International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Performance Evaluation of Black Hole Attack Using GA in Routing Protocols

[1]Er. Bhavna Jain, [2]Er.Yogesh Kumar
[1]MTech (CSE)
Shaheed Udham Singh College of Engg. & Technology, Tangori
[2]Asst. Prof
Shaheed Udham Singh College of Engg. & Technology, Tangori
[1] bhavna_jain84@yahoo.com,[2] yogesharora10744@gmail.com

Abstract: *Mobile ad hoc networks (MANETs) or wireless mesh networks (WMNs), experience serious security problems due to their particular characteristics as well as routing in a MANET is a particularly challenging task compared to a conventional. Wireless communication can endure interferences or malicious interceptions; whereas multi-hop communication assumes that each node will perform properly its functions to support network services. Further, self-organization increases the complexity of security management operations as access control, node authentication, secure routing and cryptographic key distribution. In MANET research has mainly focused on developing an efficient routing mechanism in such a highly dynamic and resource-constrained network. At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a trusted and cooperative environment. However, in the presence of malicious nodes, the networks are vulnerable to various kinds of attacks. In MANET, routing attacks are particularly serious. So, aims and objectives of this thesis work are to design and implement GA protocol with Black hole attack in OLSR protocol and prevent the system for threat using this hybridization. The whole simulation has been done in MATLAB 7.10.*

Keywords: *MANET, DSR, Genetic algorithm, routing, OLSR.*

1. INTRODUCTION

Computer networks differ on the basis of physical media used to transmit their signals, the communication protocols used to organize network traffic, the size of the network, topology used in the network. Ad-hoc network is a new standard of wireless communication for mobile hosts. Basically it's a network which is used in case of urgent situations [1]. All the nodes act as router in this network. The primary challenge in building a MANET is equipping each device to continuously maintain the information which is necessary to properly route the traffic [2]. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes. As MANETs are illustrated by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes. The network is de-centralized and all the network activities like discover the topology and delivering messages must be execute by the nodes. However, similar to other networks, MANET is also vulnerable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself [3]. In MANET, security is a challenging issue due to the vulnerabilities that are associated with it. When initiating a Route Discovery, the sending node saves a copy of the original packet in a local buffer called the Send Buffer. The proposed GA uses the elitism technique to retain the best chromosome in each generation. Further, the rest of the chromosomes are replaced by using crossover and mutation operations.

2. MANET

MANET stands for Mobile Ad-hoc Network [4]. It is a self-configuring infrastructure-less network. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. Therefore, we refer to a wireless ad-hoc network with mobile nodes as a Mobile Ad Hoc Network [5]. In MANET, all the devices are connected by wireless links. Every device in a MANET is free to move independently in all the directions. It can change its links to other devices frequently. Nodes are randomly connected with each other using arbitrary topology. They can act as both routers and hosts [6]. The primary challenge in building a MANET is equipping each device to continuously maintain the information which is

necessary to properly route the traffic. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes. As MANETs are illustrated by limited bandwidth and node mobility, there is demand to take into account the energy efficiency of the nodes.

1.1 Types of MANET

- Vehicular Ad Hoc Networks (VANETs) are used for the communication surrounded by the mobile vehicles. Thus the communication being carried on even if the vehicles are moving in the different directions within a particular area.

- Intelligent Vehicular ad hoc networks (InVANETs) are used in cases like collision of vehicles or any other type of mobility problems.

- Internet Based Mobile Ad hoc Networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal ad hoc routing algorithms don't apply directly.

1.2 Security Threats in MANET

Similar to other networks, MANET also vulnerable to many security attacks [7]. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself. In MANET, security is a challenging issue due to the vulnerabilities that are associated with it. Intrusion detection is therefore incorporated as a second line of defense in addition to key based authentication schemes [8]. The ranges of attacks that can be mounted on MANETs are also wider than in case of conventional static networks.

In mobile wireless networks there is no infrastructure as such and so it becomes even more difficult to efficiently detect malicious activities by the nodes inside and outside the network. As a matter of fact, the boundary of the network is not properly defined [9]. Nodes can intermittently come into the network or leave it. Moreover malicious nodes can flood the network with junk packets hampering the network service or intentionally drop packets [10]. But these nodes can but these nodes can subtly manipulate their harmful activities in such a manner that it becomes difficult to declare a node as malicious.

1.3 Black hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept [11]. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [12]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [13]. The method how malicious node fits in the data routes varies.

Below figure shows how black hole problem arises, here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other replies and will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost [3].

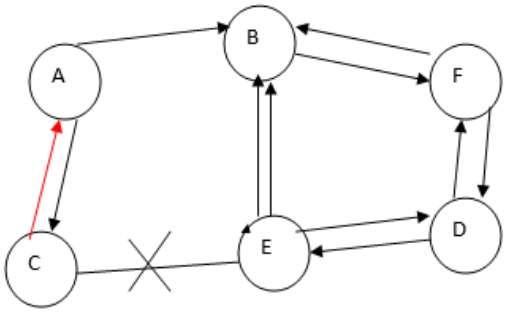

Figure 1: Black hole attack

The malicious nodes in this attack acts as Black hole that drop all the data packets passed by it [14]. If the attacking node acts as a connecting node of two components, the separation of network in two disconnected components wound taken place.

