IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

Hybridization of GSA and AFSA to Detect Black Hole Attack in Wireless Sensor Network

Soni Rani[1], **Charanjit Singh**[2]

Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India[1]

Professor, Electronics and Communication Engineering, Punjabi University, Patiala, Punjab, India[2]

Abstract: In today's world, wireless sensor network is very important in our daily life due to its variety of applications like in military and battlefield areas, business purposes, in education, or all other applications. Everything or every person is connected to wireless sensor network. Several nodes are connected through the wireless links. Wireless sensor network is vulnerable to various types of attacks. But black hole attack is very common and every hacker or attacker choose this attack because it stops the flow from source to destination. GSA and AFSA is natural phenomenon so we choose this to detect the black hole attack from the network. In this paper, we hybrid the GSA and AFSA to detect and prevent the black hole attack from the network. The main challenging problem is to design the fitness function and other parameters related to GSA and AFSA.

Keywords: Wireless Sensor Network, Black Hole Attack, GSA, AFSA.

I. INTRODUCTION

Wireless Sensor Network is the type of Ad Hoc network (infrastructure less) in which various independent sensor nodes communicates with each other or to the base station through multi hop wireless links. As there are many applications of wireless sensor network such as in battlefield (unmanned ground, airborne and underwater vehicles) and wearable computing etc. Ad hoc network is resilience that is used in military and emergency applications. While communicating, there must be confidentiality of data that must be sending from source to intended destination. But there are two major issues of Ad hoc network such as routing and security. Routing issue includes some factor like routing acquisition delay, quick refining and loop free. Security issue includes DOS (denial of service), jamming and energy depletion. Various types of attacks i.e. data traffic attacks and routing attacks that challenges the security. Routing attacks occurs on the network layer of the OSI model.

Black hole attack is the type of attack that occurs on the network layer and in which the malicious node falsely ensures the source node that it has the optimized fresh and shortest path to send all packets to the required destination node or base station. According to this information, source node sends its data in form of packets to the destination through that path whenever requires. Malicious node get chance to drop all the packets and attack on network occurs known as black hole attack.

In wireless sensor network, black hole refers to places in network where incoming or outgoing traffic is silently discarded (or dropped) without informing the source that the data did not reach its intended receipt. While examining the topology of the network, the black holes themselves are invisible and can only be detected by monitoring the lost traffic, hence the name.

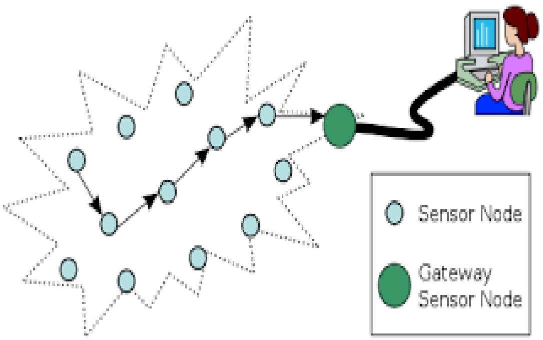

Figure1. Wireless Sensor Network

Black hole attacks can be categorized into two parts as single black hole attack or cooperative black hole attack. In single black hole attacks only one node behaves as malicious in the network. And in cooperative black hole attack, one node cooperates to another act as malicious nodes [1]

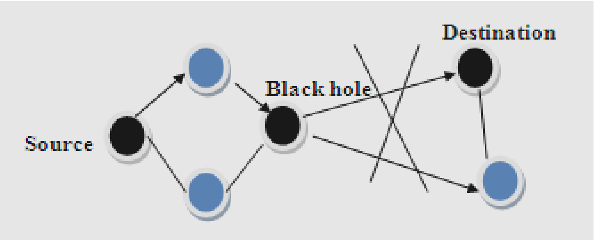

Figure2. Black hole attack

Black hole attack is very useful in some warfare areas such as hackers and intruder use traffic jam as their weapons so we have to prevent it for our security purposes. So we take step to detect and prevent it. In this paper we use hybridization of GSA and AFSA algorithm

