DOI: http://dx.doi.org/10.26483/ijarcs.v9i6.6335

ISSN No. 0976-5697

Volume 9, No. 6, November-December 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

DETECTION AND REMOVAL OF BLACK HOLE ATTACK IN MOBILE AD HOC NETWORKS USING GRP PROTOCOL

Amin Salih Mohammed/Dean
College of Engineering and Computer Science
Lebanese French University
Erbil, Kurdistan Region, Iraq

M. Sivaram / Assistant Professor
Department of Computer Networking
Lebanese French University
Erbil, Kurdistan Region, Iraq

Dr. D.Yuvaraj/Lecturer
Department of Computer Science
Cihan University- Duhok Campus,
Kurdistan Region- Iraq

V. Porkodi/Assistant Professor
Department of Information Technology
Lebanese French University
Erbil, Kurdistan Region, Iraq

Abstract: An AD HOC Mobile network is a collection of nodes that can be freely, and without any network infrastructure, communicate with each other via radio frequencies **.** Easy implementation, establishment and infrastructureless make AD HOC network to play an important role in various area such as military, emergency, natural disasters, urban campus, etc. Nowadays, development of wireless networks, as well as, information security requirement is growing rapidly. Wireless network security is one of the most important research topics. In this work, the analyze of Gateway Routing Protocol(GRP) and security of this routing protocol is discussed. GRP is selected for this study. In the paper the effect of the Wormhole and black hole attack in GRP routing protocol will be investigated and diagnosing and solution is provided for this type of attack. GRP is a proactive protocol and uses quadrants for fuzzy routing. This controls the amount of flooding done by GRP.

Keywords: AD HOC, GRP routing protocol, Black Hole Attack, Network Security

I. INTRODUCTION

Today's tendency to use wireless networks is increasing day by day, because anyone, anywhere and at any time can use it. In recent years there has been tremendous growth in sales of portable computers. These small computers are equip with several GB of disk, high-definition color screen and wireless network cards. In addition, these small computers can work several hours with battery power, therefore, users are free to easily move them to any side. When users start using their mobile computers, sharing of information between computers became a natural necessity. Sharing information happens in areas such as conference halls, terminals, airports, classes and also in the military environment. Specific mobile wireless networks are a groups that can be set dynamically at any place and at any time without using any form of network infrastructure. They often act as a nodes and at the same time act as a router. In cases of emergency when there is no possibility of building and establishing a pre-defined and fixed structure network, such as the military or floods and etc, this type of network can be used. The network communication between the nodes takes place via radio waves and if one node is in the radio range of another node they considered it as neighbor. Otherwise in the case when two nodes are not within the radio range of each other the connection between them is made through other nodes. Therefore, the communication between the nodes in network takes place on the basis of trust and partnership between them. Today, the network security is an important issue in research about ad hoc mobile network. Node mobility, wireless communications, dynamically change the network structure, the lack of centralized management to investigate the behavior and operations, the lack of specific defense and limited power of nodes, provide suitable environment for various attacks on these networks. Because of specific routing structure of Ad Hoc [1, 2, 3, 5] mobile network that somehow based on a kind of trust between nodes, provides a good opportunity for attackers to participate in the routing process somehow disrupt the routing process and eventually they would disrupt this process. One of the most famous routing protocols in Ad Hoc network is Gateway Routing Protocol(GRP) [4-8]. Many studies have investigated the effect of various attacks on this protocol. GRP for using by mobile nodes in Ad Hoc network. In the Ad Hoc network, this protocols quickly adapt to dynamic link conditions, the memory overhead, and low use of the network and specify the path to the Unicast destination. The protocol to ensure the absence of loop use the sequence number of destination. Using a cycle mechanism of request/replying for a route make a path to destination. When the source node requests a route to the destination, node that currently has no route to that destination broadcast the request packet of source node to all network. Nodes that receive the packet will update their information according to information received from the source node and create some reverse route entry to the source. Otherwise, if the node has a route to requested destination, the node informs the source to send its data through. One type of the attacks in the Ad Hoc network is a black hole [6, 7, 8,21]. This attack is applied by one of the nodes in the network. In this type of attack, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets needed to be intercepted. In a flooding-based protocol, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply consisting of an extremely short route. [9, 10, 12]. In which case a black hole is created and the node is known as a black hole? The malicious node receives/discards data instead of sending to destination. So to solve this problem a new method is presented in this paper and base on the behavior of nodes in the network determines that node is malicious or not.

