International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Research Article

Prevention of Black Hole Attack in MANET using Addition of Genetic Algorithm to Bacterial Foraging Optimization

Kanika Bawa[†*] and Shashi B. Rana[†]

[†]ECE Department, GNDU RC Gurdaspur, Punjab, India

Accepted 05 July 2015, Available online 11 July 2015, **Vol.5, No.4 (Aug 2015)**

Abstract

At present, several efficient routing protocols have been proposed for MANET. Most of these protocols assume a reliable and cooperative environment. However, when malicious nodes are present, the networks are penetrable to various kinds of attacks. In MANET, routing attacks are peculiarly serious. So, this proposed work tries to design and implement Mobile Ad-hoc Networks using GA and BFO algorithm with Black hole attack and prevent the system from threat using these optimization algorithms.

Keywords: *Mobile ad hoc network, Genetic Algorithm, Bacterial Foraging Optimization, Dynamic Source Routing protocol.*

1. Introduction

The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to take up ad hoc networks for commercial uses due to their unique properties (Sheenu Sharma *et al*, 2009). However, similar to other networks, MANET is also penetrable to many security attacks. MANET not only inherits all the security threats faced in both wired and wireless networks, but it also brings in security attacks unique to itself. In MANET, security is a challenging and difficult issue due to the vulnerabilities that are associated with it (Akansha Saini *et al*, 2010).

Intrusion detection is therefore incorporated as a second line of defense in addition to key based authentication schemes. The ranges of attacks that can be mounted on MANETs are also wider than in case of conventional static networks. In case of 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 (Rajib Das *et al*, 2009). As a matter of fact, the boundary of the network is not properly defined. Nodes can come into the network or leave it at irregular intervals. Moreover malicious nodes can flood the network with junk packets at overwhelming number, hampering the network service or intentionally drop packets. But these nodes can elusively manipulate their harmful activities in such a manner that it becomes difficult to declare a node as malicious (P. Michiardi *et al*, 2002).

This paper elaborates the ongoing research on intrusion detection systems for detecting network layer attacks in mobile Ad-hoc networks. Precisely, GA and BFO protocolhas been adopted and specifically monitors the vulnerabilities in the network layer. Based on the GA and BFO IDS technique, a solution is proposed for the detection of vulnerabilities in MANET.

2. Related Work

Anup Goyal and Chetan Kumar (2010), has suggested a systematic learning method known as Genetic Algorithm (GA), to identify illegitimate nodes. The algorithm considers the varied features in network connectivity like protocol type, network service to destination and connection status to generate a type based rules. This was experimented by implementing in GA and trained it on the KDD Cup 99 data set to generate rules that can be applied to the IDS to categorize based on the attack types (Anup Goyal *et al*, 2010).

Ahmed Shariff (2013), showed Mobile Ad-Hoc Networks (MANETs) are characterized by the lack of infrastructure, dynamic topology, and their use of the open wireless medium. Black-hole attack represents a major threat for such type of networks. The purpose of this paper is two folds. First, to present an extensive survey of the known black-hole detection and prevention approaches. Another objective is to present new dimensions for their classification (Ahmed Shariff *et al*, 2013).

K.S. Sujatha (2012), proposed a technique to analyze the exposure to attacks in AODV, specifically the most common network layer hazard, Black Hole

*Corresponding author: **Kanika Bawa**

attack and to develop a specification based Intrusion Detection System (IDS) using Genetic Algorithm approach. The proposed system is based on Genetic Algorithm, which analyzes the behaviors of every node and provides details about the attack. Genetic Algorithm Control (GAC) is a set of various rules based on the vital features of AODV such as Request Forwarding Rate, Reply Receive Rate and so on. The performance of MANET is analyzed based on GAC (K.S. Sujatha *et al*, 2012).

Dokurer (2007), investigated the effects of Black Hole attacks on the network performance. We simulated black hole attacks in Network Simulator 2 (ns-2) and measured the packet loss in the network (Dokurer *et al*, 2007).