DOI 10.17148/IJARCCE.2016.5833

to detect and prevent black hole attack in wireless sensor network. GSA is nature inspired optimization algorithm which has been increasing much fascinate among the technical world. It is based on two famous laws of Newton i.e. law of gravity and the law of motion. GSA is characterized under populace based strategy and is accounted for to be more intuitive. GSA is a memory-less algorithm. However, it works competently like the algorithms with memory [2]. AFSA is a algorithm in light of swarm conduct that was propelled from social practices of fish swarm in nature AFSA works in view of populace, arbitrary hunt and behaviorism. This algorithm has been utilized as a part of enhancement applications. This technique is one of the best methodologies of swarm intelligence method with extensive points of interest like high convergence pace, adaptability, error resistance and high precision [3]. In this paper we use this algorithm for prevention of black hole attack in wireless sensor network. Section II gives related work. Section III proposed methodology. Section IV simulation results. Section V gives conclusion.

II. RELATED WORK

N. Chaudharyet. al [4] propose a solution for detecting and avoiding black hole attacks both single and cooperative and ensuring secure packet transmission along with efficient resource utilization of mobile hosts at the same time. According to author proposal, evaluation of trust of every node in the network is based on parameters such as stability of a node defined by its mobility and pause time, remaining battery power etc. This trust of a node forms the basis of selection of the most reliable route for transmission. The simulation results show that author solution provides good performance in terms of throughput, secure routing, and efficient resource utilization.

A. Jain et. al [5] presented a discussion on Mobile ad hoc network (MANET) that is lack of infrastructure support, so nodes of MANET are vulnerable to attacks. Denial of Service attacks (DOS) makes network inaccessible to users. Black hole attack is a type of DOS attack, in which mischievous node claims that it has a route towards the destination node. Ad Hoc on Demand Distance Vector (AODV) routing protocol is affected by Black hole attack. The proposed solution is based on first Route Reply (RREP) caching mechanism in AODV protocol.

N. Sabri et. al [6] presented a Gravitational Search Algorithm (GSA) that have been inspired by the Newtonian’s law of gravity and motion. There are various variants of GSA which have been developed to enhance and improve the original version. The algorithm has also been explored in many areas. Author is intended to dig out the algorithm’s current state of publications, advances, its applications and discover its future possibilities. This review is expected to provide an outlook on GSA especially for those researchers who are keen to explore the algorithm’s capabilities and performances.

D. Yazdaniet. al [7] proposed a technique for optimization purposes Artificial Fish Swarm Algorithm (AFSA) on data clustering classification technique which has been addressed by author in many disciplines and in many contexts. The contribution toward this study is twofold. First, weak points of standard AFSA including lack of using previous experiences of AFs during optimization process, lack of existing balance between exploration and exploitation and high computational load were investigated in order to present a New Artificial Fish Swarm Algorithm (NAFSA). For resolving the weak points, functional behaviors and the overall procedure of AFSA have been improved. Some parameters are eliminated and several supplementary parameters are added. Hybrid clustering algorithm was proposed by author based on NAFSA and k-means approaches. This combination leads to maximum utilization of the involved approaches for data clustering

III. PROPOSED METHODOLOGY

Here we implement both GSA and AFSA for detection and prevention of Black Hole Attack in the network. GSA detects those paths in which maximum packet loss occurs. AFSA algorithm choose that paths having more packet loss and give information to all companion nodes about the malicious nodes in the network and secure the network by avoiding connection from source nodes to those malicious or black hole nodes in the network.