II. ANALYSIS OF GRP PROTOCOL

Distance vector interior gateway protocol (GRP) developed by Cisco developed by Cisco. GRP protocol quickly adapting to the conditions of links, memory overhead, low using of the network and dedicating unicast of paths to the destination. It uses sequence number of destination to make guaranty of free loop in the network. GRP algorithm provide some capabilities like dynamic, self-starting, Multi Hop routing for those mobile nodes which going to create an Ad hoc network. The protocol able to unicast and multicast routing. The GRP protocol use the algorithm that works on demand, which means the path between nodes created only when it requested by the source node. And save the routes as long as the source needed. GRP uses sequence numbers to ensure the updated information about the condition of the paths. Another notable feature of the protocol is that the protocol create routes without loops, and also using in large scales network which included a lot of mobile nodes[4].

A. Route discovery

When the source node needs to communicate with the destination node, it will first check its routing table whether there exists a valid route to the destination node. If exists, it will send data through this route. If not, the source node will broadcast RREQ (route request packet) to create a route to the destination node [10, 11]. The RREQ packet send by the source node contains two serial numbers, namely the source node serial number and the most recent serial number of the destination node that source node knows. The former is used to maintain a reverse route to the source node and the later shows the newness degree of the route reaching to destination node. Node will choose the item with a larger serial number to create a route.

When node along the route receives RREQ, it will first establish a reverse route to the source node according to the information in RREQ, then it will transmit the RREQ message to its neighbors and to the destination node or an intermediate node with the route to destination node. The destination node or intermediate node will reply a RREP (routing reply packet) to source node along the reverse route. Node receiving RREQ message will establish a forward route to the destination node according to the RREP information, GRP establishes a valid route to the destination node through RREQ and RREP control the sending and receiving messages.

B. Route maintain

Since Ad Hoc network nodes keep moving constantly, any node in the network is likely to move out the effective communication range of its neighbor nodes, and this will cause part link interrupted. So rout maintenance process is necessary in GRP.

When a valid route is established, nodes on the route will periodically broadcast HELLO packets to check the link state of each section on the route, HELLO packet is essentially a special RREP packet, whose TTL is 1, Since TTL is equal to 1, HELLO packet can only propagate one hop distance. When it reaches its neighbors, it will be discarded as its TTL becomes 0 [10], by broadcasting HELLO packets, a node tells its neighbors that it is effective. The neighbor node receiving this HELLO packet considers that the rout between them is complete and available. If after a period of time, a node dose not receive HELLO packet from one of its neighbors or any other grouping, it considers that the route between it and the node has failed,

III. BLACK HOLE ATTACK IN GRP

Attack black hole is divided into two categories:

1. A single black hole attack
2. Cooperative black hole attack

As shown in figure 1 single black hole attacks happen through one of the nodes on the network. It means that this node, regardless of whether its routing table and if there is a route to destination node or not it responds to received RREQ by sending RREP packets. Which results in shortening of RREP packages to this node compared to the other nodes. As a result of other nodes send packets through this node considered as an appropriate route and short route for sending their packages. In this case, the black hole is created and the node which indicated as black hole receives information or discards all data packets instead of sending to destination. If the black hole node introduce itself as a shortest route to others nodes in the network, in this case all packets will be lost, which leads to Denial Of Service.