1.4 OLSR

The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad hoc networks, which can also be used on other wireless ad hoc networks. OLSR is a proactive link-state routing protocol, which uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths [17].

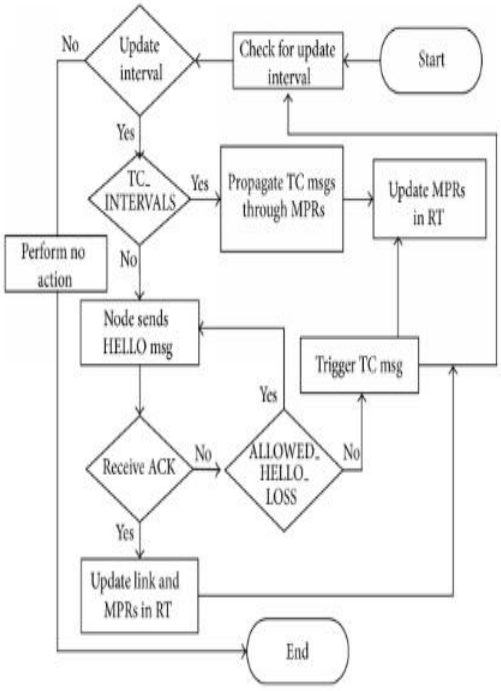

Figure 2: OLSR

In OLSR black hole attack, a malicious node forcefully selects itself as MPR. Malicious node keep its willingness field to Will always constantly in its HELLO message. So in this case, neighbors of malicious node will always select it as MPR. Hence the malicious node earns a privileged position in the network which it exploits to carry out the denial of service attack. The effect of this attack is much vulnerable when more than one malicious node is present near the sender and destination nodes [13].

1.5 Dynamic Source Routing

Dynamic Source Routing (DSR) is the very efficient protocol designed mainly for WSN, adhoc networks. Dynamic Source Routing (DSR allows network to be self- organizing as well as self- configured. The DSR contains two terms.

- Route Discovery [14]
- Route Maintenance

Route discovery and Route Maintenance operations are both unidirectional. It is made unidirectional so that performance can be made strong. DSR also allows various types of internetworking between various wireless networks [15]. Source routing helps to remove loops, packet forwarding etc. It is similar to AODV protocol in which demands are made on requirement. DSR also scales automatically, only when changes are needed. In DSR nodes forwards data packets from one node to another in order to enhance cooperation. AS sequence number is needed at destination, so rich topology is need like mesh, ring etc.

Dynamic Source Routing (DSR) protocol allows to search source node dynamically in whole network. Each data packet contains header that contains the information of destination as well as routing path. Thus there is no need to update regularly the routing table. DSR is mainly designed so that routing overhead can be minimized [16]. So that successful delivery of the data can take place. DSR also supports in heterogeneous networking and interconnection in internet.

3. PROPOSED MODEL

In our proposed work we have optimized the black hole attack using GA-OLSR Algorithm. In computer network security, GA is mainly used to find an optimal solution to a problem. The Genetic Algorithm starts by identifying a data set called population. Then these are individually encoded using bits, characters or integers and they form a chromosome. The next operation on them is an 'Evaluation Function' used to determine the genuine chromosome. During this process, two different operations namely, crossover and mutation are performed which is used to imitate the breeding and evolution. The selection of the chromosome is biased towards the fittest of the species. At last, the fit chromosome is selected once the optimization criterion is met. Hence in proposed model GA-OLSR has been shown and Routing with DSR in following way:

GA-OLSR Steps:

Step 1 : Initialize.
Step 2 : Enter length and width of the network.
Step 3 : Packet size.
Step 4 : Enter no. of nodes and buffer size.
Step 5 : Nodes Can Not Be More Than 300.
Step 6 : Plot x- coordinates
Step 7 : Plot y-coordinates
Step 8 : Unique ids of nodes
Step 9 : Covered set is the set of coverage of all nodes
Step 10 : Plot source node
Step 11 : Plot destination node
Step 12 : Data packets to be send
Step 13 : Calculating the uncovered neighbor sets
Step 14 : Destination_node_ids=source_node_covered;
Step 15 : Send=source_node_covered;
Step 16 : Load coverage set
Step 17 : Computing the difference between the source and the destination
Step 18 : Checking whether the destination is in different direction or not
Step 19 : Coverage set for the destination
Step 20 : Source coverage set -----source_node_covered

Step 21 : To check that if a data is getting transferred through any node , if its node speed would be more than average speed
Step 22 : Store network life time
Step 23 : Packet dropping
Step 24 : GA application
Step 25 : Call fitness function
Step 26 : Reduces features.
Step 27 : Evaluate parameters.