PROPOSED FLOW CHART

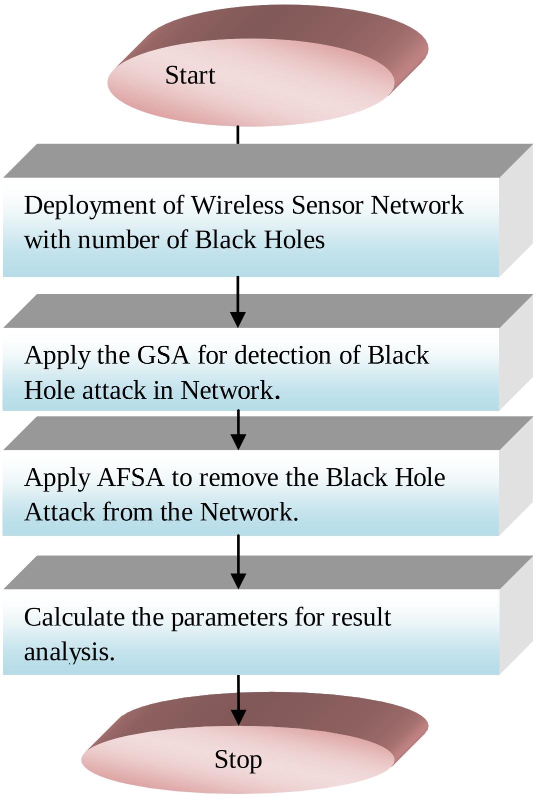
Start
Deployment of Wireless Sensor Network with number of Black Holes
Apply the GSA for detection of Black Hole attack in Network.
Apply AFSA to remove the Black Hole Attack from the Network.
Calculate the parameters for result analysis.
Stop

Figure 3: Proposed Flow Chart

DOI 10.17148/IJARCCE.2016.5833

A. GSA Algorithm:

This section describes about GSA optimization algorithm to detect black hole in the network, which is based on two Newton's law of gravitational i.e. Law of gravity and Law of Motion. Law of gravity says that 'Every particle in the universe attracts every other particle with a force that is directly proportional to the products of their masses and inversely proportional to the square of distance between them'. And Law of motion says variation in velocity or acceleration of the particle is ratio of the force acted on the network to the mass of nodes. In proposed GSA, Each object (sensor node) has the specifications like mass of object, total packets, and received packets at the particular sensor node. The rate of packet loss gives the solution of our problem. Packet loss and force are calculated with the help of fitness function. The algorithm is directed by properly regulating the packet loss and force in the network.

(a) Law of gravity: Basically it states that every particle in the universe attracts every other particle with a force that is directly proportional to the products of their masses and inversely proportional to the square of distance between them' But we define this in terms of packet loss occur in the network to detect the black hole. If there is more packet loss then black hole attack occurs otherwise not.

Consider the network with N sensor nodes. The Position of ith sensor node is given by its coordinates in the r dimension.

$$X_r = \text{rand}(1,N)*\ ar \qquad 1$$

Where X_r represents the coordinate towards r dimension. Rand (1,N) represents the random number between 1 and N. ar is total defined area of network.

Fitness function is calculated in terms of packet loss that is given by following equation:

$$P_{ik}\ (x) = M_{ik}\ (x) – N_{ki}\ (x) \qquad 2$$

Where P(x) is the packet loss related to path x. M_{ik} (x) represents the total packets send from the i node to j node. N_{ki} (x)represents the packets received by node j from the node i. i is source node and k is intermediate node and range from 2 to N.

For path k in the network, the force from node i to j is defined as:

$$F_{ik}\ (x) = \frac{Mik\ (x)*Nki\ (x)}{P_{ik}\ (x)} \qquad 3$$

Where F(x) represents force calculated of path x in the network ……x = 1,2,3,…..N-1

$P_{ik}(x)$ is packet loss related to path x. and. $M_{ik}(x)$ represents the total packets send from the i node to k node, $N_{ki}(x)$ represents the packets received by node k from the node i.

Illustration -

The detection of black hole attack depends upon the fitness value calculated. Fitness function i.e. force value is calculated in terms of sending and receiving packets at the particular node from the source node. Performance of the network checked by parameter known as packet loss. More packet loss results more chances of black hole attack in network. Packet loss is the difference of sending and receiving packets to that node.

$$F_{ik}\ (x) = \frac{M_{ik}\ (x)*N_{ki}\ (x)}{P_{ik}\ (x)} \qquad 4$$

When There is No Black Hole In The Network

Suppose total packs send by source node i to intermediate node k is 1500 and received packets by randomly deployed node k from source node is 1300. Let's say 200 packets lost due to some other network problems i.e. routing delay, traffic jam etc.