3. Simulation Model

A packet drop attack is also known as black hole attack in the network layer (Wei Li *et al*, 2010). In black hole attack node drops packets at each step, then high loss of data packets takes place in the network. The node that drops the packet is malicious node. This malicious node attack can be viewed as following:

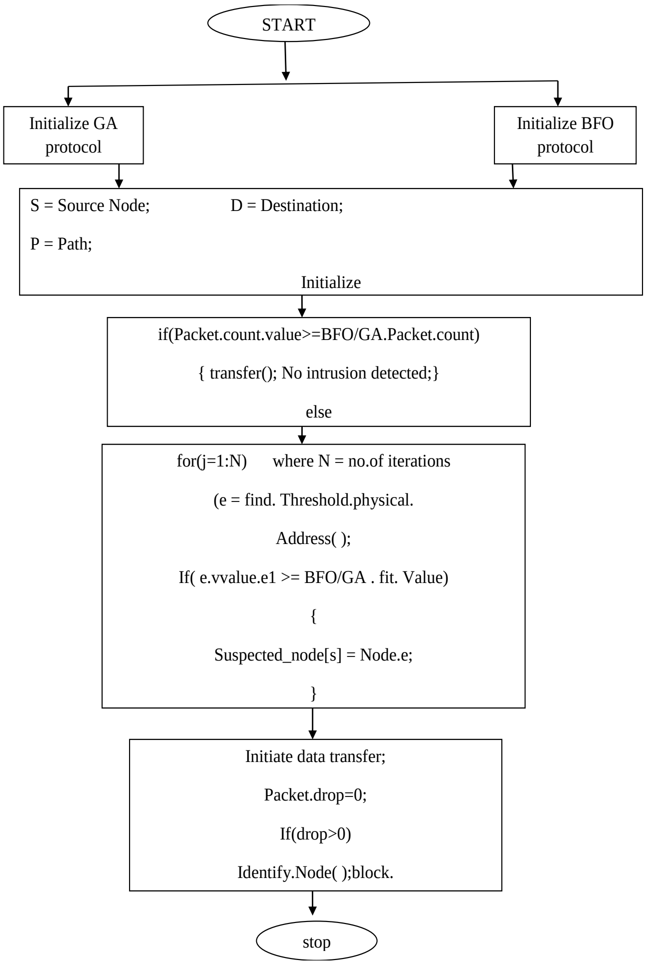
START
Initialize GA protocol
Initialize BFO protocol
S = Source Node; D = Destination;
P = Path;
Initialize
if(Packet.count.value>=BFO/GA.Packet.count)
{ transfer(); No intrusion detected;}
else
for(j=1:N) where N = no.of iterations
(e = find. Threshold.physical.
Address( );
If(e.vvalue.e1 >= BFO/GA . fit. Value)
{
Suspected_node[s] = Node.e;
}
Initiate data transfer;
Packet.drop=0;
If(drop>0)
Identify.Node( );block.
stop

Fig. 1 shows that node A wants to send data to node D. If node C is the shortest distance path from A to D, then it has to be followed. It will then receive the RREQ message from node A. As soon as node A starts to send the packet the node C drops packet in the middle of the data sending process (Ganapathy S *et al*, 2012).

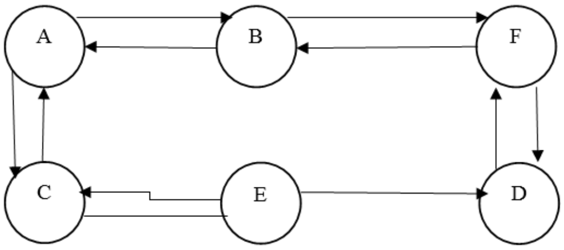

Fig. 1 Black Hole Attack/ Packet Drop Attack

4. Genetic Algorithm and BFO approach based Intrusion Detection System

```
For Each Node
Blackhole=0;
ReceiveReply (Packet P){
    if (BALCKHOLE~=1 AND P has an entry in Route Table){
        selectDest_Seq_No from routing table
        if (P.Dest_Seq_No>Dest_Seq_No){
            If (Rrep Not Sent)
                Then Blackhole=1;
            ELSE
                update entry of P in routing table
                unicast data packets to the route specified in RREP
                BLACKHOLE=0;
        }
        else {
            discard RREP
        }
    }
    else {
        if(P.Dest_Seq_No>= Src_Seq_No){
            Make entry of P in routing table
        }
        else {
            discard this RREP
}}}
```