ROUTING-DSR Steps:
Step 1 : Node deployment.
Step 2 : Enter n height of network.
Step 3 : Enter width of network.
Step 4 : Searching of source nodes.
Step 5 : Plotting source nodes.
Step 6 : Find node positions.
Step 7 : Black hole node found.
Step 8 : Node found in cache memory.
Step 9 : Evaluate parameters.

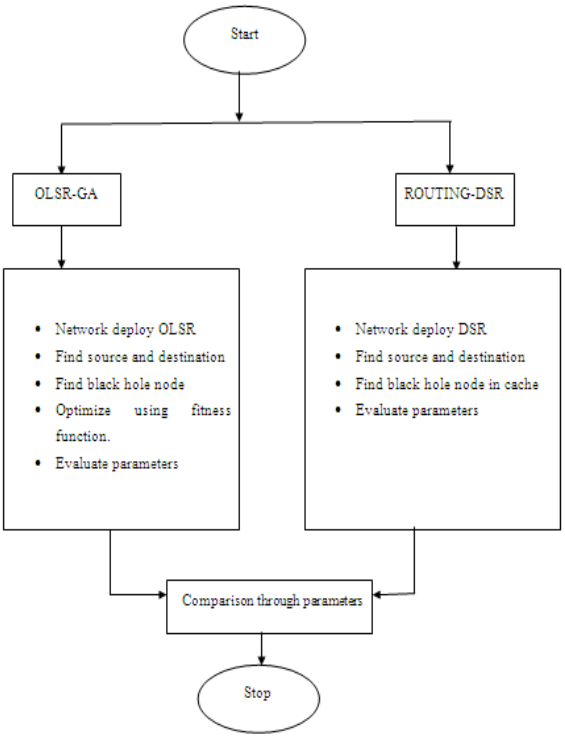

Figure 3: Proposed Flow of Work

4. RESULTS AND IMPLEMENTATIONS

4.1 Computation Parameters Formulas

1. **End Delay=** ∑ (arrive time – send time) / ∑ Number of connections.

2. **Throughput=** ∑ (Total data transferred) / ∑ Total amount of data.

3. **Error rate=** Exact Value-Approximate Value|)/Exact Value] x 100.

4. **Routing Overhead=** ∑ Number of packet delayed / ∑ Number of packet send.

5. **Packet delivery ratio=** ∑ Number of packet receive / ∑ Number of packet send.

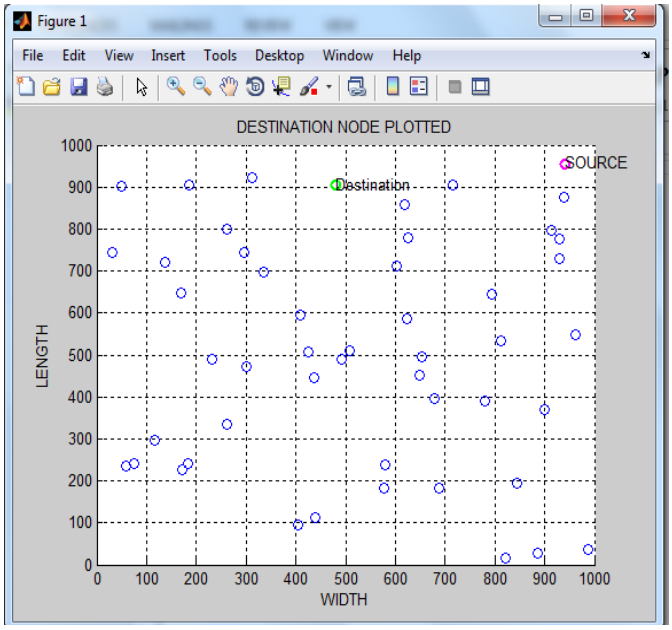

Figure 4: Network Deployment

The above figure shows the OLSR deployment of the nodes in the network. The area considered in 1000*1000 meters. The deployment of the nodes deals with the x locations and y location of the nodes.