Here..M_{ik} (x)=1500 and N_{ki} (x)=1300
P_{ik} (x)=1500-1300=200

Hence F_{ik} (x) = 1500*1300/ 200 = 9750……x be any random path between 1 to N-1

When There is Black Hole in the Network

Suppose total packs send by source node i to intermediate mode k is 1500 and received packets by randomly deployed node k from source node i is 0 because of black hole present in the network. So black hole node not allows packets to be sent to the destination. That node will absorb all the packets.

Here.M_{ik} (x)=1500 and N_{ki} (x)=0
P_{ik} (x) =1500-0=1500

Hence F_{ik} (x) = 1500*0/ 1498 = 0……x be any random path between 1 to N-1

- By differentiating value of force, we can detect the black hole presence in the network. If the force has some value, then there is no black hole present, but if the force value is zero, then there is black hole present in the network. Because particular node has no connection with the destination.
-

(b) Law of motion: - The present speed of any mass is equivalent to the aggregate of the division of its past speed and the deviation in the speed. Deviation in the speed or increasing speed of any mass is equivalent to the ratio of force calculated of any path to the mass of object.

Hence according to the law of motion, the acceleration of path x at a particular time t from the node defined i to node k, in the direction eth

Then $a_{ik}(x)$ can be written as:

$$a_{ik}(x) = \frac{F_{ik}\ (x)}{m_{ik}\ (x)} \qquad 5$$

Where m_{ik} (x) represents the mass in terms of packet loss occur in particular path.

$$m_{ik}\ (x) = abs(p(x)-q(x)) \qquad 6$$

Where abs is absolute value or magnitude of the r(x), and r(x) = p(x)-q(x);
p(x) represent the theoretical packet loss w.r.t path x from node i to kth node. q(x) is actual packet loss w.r.t path x from node i to kth node.

$$p(x) = c(x) / c(x)+d(x) \qquad 7$$

Here c(x) is the probability of packets is not good and not successfully delivered. d(x) is the probability of packets are good and successfully delivered.

$$q(x) = 1- {}^{r(x)}\!/_{t(x)} \qquad 8$$

Here r(x) received packets to the particular node N and t(x) represents the total packets send by the ith source node. The fitness function value will be used in proposed AGSA algorithm to detect the particular black hole node or the path in the network. The hybridization of these two algorithms gives black hole detection and prevention more securely and in improved way.

B. AFSA algorithm:

AFSA algorithm has 3 steps to complete its process.
(i) AF_prey
(ii)AF_swarm
(iii)AF_Follow

(i) **AF_prey**: In AF_prey, generally fishes search for food to determine the presence of food and receives the information about where the food is available or not. To detect black hole node, we see our fitness function value. Search for paths for having zero fitness function value

Behaviour Desription: Let x_1 is source node and $x_{2.......}x_n$ are the intermediate nodes. Here n be any integer value. Y is the food concentration, the more value of it, AF finds global maximum value.
Here check food concentration (fitness function) for all paths available in the network.
Optimal solutions can be determined by taking the maximum food available i.e. packet loss more occurs and fitness function has the zero value.

$$F_1(d)=zero(F) \qquad 9$$

Here F_1 is the fitness function values in presence of black hole attack occur in the network. F_1 is function of d i.e. numbers of paths have the zero fitness function value in the network. Check this for all paths available in the network say paths k, l, m , n etc. Select those paths which has zero fitness function and then mark the nodes from these paths having no connectivity to destinations. These nodes referred as black hole nodes.

$$B(c)=B(count(d)) \qquad 10$$

d is name of paths having zero fitness function value. c is the number of black hole nodes.

(ii) AF_swarm:
In AF_swarm, fishes will assemble in group i.e. kind of living habitat to make colony, while searching for food available and avoid danger by giving information to all its neighbours.

Behaviour Description:
Let x_1 is source node and x_d are the black hole nodes. N is the total number of nodes in the network.
Broadcast this black hole nodes x_d to all its companions nodes (N_f availiable) in the network for avoid danger

$$(N_f / N) < 1 \qquad 11$$

(iii) AF_Follow: In moving process, fishes follow those paths in which they are secure.

Behaviour Description: Let x_1 is source node and x_d are black hole nodes.
Break the connection from source node to black hole nodes and obtain secure paths for communication.