5. Simulated Results

A. Parameters used

a) Energy: Efficient energy use, sometimes simply called energy efficiency, is the goal to decrease the amount of energy required to provide products and services. It is measured in Kj.

b) Throughput: Throughput is the rate of production or the rate at which something can be processed.

c) Bit Error Rate: 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 unitless performance measure, often expressed as a percentage.

d) Packet Delivery Ratio: The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender

e) End To End Delay: End to End Delay is the summation of Transmitting Delay (at MAC layer), Propagation Delay and queuing Time of a packet.

B. Experiments

Firstly, MANET environment is implemented over MATLAB-2010 to compute parameters like throughput, BER, packet delivery rate and routing overhead.

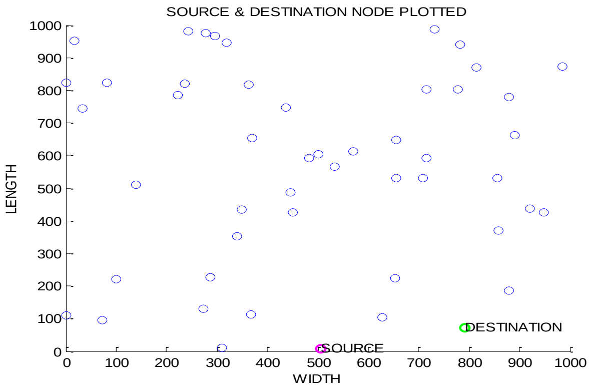

Fig. 2 MANET Network

The above figure shows the Mobile Ad-hoc networks with their length and breadth of 1000*1000. In this nodes are deployed by calculating their x and y locations and also the source and destination nodes are plotted. The source node is in magenta color and destination is in green color.

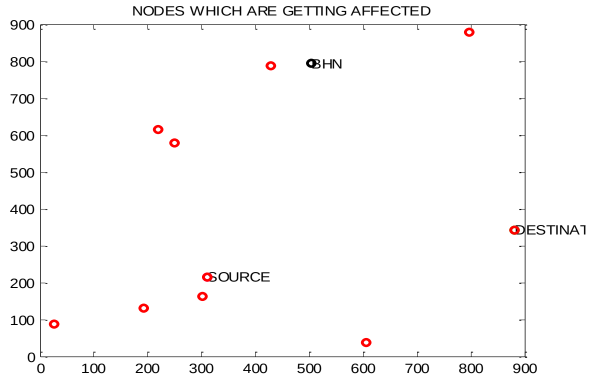

Fig.3 Nodes which are getting affected

Then Black hole node appears in MANET environment and affect the other nodes. The above figure shows the nodes which are getting affected due to black hole node and are shown in the red color.

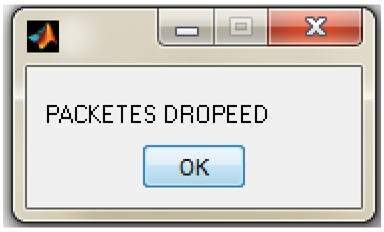
PACKETES DROPEED

Fig. 4 Packets Dropped

Due to Black hole Attack, packets starts dropping. The above figure shows the message box which shows the indication that the packets are completely dropped after black hole attack so there will be need of optimization. For optimization, firstly Genetic Algorithm is used.

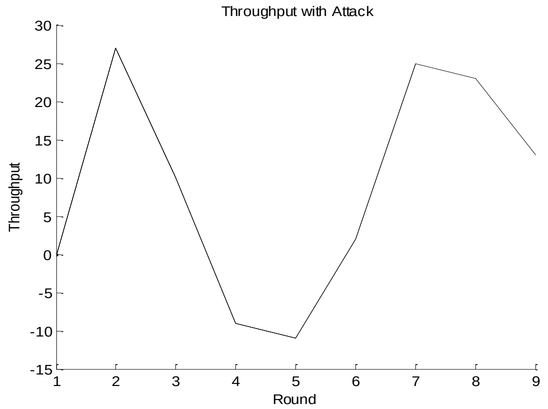

Fig. 5 Throughput with attack

The above figure shows the throughput which is very less. This measure should be high as much as possible to increase the network life time. The above figure shows the effect of attack on throughput if the network.