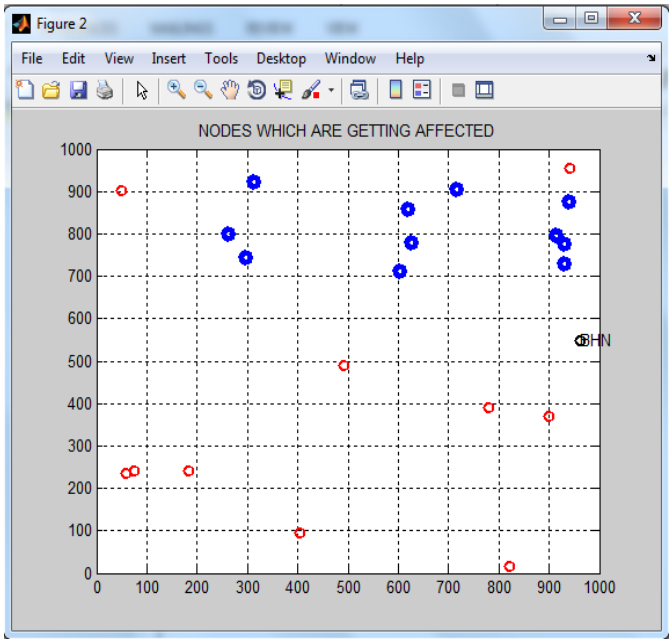

Figure 5: Affected Nodes

The above figure shows the black hole nodes at the end of the round because the nodes are the mobile nodes and their positions are changes according to the execution of rounds and the green red color nodes are affected nodes plotted in the network.

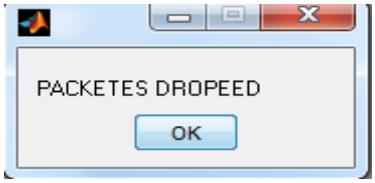

Figure 6: Packet Drop

When data packets are sent from source to destination packet dropping takes place and it has been confirmed by seeing the routing table.

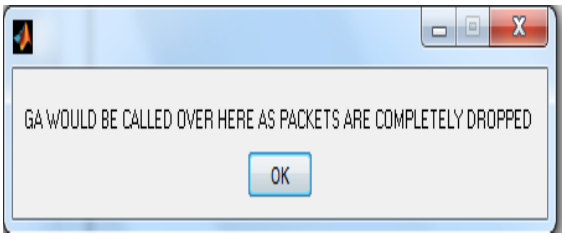

Figure 7: Calling of GA

When packet dropping occurs, GA calling has been done to optimize the fitness function.

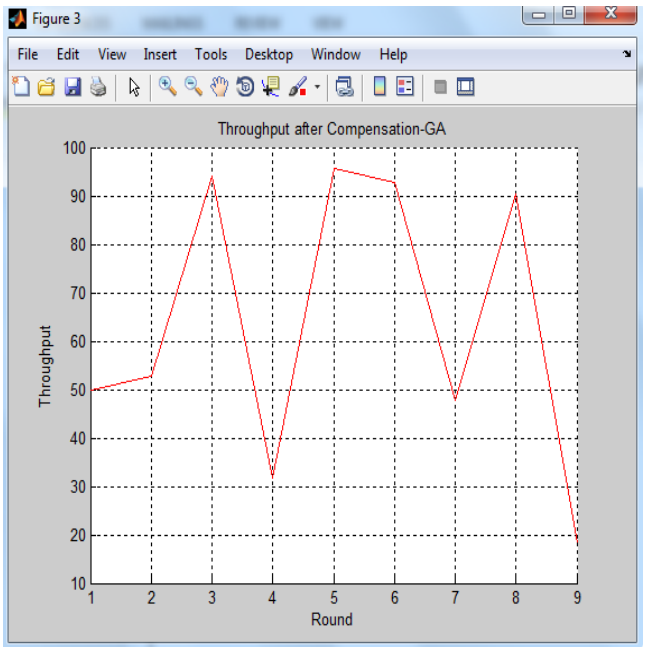

Figure 8: Throughput after Compensation

The above figure shows the throughput of the network using optimization approach using genetic algorithm which shows the overall performance of the network. This measure should be high for the efficient network.

The graph shows the throughput 93.5% which is a sufficient measure to increase network lifetime.

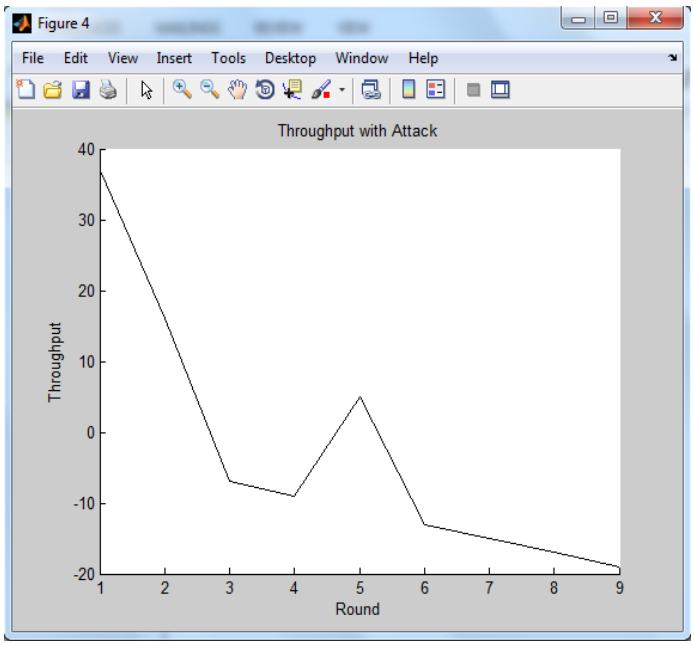

Figure 9: Throughput with Attack

The above figure shows the throughput performance graph in the presence of the black hole nodes which is very less i.e. 35 % and should be low for the overall performance of the network.