STEPS FOR OVERALL ALGORITHM:

(1) Deploy the Wireless Sensor Network in space 200*200. Number of Nodes say N. (N=1,2,3.......100) and one BS located at 150.

(2) Select the paths from source node (N=1) to destination by bellman ford algorithm.

(3) Apply GSA:
(i) Fitness function ($F_{ik}(x)$) computed for x= 1,2,3,....N-1. As given in equation 3
(ii) Whenever $F_{ik}(x)>0$ go to step 1.
(iii) Whenever $F_{ik}(x)=0$, detection of paths occurs where black hole attack is there.

(4) Apply AFSA:
(i) AF_prey: Distract paths for which Fitness Function $F_{ik}(x)=0$ i.e. more packet loss occurs across that path and Black hole attack (nodes) x_d detected..
(ii) AF_swarm: Broadcast x_d where d is no of black hole nodes in network to all companion nodes (N_f) present in network .such that $(N_f/N) < 1$.
(iii) AF_Follow: Update the paths by source nodes to destination by disconnect connectivity from source to intended black hole node $x_{d...}$
Obtain secure paths by preventing black hole attack

(5) Computation of different performance parameter values.

IV. SIMULATION RESULTS

Performation evaluation and simulation results are carried out by using MATLAB simulator. In simulation, 100 nodes are randomly deployed in the 200*200 area. Position of destination node is 250*250. Simulation parameters are summarized in Table1.

TABLE1. SIMULATION PARMETERS

S.No.	Parameter	Value
1	Simulator	MATLAB
2	Simulation Time	7.662969s
3	Area	200*200
4	Position of bs	250*250
5	Number of Nodes	100
6	Placement of Nodes	Random
7	Number of malicious Nodes	2 to 28
8	Source Node Number	2
9	Destination Node Number	150(bs)

A. PERFORMANCE METRICS

(a) **Packet Delivery Ratio** = Σ Number of packets received / Σ Number of packets sent.

$$\text{PDR} = \sum P_R / \sum P_s$$

It is defined as the ratio of total number of packets received at particular node to the total number of packets sent from the source node. For better performance of any routing algorithm, packet delivery ratio should be more.

(b) End To End Delay=Σ{arrival time– send time}/ Number of Connections

$$\text{ETD} = \sum(A_t - S_t)/N$$

It is defined as the average time taken by the packets to send from source to destination. There should be less end to end delay to have better performance results.

B. we take simulation results by varying number of malicious nodes in the network from 2 to 28. Here Table2 Shows path description with 4 number of black hole nodes and path graphs in figures 4, figure 5 and figure6.

TABLE2: PATH DESCRIPTION.

Number of Black hole nodes	Paths having black hole nodes	String of Black hole nodes	Secure Paths
4	2-3, 2-5-8-17, 2-7, 2-18-43-29-56	3-17-7-56	2-15-150, 2-13-150, 2-14-19-20-150, 2-27-150, 2-26-28-39-76-150, 2-45-150, 2-6-9-150, 1-25-34-88-150, 2-44-150, 2-11-21-34-150, 2-44-67-150, 2-33-66-150, 2-13-16-150, 2-32-150, 2-76-81-89-150, 2-48-150, 2-65-43-150, 2-60-46-87-150, 2-41-39-150, 2-51-74-150, 2-58-150, 2-63-75-150, 2-9-88-150, 2-67-45-22-94-150, 2-49-62-24-150,2-72-150, 2-59-70-150, 2-96-27-75-150,

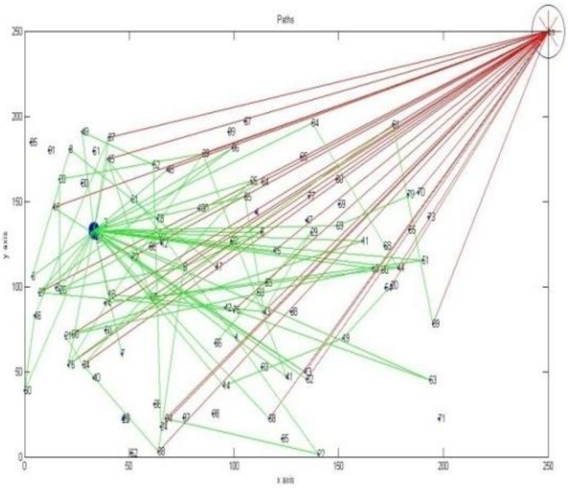

Figure5: Paths with random deployment of nodes.