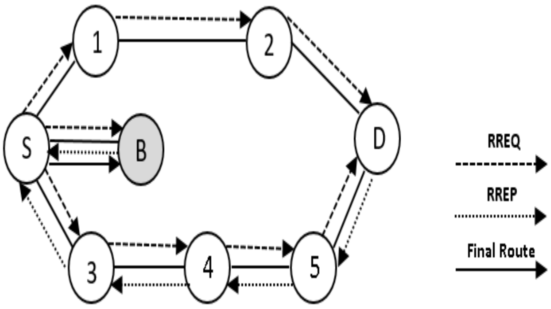
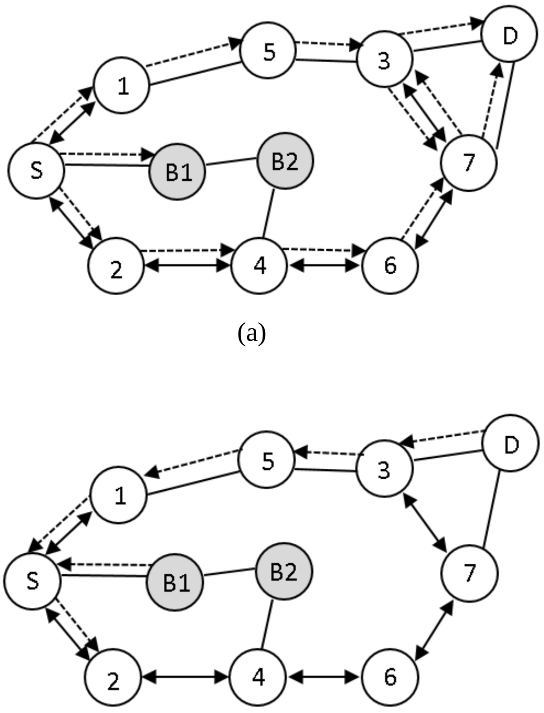


Figure (1): Single Black Hole Attack

Another type of black hole attack is Cooperative black hole attack, in which there are more than one black hole nodes that these nodes cooperate together (figure 2).



(a)

Figure (2): (a), (b) Cooperative black hole attack

IV. SOLUTIONS TO ACHIEVE SECURE LEVEL IN AD HOC NETWORKS

In [12] proposed solution to a single black hole, In that solution, information of next hope to destination should be included to RREQ package, when the intermediate group will respond to the RREQ. Then the source node resends a request (FREQ) to the next hope of responsive node and asks about responsive node and route to destination. Using this method can be detected reliability of the responsive node if the next hope is reliable. This solution cannot prevent attack in MANET during cooperative black hole. For example, if the next hope in cooperation with the responsive node, respond for FREQ for each question will be simply yes. As a result, the source trust to the next hope and sends data through responsive node. Which is a black hole. In [13] the proposed method requires the intermediate nodes to send confirmation request or CREQ to the next hope. After that, the next hop received CREW, search a new path in its memory to find a path to destination. If there is a path then sends verified answers (CREP) with information about route to the source node. The source node identifies the validation of the route in RREP by comparing information in CREP. As a result, the additional operation is added to the routing protocol, the load of this method is high. In [14] the source node finds more than one route to destination. Source node waits to receive RREP packets from more than two nodes. This route will be delayed because the node has to wait until it receives RREP from more than two nodes. Therefore, a method is needed that can navigate without delaying and increasing overhead to prevent the attack of a black hole. In [15] when node start to broadcast RREQ, around the node issued a consultation process carried out, then, based on comments of neighboring nodes, made a decision if there is malicious node or not. All the above methods have been used to single Black Hole Attacks.

In [17] another solution is provided to prevent Cooperative Black Hole Attack. This approach designed to combat the Black hole attack to make use of a ‘Fidelity Table’ wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a ‘Black hole’ and is eliminated.

V. PROPOSED METHOD

In the proposed method which is based on the behavior of nodes in the network determines and makes a decision of malicious node.

1. Record next information about the activity of nodes:
   - The number of data sent to neighboring nodes;
   - The number of data received from a neighboring node;
   - The number of REPLY packets received from a neighboring node;
2. Send request packet Comments of neighbors about the neighboring node which has sent a REPLY packets;
3. Receive the recorded information from the neighbor nodes of the node which send the REPLY packets;
4. Evaluate the information received and give the comments about the malicious node;

Here, it is mean if the node is not active during the process of data communication with other neighbor nodes, then the node is malicious and should send to quarantine.