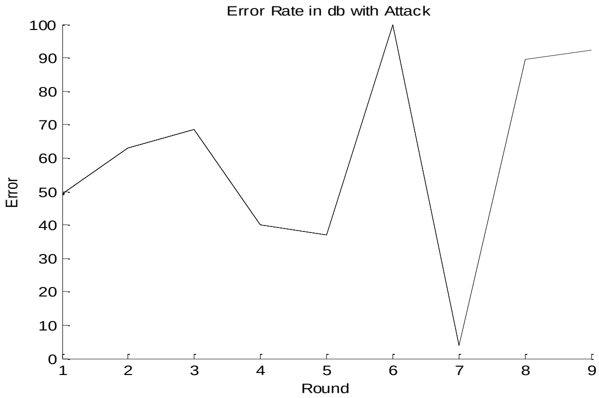

Fig. 6 Error Rate with attack

The above figure shows the error rate in db in the presence of the attack and this measure should be as low as much as possible for the proper functioning of the network in mobile ad-hoc networks. The nodes are mobile and there is a huge chance for the increase of error rate in the network.

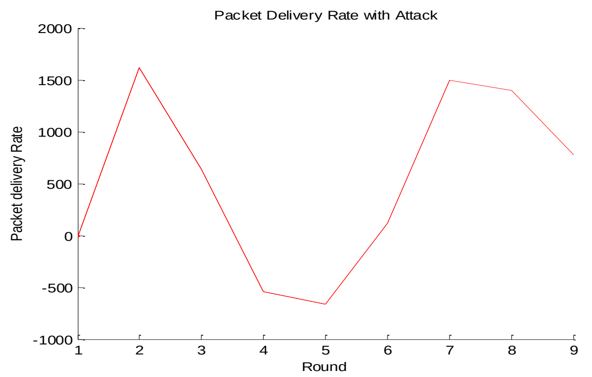

Fig.7 Packet Delivery Rate with attack

The above figure shows the packet delivery rate which should be high and the graphs shows the effect of the black hole attack in mobile Ad hoc networks with respect to the number of rounds.

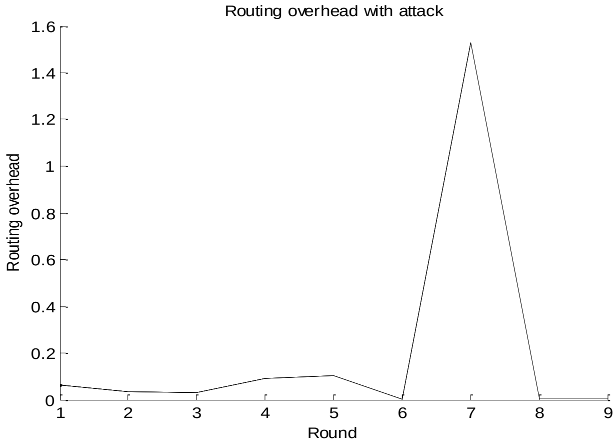

Fig.8 Routing Overhead with attack

The above figures show the routing overhead in the presence of attack which is getting high. This measure should be less to increase the network lifetime and shows the overhead requests to a particular node at a time.

C. Optimization

Due to black hole attack all the parameters are affected. There are two types of algorithm used for optimization: Genetic Algorithm and Bacterial Foraging Algorithm.

Results using Genetic algorithm are:

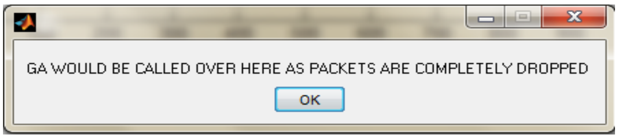
GA WOULD BE CALLED OVER HERE AS PACKETS ARE COMPLETELY DROPPED

Fig.9 Calling GA after packet dropping

The above figure shows that the message box that the genetic algorithm is required which consists of the fitness function to provide best possible solution from number of solutions for the efficient output.

