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

Detection and Mitigation of Gray hole attack over OLSR protocol in MANET using GA and Fuzzy

Gurjinder Kaur[1], Navpreet Kaur[2]
[1]BBSBEC, FGS, Punjab, India
Scholar (M.Tech)
[2]BBSBEC, FGS, Punjab, India
Assistant Professor (ECE)
[1]gurjinderchd@gmail.com, [2] navpreet.kaur@bbsbec.ac.in

Abstract: *As we know that MANET is formed by a number of mobile nodes and each node communicate with each other using bandwidth. In MANET batteries carries by each node have limited power, which in turn limiting the applications given by the MANET. Such limitations need the traffic to be evenly distributed among the mobile hosts. Otherwise, the nodes with heavy load can cause congestion, large delay and consume more energy, thus, increasing the cost of the network. In MANET, job completion becomes difficult, when massive load is given to the nodes with less processing capabilities and which do not have any resources to distribute the load. The possibility of imbalance of load is due to that the computing or processing power of the systems is non-uniform. There are situations where some nodes may be idle and some will be overloaded. A node which has high processing power finishes its own work quickly and is estimated to have less or no load at all most of the time. So, in the presence of under-loaded nodes keeps idle, the need for over-loaded nodes is objectionable. There are lots of routing approaches developed for load balancing in mobile ad hoc networks. In the proposed work, optimized Link State routing protocol (OLSR) will be used. It is a proactive link state routing protocol which uses Hello and topology control messages to discover and then deliver information throughout the MANET. The performance of OLSR will be improved by using Genetic algorithm in combination with Fuzzy logic. GA is an optimization technique that will used to improve the performance on the basis of natural selection and biological evolution. After applying these two approaches the code is simulated in MATLAB environment and thus, performance parameters of the MANET like Throughput, delay, energy consumption and Bit error rate will be determined.*

Keywords: *MANET, Optimized Link State routing protocol (OLSR), Genetic algorithm (GA), Fuzzy Logic*

I. INTRODUCTION

MANET is the main area of research because of some challenges and issues that still exist in the network [1]. MANET is the type of wireless network in which each node communicates with other node via wireless medium. MANET can be broadly classified into three types:

i. Vehicular Ad hoc Networks (VANETs)

It can be 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 [7].

ii. Intelligent Vehicular Ad hoc Networks (InVANETs)

These are used in cases like collision of vehicles or any other type of mobility problems.

iii. Internet Based Mobile Ad hoc Networks (iMANET)

Ad hoc networks that link mobile nodes and fixed Internet-gateway nodes are iMANETs. Normal Ad hoc routing algorithms don't apply directly in these types of networks [8].

Within MANET, a user can find several types of routing protocols every one of them is employed based on the network [2].

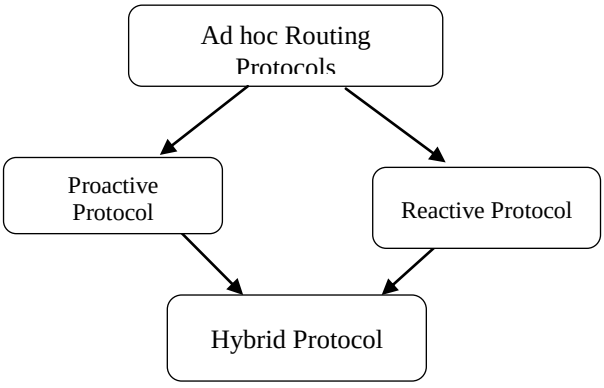

Figure 1: Classification of routing protocols

Proactive protocols are certainly not made for huge networks while they must preserve node records for each and every node from the routing table of each and every node. These protocols preserve diverse quantity of routing furnishings various by protocol in order to protocol [3]. There are numerous well-known pro-active routing protocols. Illustration: DSDV, OLSR, WRP etc. Reactive routing protocol is also known as on demand routing protocol. On this protocol route is identified every time it can be desired Nodes start route breakthrough upon requirement foundation. Supply node recognize its route cache for that accessible route by supply in order to purpose spot in the event the route is not accessible subsequently that initiates route penetrate process. Hybrid routing protocols is the hybridization of proactive as well as reactive protocols like ZRP (Zone routing protocols), SHARP (Sharp hybrid adaptive routing protocol) [4].