5. Send a risk package to quarantine the malicious node;
6. Remove the quarantined nodes in the routing process.

In the proposed method, each network node has a following data structure:

- Each node contains a table of neighbors and their behavior. Each entry in this table indicates that neighboring node (with identified ID) how many data, how many REPLY packets sent to this node, and the node how many data packet delivered to a neighbor.
- Each node has a list of groups node that are in quarantine which should be removed in the routing process

Malicious nodes are nodes that respond to RREQ packets by sending RREP packets. And a large number of data packets delivered to it, but at least have been send by it to the neighbors. When a node, receives a RREP packet from its neighboring node, if the node responding to RREQ is a central node and is not a destination node, investigated whether respondent’s node is not one from quarantine groups. If the node is a malicious node RREQ packet is discarded. Otherwise, the voting process can be carried around responding node to acquire all activities of the node. Then based on the information collected evaluate the node and if it is malicious node broadcast an alarm message in the network is quarantined to place the node in quarantine.

The proposed algorithm was implemented on GRP protocol and to conduct its operations use several new packets:

1. Packet which request information about a node. Packet includes: node ID in question, ID of request Sender and Time to live of packet.

2. Information package of neighboring nodes about a node in question: This package includes a number of data packets received from the target node, number of packets sent to the target node and the number of RREP packets received from the target node.

3. Alert packets: this package includes nodes that are known as malicious and must be in the quarantine list.

The advantages of the proposed method is that the node starts the consultation process that received a packet from a none-safe node. That is if a node already has safety proved, no necessary to take opinions of them. This will reduce the overhead of the proposed algorithm. Second, when requesting information Table of neighboring nodes are updated to reduce the overhead of the algorithm.

VI. SIMULATION ENVIRONMENT AND SIMULATION RESULTS

Our simulation model was carried out using the OPNET Modeler 14.0[18, 19]. It is a useful research tool for achieving good simulation results. This network has 50 nodes and has been divided into four mobility domains. Within each domain, the nodes are set to move at speeds of 25m/s using random mobility. The size of the quadrant for GRP is set to 1000m. All scenarios are run under identical mobility and traffic conditions. The performance metrics chosen for the evaluation of our algorithm with black hole were total packet dropped, traffic sent and received, wireless end to end delay, network throughput and network load. The network topology graph for 50 nodes is shown below. (Figure 3).

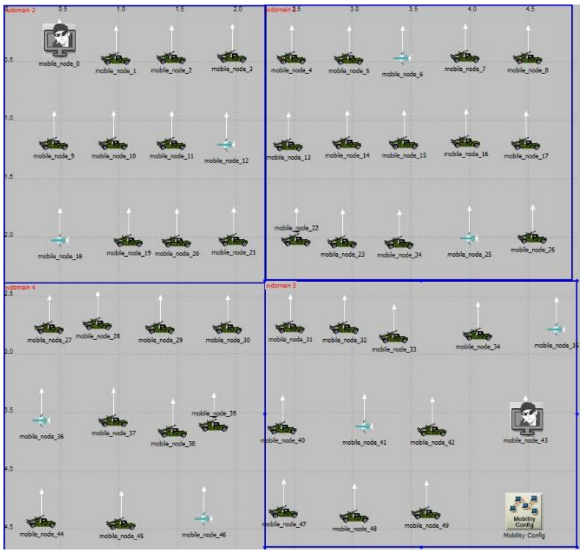


Figure 3: Network topology and animation graph

Other simulation parameters are set in table 1:

Table I. The simulation parameters setting

Ad Hoc Network Parameters	**Values**
Route Request Retries	5
Route Request Rate (pkts/sec)	10
Active Route Time Out (Seconds)	**15 s**
Hello Interval (Seconds)	**Uniform (5,6)**
Allowed Hello Loss	2
Net Diameter	35
Node Traversal Time (Seconds)	0.04
Route Error Rate Limit (pkts/sec)	10
Time Out Buffer	2
TTL Threshold	7
Addressing Mode	**IPV4**

After creating scenarios it should settings the node (Node 4) as an attacker with black hole's attack according to the table below.

Value	**Simulation parameters**
67	Number of nodes
1000*1000(m)	Network size
600(sec)	Simulation duration
.0001	Transmit power(w)
-95	Packet Reception-power Threshold(dBm)
SHA-1	Hash function
Mobile-node-4	Source node
Mobile-node-60	Destination node
Uniform(.1, 1.1)	Packet Inter-Arrival

	Time(sec)
Exponential(1024)	Packet size(bits)

Table (2) Attacker with black hole's attack

Figure 4 shows the average delay of the entire wireless network shows up . It is shown that the delay is almost has equal value in the scenario without, attack and wormhole. So, the delay did not affect the entire network are even less delay. This is because the nature of the wormhole to create a tunnel between two attacker nodes that ignoring all nodes between them during data transmission. So, did not affect on the total delay of the entire network, even reduce the total delay. In the scenario with black hole because of the nature of the attacker node, transmission of the HELLO and RREQ occurs much earlier and more frequently. In this case, most of the data stream to this node and a lot of them will be DROP, therefore total network delay lower than usual.