(a) Throughput

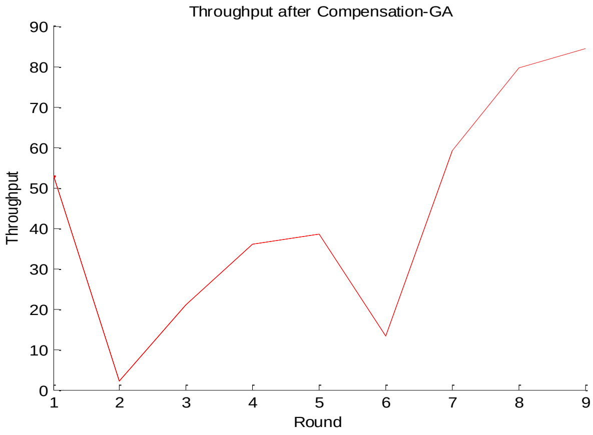

Fig. 10 Throughput after compensation-GA

The above figure shows throughput after compensation with Genetic algorithm. Due to black hole attack, throughput was decreasing. But Genetic algorithm has improved throughput of network.

(b) Bit Error Rate

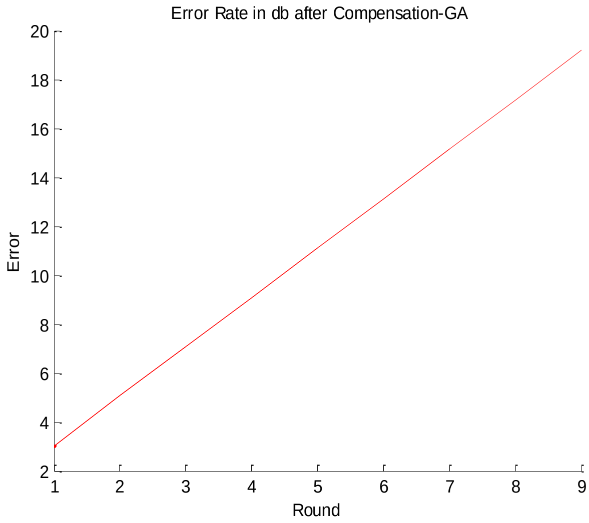

Fig. 11 Error Rate after compensation-GA

The above figure shows the error rate in db after applying optimization of the network i.e. genetic algorithm and shows that the network is having less error rate than in the presence of the attack to increase the life span of the network.

(c) Packet Delivery Rate

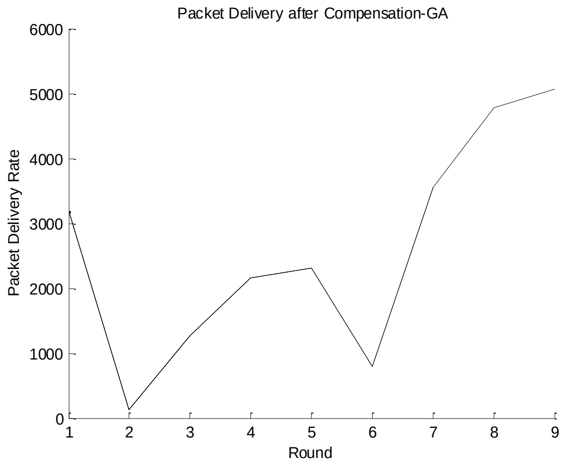

Fig. 12 Packet Delivery Rate after compensation-GA

The above figure shows the packet delivery rate which is an important measure to reach the packets successfully from source to the destination and shows that the after applying Genetic the more packets are delivered from source to the destination.

