125	42292	447267	56019
DSR	20	0.05296	0.03834	147672	83385	147731	83385
GRP	20	0.006332	0.004410	394575	84024	509377	208413

9. CONCLUSION

Loop Holes of network attract attackers to exploit network resources.Routing is process to select best path for forwarding of data packets from source to destination.In routing process routing protocols play very important role. Without routing protocols routing cannot be imagined. Routing protocols is mechanism which is used to route data packets from source to destination. If routing protocols affected by network security attack whole routing process will parlysed.To avoid destruction caused by these network security attacks it is mandatory for every routing protocol to more secure against these type of network security attacks. This research presents evaluation of two routing protocols DSR and GRP under black hole attack.The evaluation is drawn in terms of end-to-end delay,network load and throughput.Both routing protocols are compared under normal operation and black hole attack.The objective of this research to found that which routing protocol is more vulnerable under black hole attack.On the basis of observations it found that in terms of end-to-end delay DSR is more vulnerable as compared to GRP under black hole attack.The severance percentage between two routing protocols is 2% to 5% in case of GRP and 5% to 10% in case of DSR.In terms of network load DSR is less affected as compared to GRP.In terms of throughput DSR affected more as compared to GRP.Thus it concluded that GRP performs better under black hole attack as compared to DSR.

10. REFERENCES

[1] A Tamizhselvi,Banu Wahida,R.S.D,"Performance Evaluation of Geographical Routing Protocol Under Different Scenario", International Journal of Computer Science and Telecommunications(IJCST),ISSN 2047-3338,Vol.3,No.3,pp 64-67,2012

[2] Bo Sun,Yong Guan,Jian Chen and Udo W.Pooch, "Detecting Black Hole Attack in Mobile Adhoc Networks", The Institute of Electrical Engineers, Michael Faraday House, Six Hill Way,Stevenage,SGI2AY,EPMCC,2003

[3] C.S Murthy, B.S Manoj, "Ad Hoc Wireless Networks: Architectures and Protocols", Pearson Education,2004

[4] D Johnson Hu, D Maltz, "The Dynamic Source Routing Protocol (DSR) For Mobile Ad Hoc Networks for IPv4", IETF, RFC 4728,February 2007

[5] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, "A Survey of Black Hole Attacks in Wireless Mobile Adhoc Networks", Human Centric Computing and Informational Sciences, A Springer Open Journal, 2011

[6] Gagandeep,Aashima,Pawan Kumar, "Analysis of Different Security Attacks in MANETS on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology(IJEAT),ISSN 2249-8958,Vol.1,No.5,pp 269-275,2012

[7] Harjeet Kaur,Manju Bala,Varsha Shani, "Performance Evaluation of AODV,OLSR and ZRP Routing Protocols Under The Black Hole Attack in MANET",International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering(IJAREEIE),ISSN(Print) 2320-3765 ISSN(Online) 2278-8875,Vol.2,No.6,pp 2555-2563,2013

[8] Irshad Ullah,Shahzad Anwar, "Effects of Black Hole Attack on MANET Using Reactive And Proactive Protocols", International Journal of Computer Science Issues(IJCSI),ISSN(Print) 1694-0814 ISSN(Online)1694-0784,Vol.10,Issue 3,No.1, pp 152-159,2013

[9] Ms. Gayatri Wahane and Prof. Ashok Kanthe, "Technique for Detection of Cooperative Black Hole Attack in MANET", IOSR Journal of Computer Science (IOSR-JCE), e-ISSN 2278-0661, pp 59-67,2014

[10] Mohammad Al-Shurman and Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Adhoc Networks", AMCSE 04, April 2-3, Huntsville, AL, USA, 2004

[11] Najiya Sultana ,S.S Saragdevot, "The Effects of Black Hole Attack in Mobile Ad Hoc Network Using OLSR and AODV",International Journal of Science and Engineering Investigations(IJSEI),ISSN 2251-8843,Vol.2,No.15,pp 97-102,2013

[12] Neha Kaushik and Ajay Dureja,"A Comparative Study of Black Hole Attack in MANET",International Journal of Electronics and Communication Engineering and Technology(IJECET),Vol.4, Issue 2,pp 93-102,2013

[13] P.V.Jani,"Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop,September 2002

[14] Vandna Dahiya,"Analysis of Black Hole Attack on MANET Using Different Routing Protocols", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),ISSN 2278 –1323,Vol.3, No.10,pp 3309-3316,2014