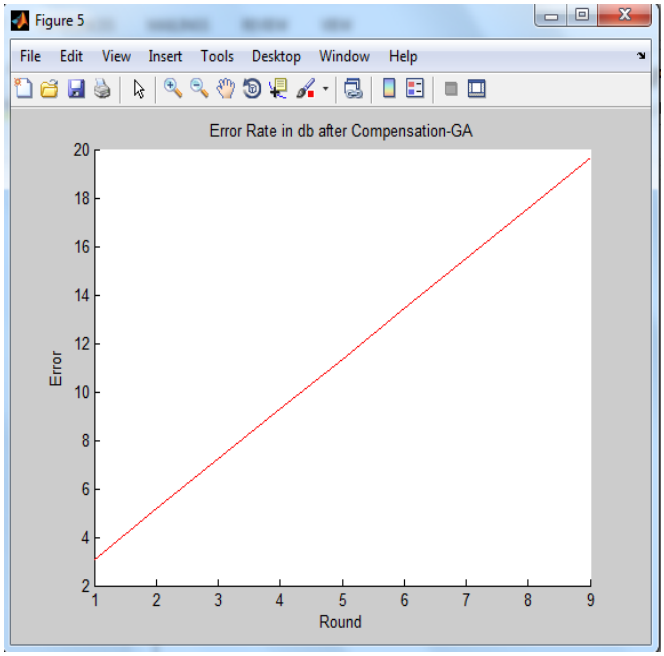

Figure 10: Error Rate with Compensation

Above figure shows the BER using GA. The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a unit less

performance measure, often expressed as a percentage. It has been found that error rate is very low i.e. 20.

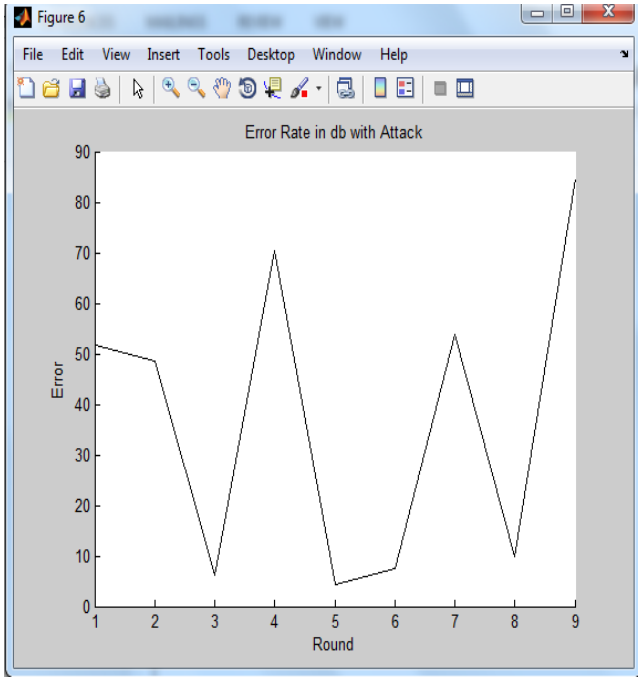

Figure 11: Error Rate with Attack

Above figure shows the BER in attack. The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage. It has been found that error rate is very high i.e. 90.

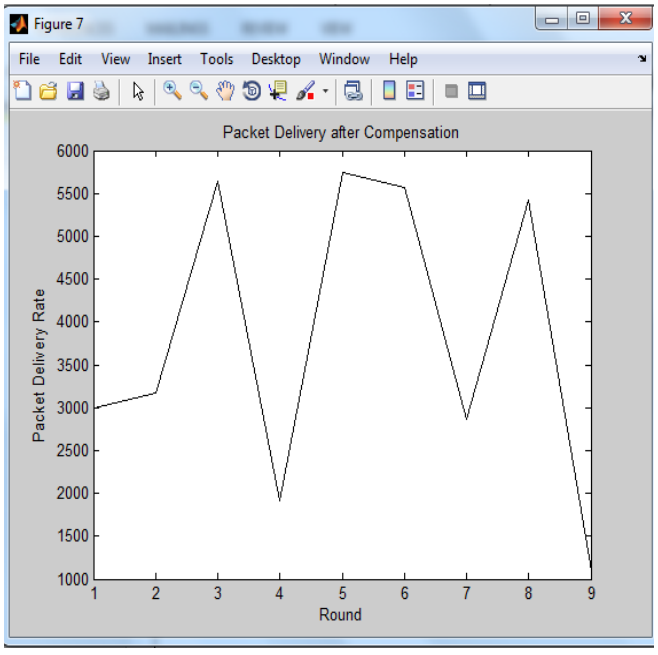

Figure 12: Packet delivery after compensation

It is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent. Above figure shows the delivery ratio with GA. Packet delivery ratio has found to be very high e.g. 6000 packets in given time.