An Ad hoc Network is a connected component of different tiny wireless nodes charged with small batteries. The batteries can't be recharged once the nodes are deployed into the network. In such a case, it becomes quite important to use the battery very efficiently. The battery is consumed in order to perform the following set of operations [5]

i. Routing
ii. Trafficking
iii. Load Balancing
iv. Intrusion Management

Routing refers to setting up the path for the transfer of the data from the source to destination. There are more than 20 routing algorithms; still the Ad hoc Network suffers the coverage, presence of intruders and cost management problems in routing. The first problem of this research work is apply a trust model which would prevent the system from any kind of extra cost in search of suitable node for the transfer of the data. For such purpose, no algorithm other than optimization based algorithm can be thought of. Here the purpose would be solved using Genetic algorithm with OLSR routing protocol. OLSR is an IP routing protocol optimized for mobile Ad hoc networks [6].

Another face of Ad hoc Network is that the network has always struggled in managing the intrusion. With the passage of time, attackers have become smarter and in the similar fusion, smart attack, namely, Gray Hole has come into light. The attacks have been termed "SMART" due to their unpredictable behavior in the network. It has been seen often that the network does not even come to know that it is under the influence of any attack if smart attacks are considered. There is one more issue which should be focused and that would be prevention of innocent nodes, getting harmed due to suspicion. An intelligent sense of think is required in such situation which can take dynamic decision. Fuzzy logic can be a very well suited solution for this problem and hence the problem statement of this research work includes the introduction of Fuzzy logic. The evaluation of the solution would be based on QOS (Quality of Service) Parameters. The expected parameters would be [7]:

- **Throughput**

Throughput is defined as the total number of packets transmitted n the whole simulation time. Mathematically, it is defined as:

$$\text{Throughput} = \frac{\sum Packtssent}{Totaldatapackets}$$

- **Bit Error rate**

Bit Error rate (BER) is defined as the number of bits per unit time. It is the division of bit errors by the total number of transferred bits during time interval. It is often defined in the form of percentage and it is a measure of unit less performance.

- **Energy Consumption**

Energy consumption is the defined as the total amount of energy being consumed by each node in MANET at different network layers. It is obtained by energy consumed summation in every operation mode during simulation time. It is defined mathematically as below:

$$Energy\ Consumption = \sum_{i=0}^{n-1} (Energy\_consumed\_by\_node(i))$$

- **End to end delay**

End-to-end delay refers to the time taken for a packet data to be transmitted across a network from source node to destination node. So, in network, we use those routes in which the probability of end to end delay is less, so performance of the propose work is better. In the mathematical term, we can say that the end to end delay is the total amount of time which is elapsed during the transmission of packet data.

$$Dend - end = Dtrans + Dprop + Dproc$$
$$Where\ Dend - end = End - To - End\ Delay$$
$$Dtrans = Transmission\ Delay$$
$$Dprop = Propagation\ Delay$$
$$Dproc = Processing\ Delay$$

II. RELATED WORK

A lot of work been done in the field of MANET for the detection and mitigation of gray hole attack. Few of them are listed below:

Alex Hinds et al. [2013] focused on the range of available MANET routing protocols and discussed several features ranging from early protocols (e.g. DSDV) to higher level (e.g. MAODV). Arun Biradar [2013], focused on Mobile Ad Hoc Networks (MANETs) that consists of mobile platforms that are freely mobile. These are self-organizing and adaptive

networks. These networks allow the spontaneous formation and deformation of mobile networks. The shortest path problem in MANETS requires that the path from the source node to the destination node be calculated, thereby, minimizing the sum of the total costs associated with the path.

Azzedine Boukerchea et al. [2011] focused on Ad hoc wireless network to accomplish the difficult task of multi-hop communication in the absence of special infrastructure, the mobile node and change the topology network environment. It shows different limits for deployment as calorie restriction option, knowledge of the physical location of nodes, in some cases, such as real-time or multicast traffic, as well as requirements.