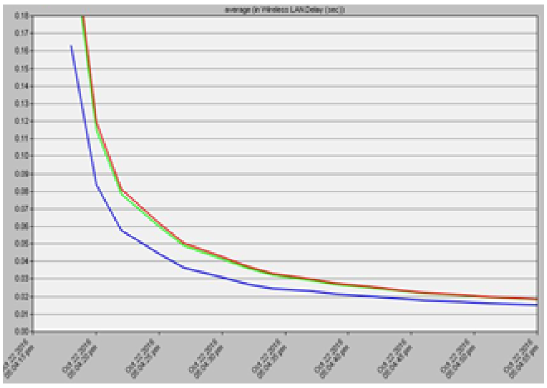


Figure 4: Packet Delivery Ratio versus mobility Speed

In this figure, once can see that in the scenario without attacking the throughput of the entire network is clearly better than throughput with wormhole and at the end the scenario with black hole attack has lower throughput.

Figure 5 shows that the proposed method has additional overhead because of request broadcasting, however, due to update routing tables, additional overhead volume decreases. In AODV3 because malicious node always suggests a route to other nodes, so it has less overhead. It should be noted that this protocol deliver very little data.

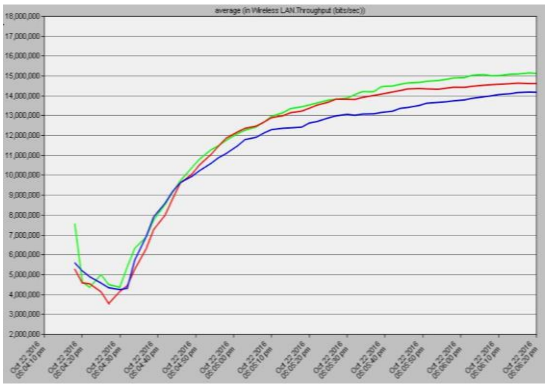


Figure (5): Overhead of the algorithm

The total amount of received network traffic shows that black hole attack is most harmful to the network, but wormhole attack because of a hidden tunnel data shows the highest of the received data.

As shown in figure 5 the AODV3 has the lowest overhead, therefore, it has the least delay. Also the proposed method due to send the lower RREQ packets has the lowest delay.

In the proposed method when the nodes have a low speed because it may be difficult to establish routes between nodes or even impossible to establish the route, more RREQ request have been sent. And also due to the lack of sufficient data, frequently request for comment will be sent. As shown in figure 6 this causes a delay in begin of the proposed method.

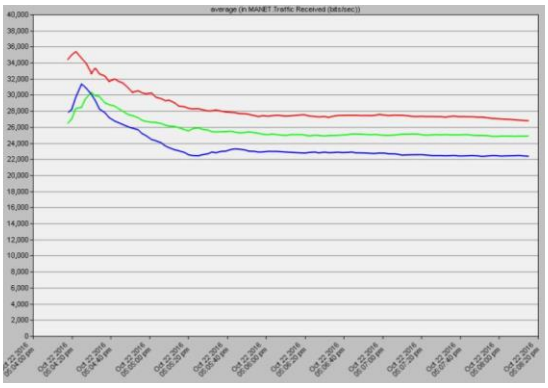


Figure (6): Packet received versus mobility speed

Because the proposed method has high latency and overhead number of the data packets received is very low. As the speed increases it will identify and quarantin the malicious node shows in Figure 7.