(d) Routing Overhead

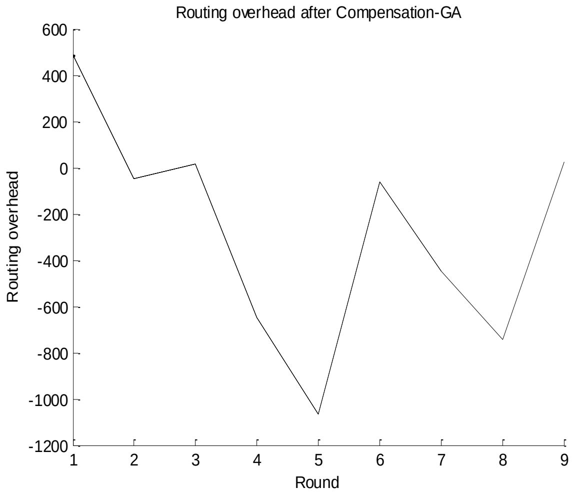

Fig. 13 Routing Overhead after compensation-GA

The above figure shows the routing overhead after compensation with Genetic Algorithm and shows that the overhead at the nodes decreases. If the routing overhead decreases then there will be the less chance of node failures

Results using Bacterial Foraging Optimization are:

a) Throughput

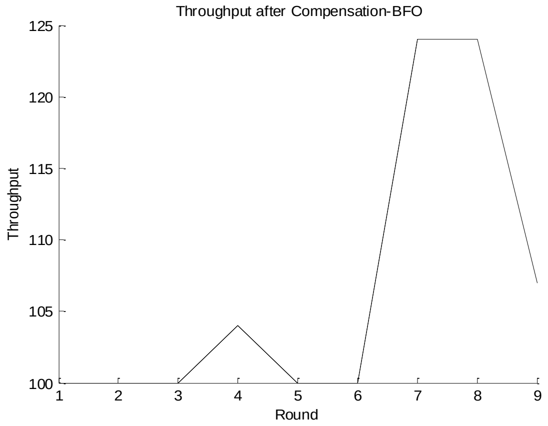

Fig. 14 Throughput after compensation-BFO

The above figure shows throughput after compensation with BFO. Due to black hole attack, throughput was decreasing. But Genetic algorithm has improved throughput of network. But BFO has worked better as throughput is more in case of BFO as compared to GA.

b) Bit Error Rate

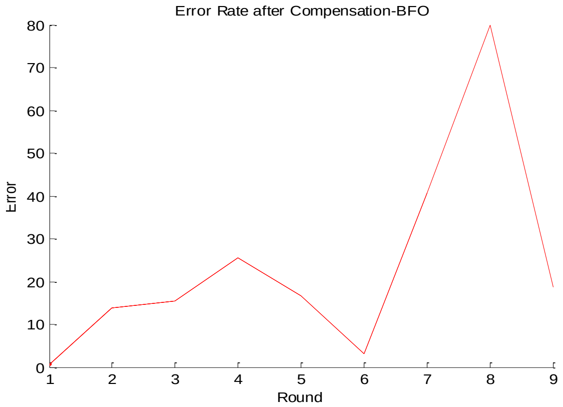

Fig. 15 Error Rate after compensation-BFO

The above figure shows the error rate using Bacteria foraging optimization which shows that the error rate is very less as compared to the network in the presence of the black hole attack in MANET and this measure should be low to achieve high throughput in the networks. But in case of GA, Bit Error rate is symmetrical as shown in fig 5.14.

c) Packet Delivery Rate

The below figure shows the packet delivery rate using bacteria foraging optimization and shows that the more number of packets are delivered after compensation of bacteria foraging optimization and this measure should be high as much as possible to increase the lifetime of the network. In case of packet delivery rate, BFO is better than GA which is found by comparing fig 12 and fig. 16