Bow-Nan Cheng et al. [2012] proposed a comparative analysis of various routing protocols in MANET. Various routing protocols has been analysed like AODV, OLSR and OSPF-MDR. Their performance has been evaluated in terms of routing overhead traffic, end-to-end message completion rate, and end-to-end delay, to examine performance vs. Trade-off.

Chetana Khetmal et al. [2013] have implemented black hole attack based on AODV, termed as BAODV Routing Protocol. NS2 Simulator is used for simulating MANET [using BAODV, SAODV, MANET, and CBR with FTP by taking 50 nodes.

Gurpinder Singh [2012] investigated the behaviour of DSR, AODV, TORA protocols, using metric throughput and network loading. Behaviour analysis was performed using the simulation tool opnet as the primary simulator. HarjeetKaur et al. [2013] focused on Ad hoc network (MANETs) that consists of different types of mobile nodes. The research focuses on reactive, active and hybrid routing protocols such as AODV, OLSR and ZRP.

K. Chadhaand et al. [2014], has presented the preventive measure for black hole attack in MANET. The black hole attack possess a serious security threat to the routing services by attacking the reactive routing protocols resulting in drastic drop of data packets.

Mohamed Dyabi et a.l [2014] explained the concept of Mobile Adhoc Network (MANET) with respect to clustering. The author has proposed a new algorithm in OLSR network. Varied numbers of simulations are performed for several nodes and variable nodes velocity. The simulation is calculated with and without the clustering interval. The work has given improvement with the performance and number of elected cluster heads.

Bow-Nan Cheng et at. [2012] proposed a comparative analysis of various routing protocols in MANET. Various routing protocols has been analysed like AODV, OLSR and OSPF-MDR. Their performance has been evaluated in terms of routing overhead traffic, end-to-end message completion rate, and end-to-end delay, to examine performance vs. Trade-off.

III. SIMULATION MODEL

In this research work, a novel algorithm has been developed for the route discovery by utilizing Trust model on the basis of OLSR routing protocol with Genetic Algorithm and fuzzy logic.

The methodology can be well explained using the following flow diagram.

Step 1: Initialize the network with various no. of nodes.
Step 2: Enter width and length of network to implement network.
Step 3: Calculation of X and Y location of nodes
Step 4: Deployment of sensor nodes in network
Step 5: Plotting of source and destination
Step 6: Find coverage set, and then find distance between nodes.
Step 7: Apply genetic algorithm within the network to optimize the route. If fitness function of the GA is true then apply Fuzzy rule.

Step 8: Define rule sets for Fuzzy logic to find out the routs.
Step 9: Optimize the rule sets using Genetic algorithm optimizer to find attackers based on the analysis of QoS parameters.
Step 10: If attackers are founded then call the Genetic algorithm to discover the route which provides the best optimal results.
Step 11: Calculate the QoS performance metrics like Throughput, Delay Rate, Bit Error Rate and Energy Consumption.

IV. SIMULATION RESULTS

The whole simulation is being performed in MATLAB simulation environment. The performance parameters that are calculated are shown below:

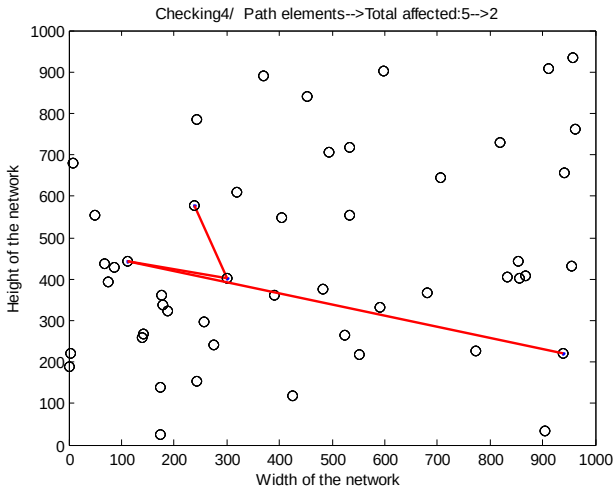

Figure 2: Network environment for MANET

The network area of the proposed work in wireless sensor network consists of area 1000× 1000 having 50 numbers of nodes to run the network. The network is run for five times that means five iterations have been applied so that best results can be obtained.