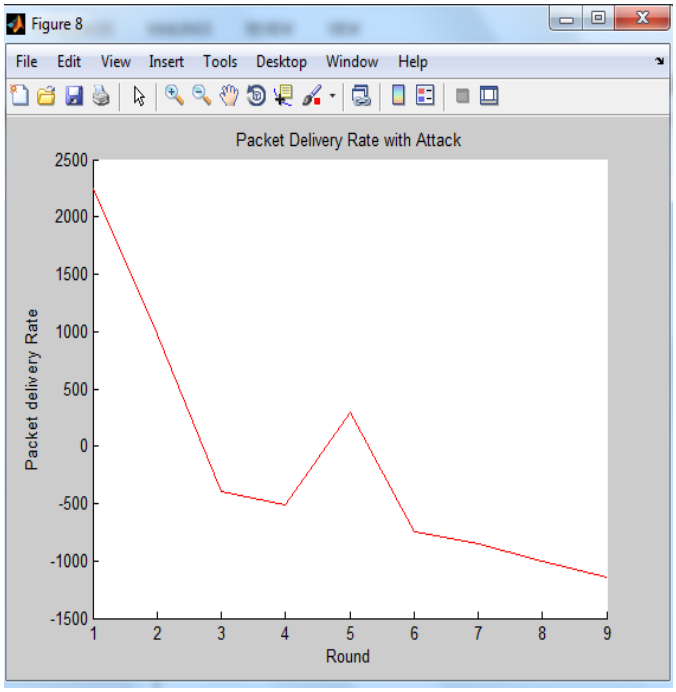

Figure 13: Packet Delivery rate with Attack

It is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent. Above figure shows the delivery ratio with attack. During attack no. of packets are reduced so packet delivery ratio has found to be 2200 in given time.

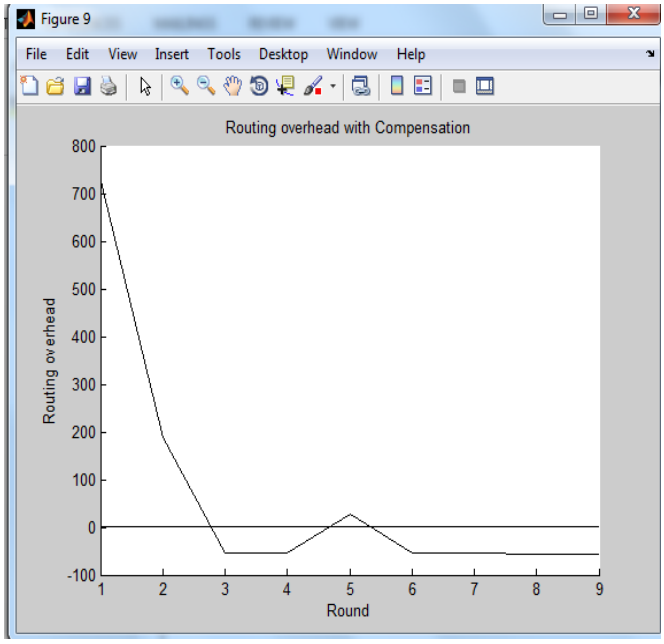

Figure 14: Routing Overhead with Compensation

Routing overhead is the total number of control packets or routing packets generated by routing protocol during simulation. The variation in network load gives

considerable reduction. Above figure shows the routing overhead with GA.

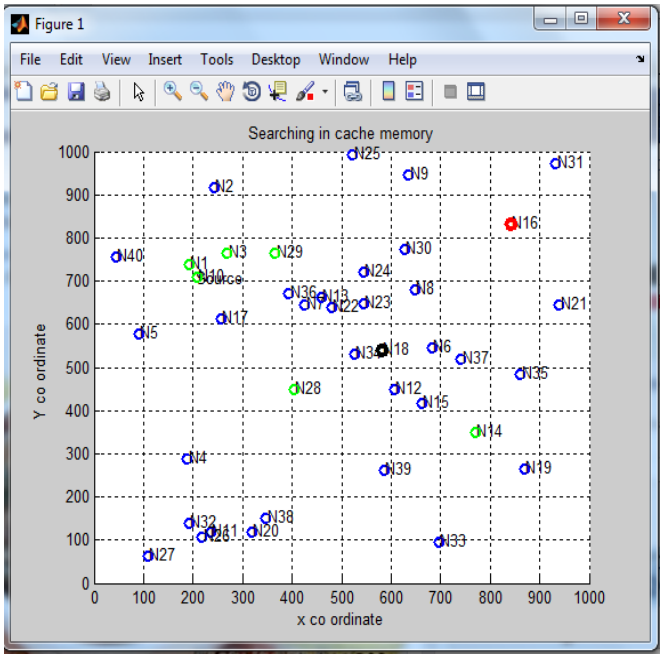

Figure 15: Black hole searching in Cache Memory

Above figure shows the simulation of the 1000* 1000 network. Above figure shows the source and destination nodes. Then searching of black hole node takes place in the cache memory.