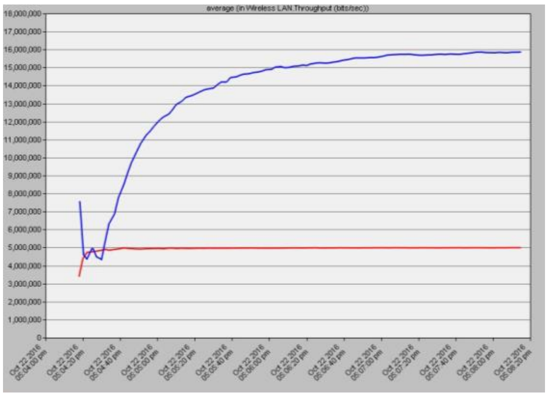


Figure 7: Average End to End Delay versus mobility speed

The overall wireless network delay in these two protocol shows that the OLSR protocols has lower delay. This is because the mechanism of the protocols. AODV is more stable and faster than OLSR in two scenarios with wormhole, delay for OLSR is lower, but the difference is small is shows in figure 8.

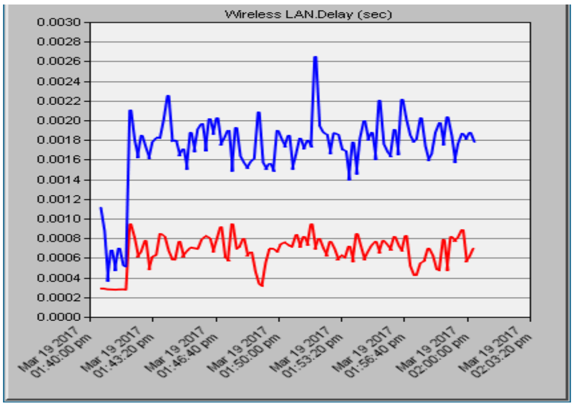


Figure 8 : OLSR is lower, difference is small

Throughput in AODV is more than OLSR protocol, this is due to the much more request for sending and receiving data. On the other hand, OLSR the amount of receiving traffic is on the rise because of lower latency compared to AODV, it shows in figure9.

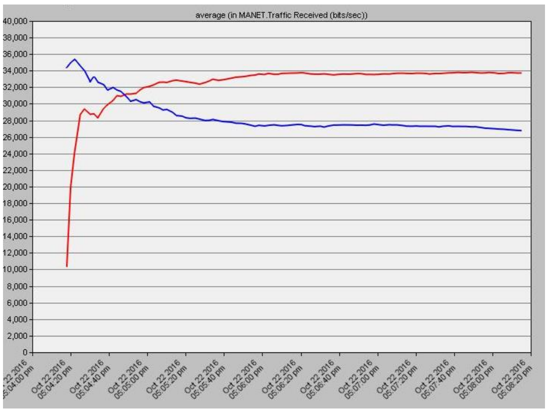


Figure 9. Lower latency compared to AODV

According to the amount of data drop in the two protocols can be concluded that AODV traffic receiving is declining due to increasing dropping. It shows in figure 10.

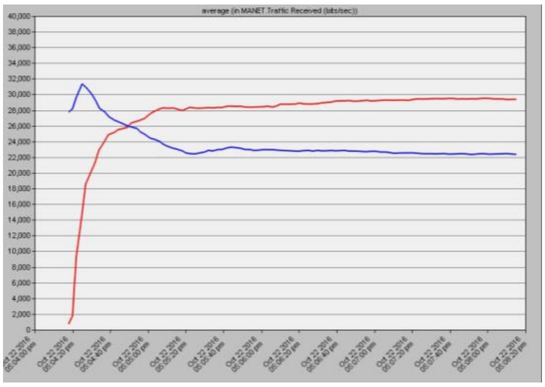


Figure 10 : AODV traffic receiving is declining due to increasing dropping

VII. Conclusions

In this paper proposed a method to detect and prevent black hole attack in ad hoc mobile network, which with a minimum of cost or overhead could detect malicious nodes and put in quarantine. This method because of its simplicity of implementation and low overhead can be used in networks. - The proposed method can accurately predict and detect malicious nodes. When the number of malicious node is low, with very little costs can detect them. - The proposed method has additional overhead because of request broadcasting, however, due to the update of the routing tables, additional overhead volume decreases. The implementation of the proposed algorithm has not complicated and can easily be implemented Simulation and analysis of the protocols show that the network with OLSR routing protocol has a better performance than AODV routing protocol in terms of attacking (Wormhole and Blackhole attacks).The result illustrates the comparison of GRP and OLSR in such a scenario with high mobility. The amount of MANET traffic received is comparible in both scenarios. Also the amount of routing traffic sent is better in GRP over OLSR.