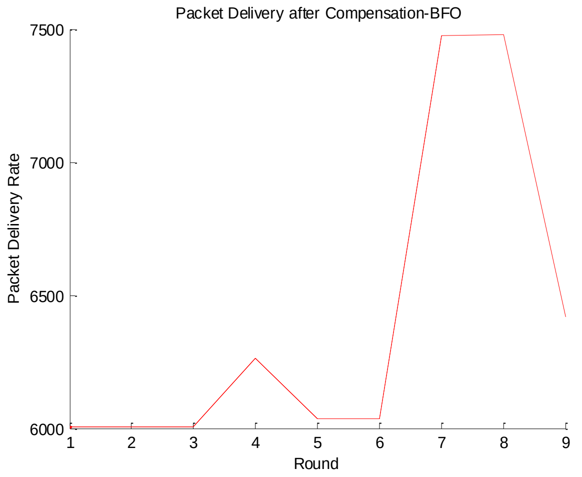

Fig. 16 Packet Delivery rate after compensation-BFO

d) Routing Overhead

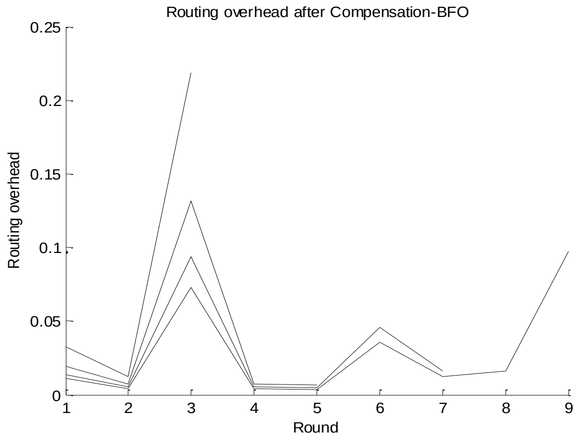

Fig. 17 Routing Overhead after compensation-BFO

The above figure shows the routing overhead after compensation with Bacteria Foraging optimization and shows that the overhead at the nodes decreases. It the routing overhead decreases then there will be the less chance of node failures

Conclusion and Future Scope

In this proposal, we have analyzed the effect of black hole attack in the performance of GA and BFO protocol. The simulation has been done using the MATLAB. The results of simulation show that when the black hole node exists in the network, it can be affect and decrease the performance of network and it can be optimized by using BFO and Genetic optimization algorithm. For the simulation purpose, a hypothetical network was constructed and then monitored for a number of parameters. We simulate our model for various distinct nodes. Initial position for the node is specified in a movement scenario file created for the simulation using a MATLAB. The nodes move in random manner among the simulation area. So, it is a challenging task to detect and prevent the black hole attack in the network.

For future work, we intends to simulate and analyze the effect of the black hole attack in other routing protocols and we intend to perform the solution for the black hole attack and compare its performance with the AODV protocol.

References

Sheenu Sharma and Roopam Gupta (2009), Simulation Study of Black hole Attack in Mobile Adhoc Networks, *Engineering Science and Technology*, pp. 243-250.

Akansha Saini and Harish Kumar (2010), Effect of Blackhole attack on AODV Routing Protocol in MANET, *International Journal of Computer Technology*, pp 245-250.

Rajib Das, Bipul Syam Purkayastha and Pradipto Das (2009), Security Measures for Black holeAttack in MANET, *An Approach International Journal of Engineering Science and Technology*, pp 76-81.

P. Michiardi, R. Molva (2002), Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks, *European Wireless Conference*, pp 15-17.

Anup Goyal and Chetan Kumar (2010), GA-NIDS: A Genetic Algorithm based Intrusion Detection System, *Communications surveys & tutorials*, pp 13-18.

Ahmed Sherif, Maha Elsabrouty. Amin Shoukry (2013), A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET), *IEEE Systems Journal*, pp. 346-352.

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

Dokurer, S., Erten Y.M., Acar. C.E. (2007), SoutheastCon Journal, Performance analysis of ad-hoc networks under black hole attacks, *Proceedings IEEE Volume*, pp 148 –153.

Wei Li (2010), Using Genetic Algorithm for Network Intrusion Detection, *IEEE Institute of Electrical and Electronics Engineers conference*, pp 1-8.

Ganapathy S, Yogesh P and Kannan A (2012), Intelligent agent based intrusion detection system using enhanced multiclass SVM, *Hindawi Publishing Corporation, Computational Intelligence and Neuroscience*, pp 23-29.

Revathi B, Geetha D (2012), A Survey of Cooperative Black and Gray hole Attack in MANET, *International Journal of Computer Science and Management Research*, pp 51-53,

Vijayan R, Mareeswari V and Ramakrishna K, (2011), Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic, *International Journal of Research and review in computer science*, pp 83-86.