Figure 16: Finding of Path from round 1 to round 5

Above figure shows the finding of the path to detect the black hole nodes.

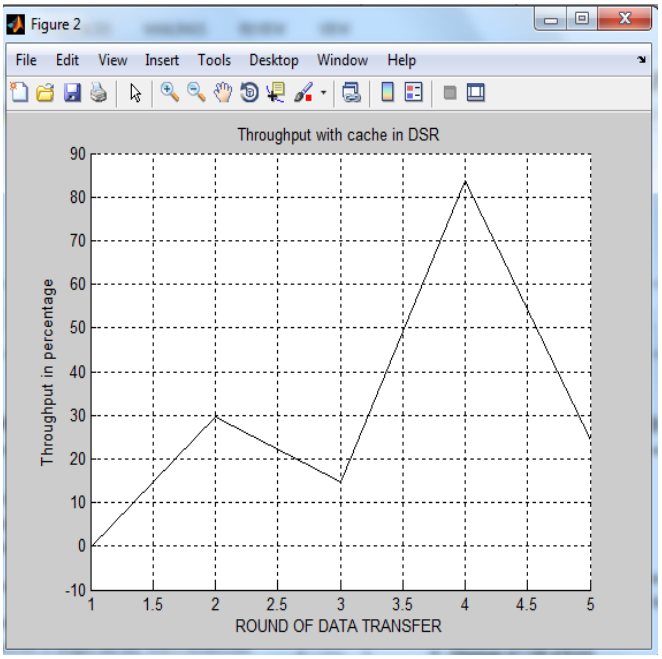

Figure 17: Throughput with cache in DSR

The above figure shows the throughput of the network using cache in DSR which shows the overall performance of the network. This measure should be high for the efficient network. The graph shows the throughput 83.5% which is a sufficient measure to increase network lifetime.

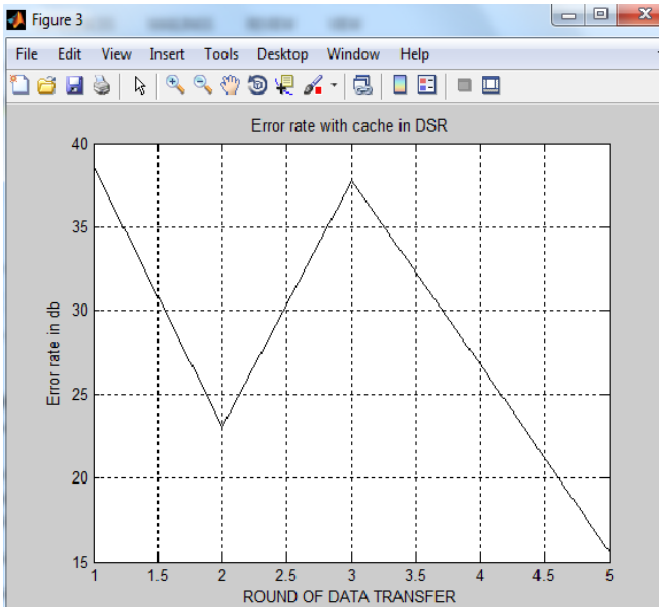

Figure 18: Error rate with Cache in DSR

Above figure shows the BER using cache in DSR. The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. BER is a unit less performance measure, often expressed as a percentage. It has been found that error rate is very low i.e. 40.

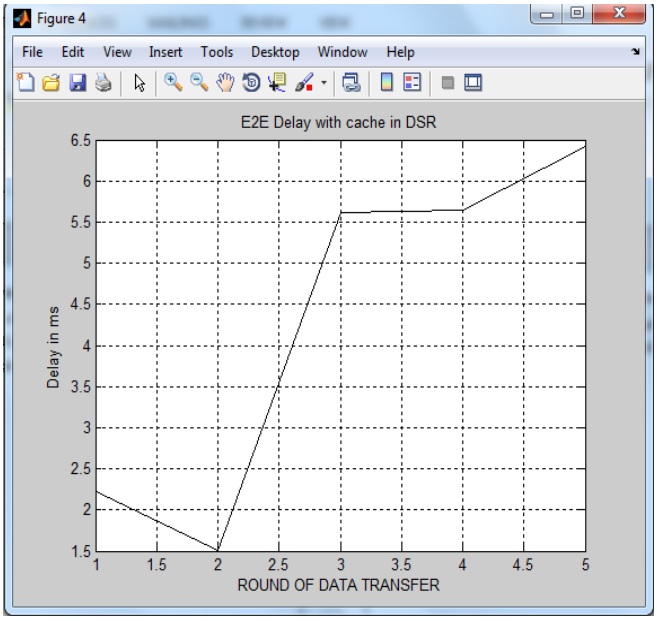

Figure 19: End Delay with cache in DSR

It refers to the time taken for a packet to be transmitted across a network from source to destination. Above graph shows the high delay value in DSY i.e. 6.5 ms in comparison to OLSR protocol.