VIII. References

[1] Sajal, S., Raja, D., and Abderrahmane L.(2016). A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. Elsevier,Volume 37, Part 2, (209–227).

[2] Moumena, C., and Abderrahmane, L.(2016). A novel approach for scalable multi-hop data dissemination in vehicular ad hoc networks. Elsevier, Volume 37, Part 2,(228–239).

[3] Deyun, G., Chuan, H., Foh, B., and Oliver, W.(2015). Wireless Vehicular Sensor and Ad Hoc Networks. International Journal of Distributed Sensor Networks.

[4] RFC of AODV,DSR:

[5] www.ietf.org/rfc/rfc3561.txt,www.ietf.org/rfc/rfc4728.txt.

[6] Remo, C.(2013). Optimizing ad-hoc on-demand distance vector (aodv) routing protocol using geographic allocation data. Department of Computer ScienceCollege of Science and Mathematics.

[7] Kumar, J, Kulkarni, M. and Gupta, D.(2013). Effect of Black Hole Attack on MANET Routing Protocols. Comput. Netw. Inf. Secur., vol. 5, (64–72), April.

[8] IRSHAD, U., and SHOAIB U. Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols. School of Computing Blekinge Institute of Technology, Sweden.

[9] Reza, F., Shahram, J., Fateme, S., and Shahram, B.(2013). An Improvement over AODV Routing Protocol by Limiting Visited Hop Count. I.J. Information Technology and Computer Science.

[10] Anurag, S., Tomar, and Gaurav, K.(2014). Optimized positioning of multiple base stations for black hole attack. International journal of advanced research in computer engineering and technology, volume3,issue 8,August.

[11] Samah, A., Ahmed, I., and Nagy, E.(2015). Solution to Black Hole Attack in Ad Hoc on Demand Distance Vector Routing Protocol. Journal of Computer Sciences and ApplicationsVol. 3, No. 4 (90-93).

[12] Man, M., Sharma, and Maninder, S.(2014). Enhanced multiple approaches for preventation and elimination of black hole attack in mobile ad-hoc networks considering the enhancement of network throughputs. International journal of engineering science and research technology , ISSN:2277-9655,may.

[13] Raut, D., and Hande, K.(2014). Detection and Prevention of Gray Hole and Black Hole Attack in MANET. IJCA 2014.

[14] Vipan, C., Atul, G., and Vivek, D.(2013). Detection of Black Hole Attack in MANET under AODV Routing Protocol. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June ISSN: 2277 128X.

[15] Funde Nitesh A., Pardhi P. R., Detection & Prevention Techniques to Black & Gray Hole Attacks In MANET: A Survey. International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 10, October , ISSN (Print) : 2319-5940.

[16] Lalita, P., and Anurag, T.(2015). Detection of Black Hole Attack With Improved AODV Protocol in Manet. International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 5, May.

[17] Amreen, Sh.,and Neelesh, G.(2015). Review of Exposure of Black Hole Attack AODV based Routing Protocol in Mobile Ad Hoc Network. International Journal of Computer Applications (0975 – 8887) Volume 124 – No.4, August.

[18] Tarek, M., Abdelmgeid, A., and Omar, M.(2015). A Modified AODV Routing Protocol to Avoid Black Hole Attack in MANETs. International Journal of Computer Applications (0975 – 8887) Volume 109 – No. 6, January.

[19] Hnatyshin, V., and Asenov, H.(2010). Design and Implementation of an OPNET model for simulating GeoAODV MANET routing protocol. Proc. of the OPNETWORK 2010 International Conference, Session: Wireless Ad Hoc and Wireless Personal Area Networks, Washington DC, August.

[20] OPNET Tutorial http://www.ensc.sfu.ca/research/cnl School of Engineering Science Simon Fraser University

[21] "Securing the Sensor Networks Along With Secured Routing Protocols for Data Transfer in Wireless Sensor Networks", International Journal of Emerging Technologies and Innovative Research (www.jetir.org | UGC and issn Approved), ISSN:2349-5162, Vol.5, Issue 10, page no. pp316-321, October-2018, Available at : http://www.jetir.org/papers/JETIR1810599.pdf