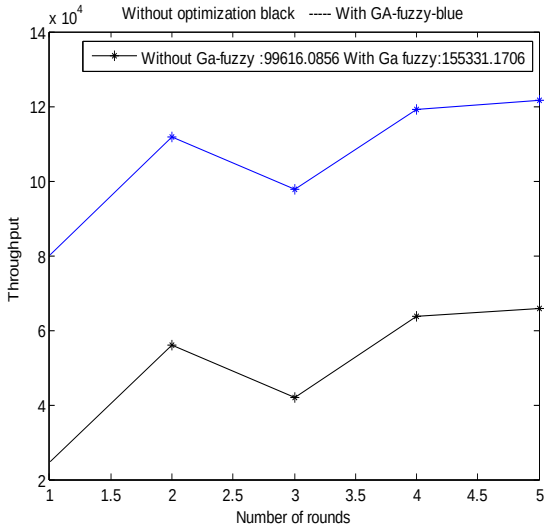

Figure 3: Throughput with and without optimization

Throughput means the number of packets that are transmitting by the source node to the destination nodes or we can say that it is the total number of packets delivered to the destination node within a total simulation time. As it is shown in figure above, the black color line indicates the throughput values obtained from the MANET without optimization i.e. no algorithm or protocol is used to reach the packet at the destination node. Whereas the blue line indicates the throughput values obtained for the MANET with optimization i.e. GA and fuzzy logic is used to find the accurate path and the packet has to reach at their appropriate position. The process is repeated five times in order to obtained accurate results. The values of throughput obtained for the network are listed in table below:

Table 1: Performance values for throughput with and without optimization

Number of rounds	***Throughput (104)***	
	With Optimization	***Without Optimization***
1	8	2
2	11	5
3	9	4
4	12	6
5	12	7

Thus, the average throughput values obtained for the network without optimization is 10.4 *104 whereas the throughput values obtained for network with GA and Fuzzy is 4.8*104.Therefore, it is clear that the average value obtained for network with optimization is better as compared to without optimization. Because when optimization is not applied in the network then the data from the source may follow the wrong rout which is known as malicious attack or in this research we have consider gray hole attack .Whereas, in optimization network no malicious attack occurs data will follow the accurate path to reach at the destination, thus, their throughput value get increased.

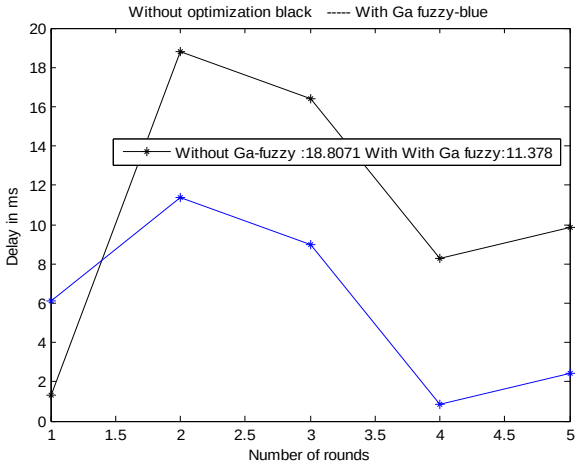

Figure 4: Delay with and without optimization in MANET

Delay is the average time a network takes to transmit data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination.

In the above figure, black line shows the delay occurred in case of without optimization and blue line is indicating delay with optimization. Therefore, it is clear from the graph that the delay value obtained for network with optimization when GA and Fuzzy logic techniques are applied is less than the value obtained for without optimization which means that in without optimization data packets takes more time to reach at the destination than with optimization. The delay values obtained for with and without optimization are listed in table below:

The average value obtained for delay without optimization is 10.4 m sec whereas with optimization delay of the MANET reduced and become equal to 4.8 m sec.