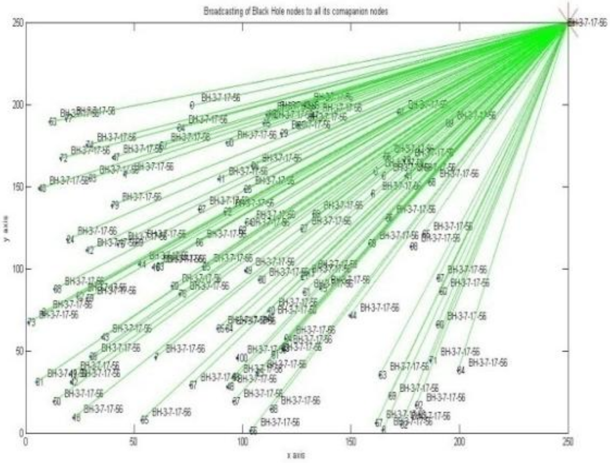

Figure6: Broadcasting of Black Hole nodes to all Its Companion nodes in network

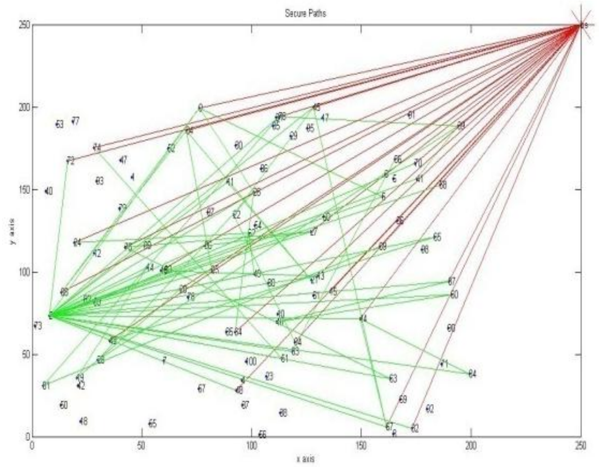

Figure7: Secure paths after removing black hole nodes in the network.

Evaluation of Performance Parameters:

Performance evaluation is done by using performance parametes i.e. Packet delivery Ratio and End to End delay. Table 3 shows the values of packet delivery ratio.

DOI 10.17148/IJARCCE.2016.5833

It compares our results with the existing algorithm Figure 8 represents the comparative graph of Packet delivery Ratio values. Table4 shows the values of End to End delay. Figure9 represents the comparative graph of End to End delay values

TABLE3: PACKET DELIVERY RATIO VALUES

S.No.	Number of Black hole nodes	Packet Delivery Ratio	
		Existing work	Proposed work
1	2	38.5	83.83
2	4	21	78.952
3	6	21	73.787
4	8	20.5	68.73
5	10	19	63.40
6	12	17	58.51
7	14	17	53.497
8	16	17.5	48.362
9	18	19	43.345
10	20	19	38.19
11	22	17.5	33.128
12	24	17	28.183
13	26	16	23.055
14	28	17	17.903

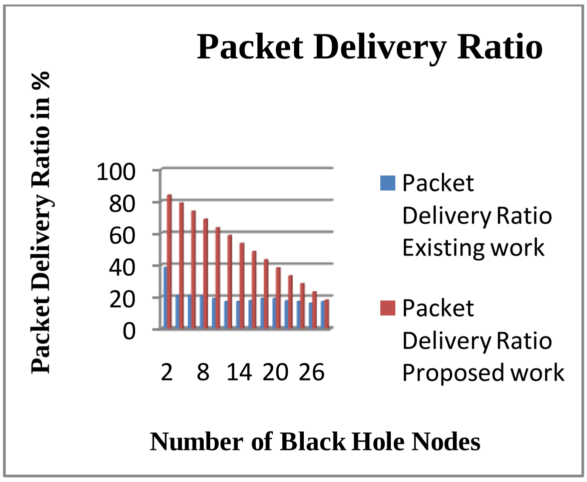

Figure8: Packet delivery Ratio Comparison Graph.