4.2 *Comparison between DSR and OLSR*

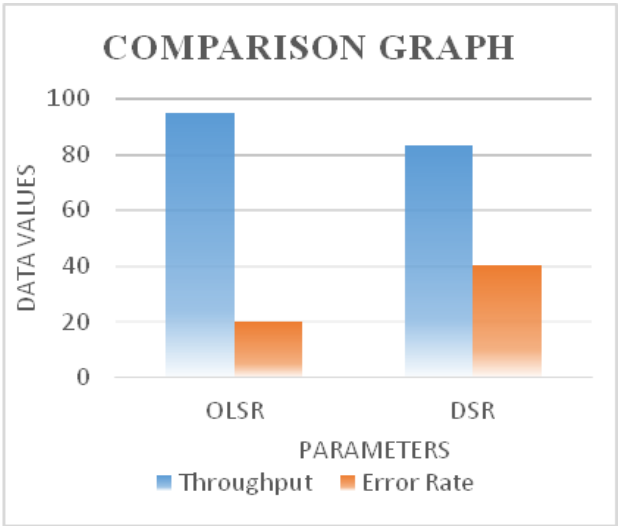

Figure 20: Comparison Graph

Above graph shows comparison between DSR and OLSR in terms of Throughput and error rate. From results OLSR founds to be better.

CONCLUSION & FUTURE WORK

Mobile Ad hoc Network (MANET) is a collection of mobile nodes by wireless links forming a dynamic topology without any network infrastructure such as routers, servers, access points/cables or centralized administration. Each mobile node functions as router as well as node. We present a simulation-based performance study of widely used reactive protocol, OLSR-GA. The research work deals with the black hole attack and its effect on network performance and optimization using genetic approach which will help to increase the lifespan of the designed network. The packets transmitted this way are made to drop so as no unauthorized access is available to transmitted data.

The future work will be based on the realization of the Sybil attack and black hole attack. Comparative study can optimize the network with other algorithms like particle swarm optimization, bacterial foraging optimization. We can also use the hybridization on different optimization algorithms like BFO and PSO hybrid, PSO and genetic hybrid, PSO and firefly algorithm. Also we can use the encryption algorithms for the data security in the network like Advanced Encryption scheme, blow fish algorithms.

REFERENCES

[1] Al Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." Proceedings of the 42nd annual Southeast regional conference. ACM, 2004.

[2] Anup Goyal and Chetan Kumar, "GA-NIDS: A Genetic Algorithm based Intrusion Detection System", 2010.

[3] Ahmed Sherif, Maha Elsabrouty. Amin Shoukry, "A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)", IEEE, pp: 346-352, 2013.

[4] BinTian ; China Inf. Technol. Security Evaluation Center, Beijing, China ; Yizhan Yao ; LeiShi ; ShuaiShao in " A Novel Sybil Attack Detection Scheme In Wsn".

[5] Crosbie, Mark, and Gene Spafford. 1995, "Applying Genetic Programming to Intrusion Detection" , InProceedings of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8. Cambridge, Massachusetts, 1995.

[6] C. Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in Proc. Securecomm Workshops, 2006, pp.1–11.

[7] Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, "Performance analysis of ad-hoc networks under black hole attacks".Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 –153.

[8] D. B. Jagannadha Rao(et.al), "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks" , International Journal of Advanced Research in Computer and Communication Engineering,Vol. 1, Issue 8, PP.522-529,October 2012

[9] Dave, Dhaval, and Pranav Dave, "An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET", Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[10] Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, "Performance analysis of ad-hoc networks under black hole attacks".Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 –153.

[11] Hadlee, N.A.; Dept. of Comput. Sci. & Eng., Anna Univ., Chennai, India ; Kayalvizhi, S. in"Increasing Sybil attack detection probability in open acess distributed system".

[12] Harley Kozhushko, "Intrusion Detection: Host Based and Network-Based Intrusion Detection Systems", Independent Study, 2003.

[13] Istikmal ; Sch. of Eng., Telkom Univ., Bandung, Indonesia ; Leanna, V.Y. ; Rahmat, B.in "comparison of proactive and reactive protocol in manet"

[14] James Newsome, Elaine Shi, Dawn Song and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses" IPSN"04, April 26-27,2004, Berkeley, California, USA.

[15] K.S. Sujatha, V. Dharmar. R.S. Bhuvaneswaran, "Design of genetic algorithm based IDS for MANET", Conference: Recent Trends In Information Technology (ICRTIT), IEEE, pp.28-33, 2012.

[16] Kaur, Harjeet, Manju Bala, and Varsha Sahni,"Study of Blackhole Attack Using Different Routing Protocols in MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering2.7 (2013): 3031-3039.