Table 2: Performance values for Delay with and without optimization

Number of rounds	***Delay***	
	With Optimization	***Without Optimization***
1	6	1
2	11	18
3	8	16
4	1	8
5	2.3	10

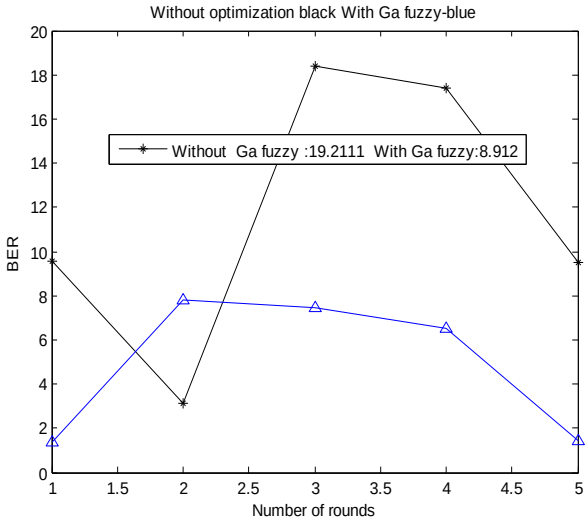

Figure 5: BER with and without optimization

Transmitted bits are correctly received at the sink node if and only if those data bits are received at each intermediate node between source and destination without error as shown in figure above. The total numbers of bit errors occurred in sending data bits from any source node to any destination node calculates the BER of the network. This means that the network must be connected in such a way that we can calculate BER of the network to know its performance. From the above figure, it is clear that the blue line is for the BER when GA and Fuzzy is applied to the network whereas black line indicates the performance when GA and Fuzzy is not applied. Thus, it is concluded that when GA and Fuzzy are applied to the network, Bit error rate is less as compared to the BER obtained for the network without GA and Fuzzy. Therefore, the results obtained for the network using optimization are better than without optimization.

Table 3: BER with and without Optimization

Number of rounds	***BER***	
	With Optimization	***Without Optimization***
1	1	9
2	8	3
3	8	18
4	7	17
5	1	9

The average value obtained for BER without optimization is 10.4 m sec whereas with optimization BER of the MANET reduced and become equal to 4.8 m sec.

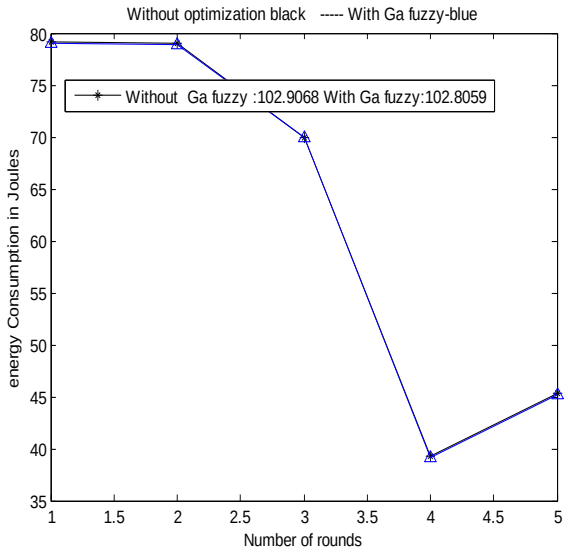

Figure 6: Energy consumption

When data is transmitted from one node to the other node within the MANET, all the nodes will consume some energy. Thus it is necessary to find the optimal route that will consume less energy and the data has been transmitted to appropriate destination. For finding route OLSR routing protocol is used and for optimizing route GA is used. It is concluded that more energy is consumed without GA and Fuzzy algorithm than with GA and fuzzy algorithm being applied to the network. Without optimization, the maximum value of energy consumption is 102.9068 whereas; with optimization the energy consumption reduced and become 102.8059 which is less as compared to without optimization.

V. CONCLUSION AND FUTURE SCOPE

Ad hoc network consists of individual devices for the communication purpose with each other. The concept of Ad hoc network is not that familiar to end users who have a typical router for sending the wireless signals. For deploying the network in Ad hoc network, configuration of network is considered. OLSR is prone to countless attacks similar to alteration in the sequence quantities or hop counts, source route channeling, spoofing in addition to construction in the error messages. Gray hole attack is an actual threat in contradiction of OLSR protocol in Mobile ad hoc network. Gray hole attack knows how to be certainly launched even in network grids that is available confidentiality in addition to authenticity. The malicious nodes generally target the routing controller messages interrelated to routing data.