TABLE 4: END TO END DELAY VALUES.

S.No	Number of Black hole nodes	End to End delay in ms	
		Existing work	Proposed work
1	16	9.8	8.2569
2	18	12.5	8.0978
3	20	10	9.8006
4	22	10.2	6.7018
5	24	11.5	5.1028
6	26	10	6.4639
7	28	11.5	4.0086

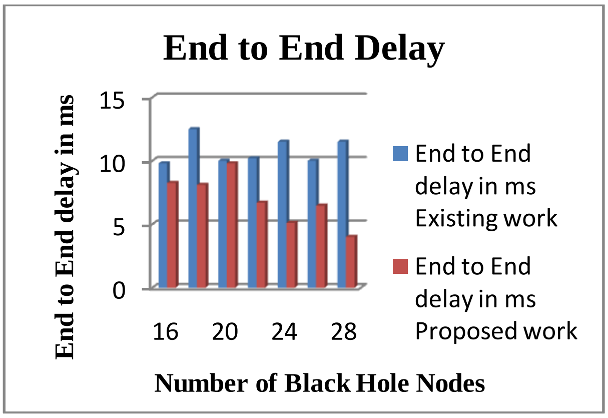

Figure9: End to End delay Comparison Graph

V. CONCLUSION AND FUTURE SCOPE

For several decades, it becomes interesting area to study natural optimization techniques to solve complex problems. In this paper, we use these natural optimization techniques to detect black hole detection and prevention. We make use of hybridization of two algorithms i.e. GSA and AFSA to detect and prevent black hole attack in the wireless sensor network. Simulation results show that proposed solution gives good performance in terms of high packet delivery ratio and low end to end delay and also effective black-hole attack detection with minimal number of packet drops. In the future work the proposed scheme will be enhanced by hybridization of various other natural optimization techniques with more innovative way to enhance the performance parameter values further.

REFERENCES

[1] Chandeep Singh, Vishal Walia , Dr.Rahul Malhotra, “Genetic Optimization Based Adaptive approach for the determination of Black Hole Attack in aodv protocol” ,2nd international conference on science, technology and management, pp 2742-2753

[2] Rashedi, E.; Nezamabadi-pour, H.; Saryazdi, S. “GSA: A Gravitational Search Algorithm”, in ELSEVIER: Information Sciences,: Volume 179, Issue 13, Iran, 2009, pp. 2232–2248

[3] Asmaa Osama Helmy, Shaimaa Ahmed, Aboul Ell Hassenian, and ”Artificial Fish Swarm Algorithm for Energy-Efficient Routing Technique” DOI: 10.1007/978-3-319-11313-5_45

[4] N. Chaudhary, "A Deep Analysis: Highly Robust Fault Tolerant Secure Optimized Energy Ad hoc Networks Methodologies for Mobile Nodes," International Journal of Advanced Research Computer Science and Software Engineering, vol. 5, no. 7, pp. 540-543, 2015.

[5] A. K. Jain and V. Tokekar, "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks.," in International Conference on Pervasive Computing, 2015.

[6] N. M. Sabri and M. Puteh, "A Review of Gravitational Search Algorithm," International Journal of Advance Software Computer Application, 2008.

[7] D Yazdani, "Fish Swarm Search Algorithm: A New Algorithm for Global Optimization," nternational Journal of Artificial Intelligence, vol. 13, no. 2, pp. 17-45, 2015.

[8] Mehdi Neshat, Ghodrat Sepidnam, Mehdi Sargolzaei, Adel Najaran Toosi,” Artificial fish swarm algorithm: a survey of the stateof-the-art, hybridization, combinatorial and indicative applications” DOI 10.1007/s10462-012-9342-2.

[9] Kai Xing, Shyaam Sundhar, Rajamadam Srinivasan , Manny Rivera, Jiang Li, Xiuzhen Cheng “Attacks and Countermeasures in Sensor Networks: A Survey” 2005 Springer

DOI 10.17148/IJARCCE.2016.5833