In this research, we have analyzed the effect of Gray Hole in the network. For this purpose, we have used an OLSR routing protocol. For optimization, fuzzy set and GA are used as a classifier. It works on the basis of rule sets which can help to find whether the attack is present or not. Through fuzzy logic technique, the rules are

being set as per OLSR routing protocol. The simulation has been executed using the MATLAB. The simulation results has shown that when the gray hole node exists in the network, the performance of the network is being affected and decreased and can be optimized by using Genetic algorithm with fuzzy rule sets. In the proposed work, throughput value (4.8*104), delay (4.8 msec), BER (4.8) and energy consumption (102.8059) are obtained when optimization is being used.

In future work, we can use neural network as classifier along with ABC for detection and prevention from various attackers. When the route is classified using neural network, the attack can be accurately detected so that more appropriate performance can be achieved.

REFERENCES

[1] Alex Hinds, Michael Ngulube, Shaoying Zhu, "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[2] ArunBiradar, "Effectiveness of Genetic Algorithm In Reactive Protocols For MANET",International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2, Issue 7, July 2013.

[3] AzzedineBoukerchea, BegumhanTurgut, "Routing protocols in ad hoc networks: A survey", 2011 Elsevier doi:10.1016/j.comnet.2011.05.010

[4] Bow-Nan Cheng; Moore, S., "A comparison of MANET routing protocols on airborne tactical networks", in Military Communications Conference – (MILCOM'12), vol., no., pp.1-6, Oct. 29, 2012, Nov. 1, 2012.

[5] Chetana Khetmal1, Prof.Shailendra Kelkar2, Mr.NileshBhosale, "MANET: Black Hole Node Detection in AODV", International Journal of Computational Engineering Research, Vol. 03, 2013

[6] Gurpinder Singh, "MANET: Issues and Behaviour Analysis of Routing Protocols",International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 4, April 2012.

[7] HarjeetKaur, VarshaSahni, Dr.ManjuBala, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", in International Journal of Computer Science and Information Technologies, (IJCSIT), Vol. 4 (3), pp. 498-500, 2013.

[8] K. Chadha and S. Jain, "Impact of black hole and grey hole attack in AODV protocol", in International Conference on *Recent Advances and Innovations in Engineering (ICRAIE)*, pp. 1-7, Jaipur, 2014.

[9] Dyabi, Mohamed, Abdelmajid Hajami, and Hakim Allali, "A new MANETs clustering algorithm based on nodes performances," 2014 International Conference on Next Generation Networks and Services (NGNS), IEEE, 2014.

[10] Bow-Nan Cheng; Moore, S., "A comparison of MANET routing protocols on airborne tactical networks," in Military Communications Conference – (MILCOM'12), pp.1-6, Oct. 29, 2012, Nov. 1, 2012.

[11] Tan et al, "Secure Route Discovery for preventing black hole attacks on AODV-based MANETs", ICT Convergence (ICTC), International Conference on. IEEE, 2013.

[12] Dave et al, "An effective Black hole attack detection mechanism using Permutation Based Acknowledgement in MANET," Advances in Computing, Communications and Informatics, IEEE, 2014.

[13] J. Nakasuwan and P. Rakluea, "Performance comparison of AODV and OLSR for MANET," *ICCAS 2010*, Gyeonggi-do, 2010, pp. 1974-1977.

[14] M. Wang, L. Lamont, P. Mason and M. Gorlatova, "An effective intrusion detection approach for OLSR MANET protocol," *1st IEEE ICNP Workshop on Secure Network Protocols, 2005. (NPSec).*, 2005, pp. 55-60.

[15] A. Loutfi and M. ElKoutbi, "Enhancing performance OLSR in MANET," *2012 International Conference on Multimedia Computing and Systems*, Tangier, 2012, pp. 505-509.