ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Intrusion Detection System for VANET Based on BFO Algorithm

Nivedita Kalia[1], Navjot Kaur[2]
[2]Assistant Professor
[1, 2]Deptt. of CSE,
Chandigarh Engg. College, Mohali, Punjab, India.

Abstract: A VANET (Vehicular Ad hoc Network) is an organization-less self-forming wireless networks of routers. It has impending applications in entirely capricious and dynamic environment. In specification based Intrusion Detection system, definite physiognomies of vital objects are examined and any anomaly is noticed. We recommend a method to investigate the exposure to attacks in network, precisely the utmost communal network layer hazard, Black Hole attack and to create a specification based Intrusion Detection System (IDS) using BFO Algorithm methodology. The recommended system is developed by using BFO Algorithm, which evaluates the activities of every single node and make available facts about the attack. The performance of VANET is evaluated depending upon BFO algorithm.

Keywords: Intrusion Detection, Black Hole Attack, BFO Algorithm.

I. INTRODUCTION

In the most recent couple of years, we have understood the prosperous of remote correspondence innovations. These advances have augmented acknowledgement overall in light of opened up end client bolster and ease of gear. One such specific system is an Ad hoc Network. Ad hoc implies unconstrained. In this system, the hubs inside a predetermined reach talk with one another suddenly.

Vehicular Ad hoc Network is an innovation having the craft of incorporating impromptu system, remote LAN and cell innovation to accomplish clever Inter-Vehicle Communications otherwise called Vehicle-to-Vehicle Communications and Roadside-to-Vehicle Communications. There are shots of various conceivable assaults in VANET because of open nature of remote medium [3]. Wellbeing is the essential concern to numerous street clients. The wellbeing prerequisites can be capably bolstered by numerous security applications, for example, movement report and mishap notice. There are possibilities of various conceivable assaults in VANET because of open nature of remote medium. Security is the essential concern to numerous street clients. The wellbeing prerequisites can be capably upheld by numerous security applications, for example, movement report and mishap warning. In this examination we can distinguish assaults and comprehend assailants by utilizing the classes of assault. In the event that we control assailants and their assaults then it would help in sparing human life. Additionally, a powerful arrangement is proposed for Black gap assault which utilizes the repetition disposal component comprises of rate diminishing calculation and state move instrument as its parts.

The remote channel is anything but difficult to get to both earnest and prohibited system clients. There is no point by point place where 24-hour consideration of movement and giving controlled access can be very much characterized. The current Ad hoc code of conduct expected as a truthful and organized environment. In this manner, a banned individual with no inconvenience can turn into a switch and hinder system forms by not consent to the convention necessities. The liabilities of VANET in the system layer is typically classified into two subdivisions, particularly steering assaults and parcel sending assaults in light of the target of operation of the assaults. An Intrusion Detection System (IDS) is a product framework which is utilized to analyze pernicious practices and strategy contaminations in a system and produces reports [6]. These in a broad sense can be categorized as one of the three gatherings particularly, Specification based IDS, Anomaly based and Signature Based.

The determination based framework, it rundowns the anticipated activities of crucial items and aptitude security points, which are further by then coordinated with essential article highlights. The Anomaly based IDS comprise of taking the profiles of regular activities of frameworks by customized preparing and hailing the unidentified activity to be dicey while under methodology. The mark based IDS is used regularly to contrast the information interestingly with recognized highlights and used to point of confinement perceived assaults. This recognizes new assaults, however prompts false caution on high likelihood [7]. The principal righteousness of this is priori data of the assault is not fundamental and thus thoroughly utilized as a part of the different utilizations of a few stringent projects and various different conventions. This paper give insights about the progressing research on interruption location frameworks proposed for distinguishing system layer assaults in vehicular Ad hoc systems. An answer is proposed which is taking into account the BFO IDS technique for the recognition of vulnerabilities.

The Optimized Link State Routing Protocol (OLSR) is created for portable impromptu systems. It works as a table driven, proactive convention, i.e. trades topology data with different hubs of the system consistently. OLSR is a proactive directing convention for portable impromptu systems. The convention acquires the strength of a connection state calculation and has the benefit of having courses instantly accessible when required because of its proactive nature. OLSR is an improvement over the established connection state convention, custom-made for portable specially appointed systems. OLSR minimizes the

overhead from flooding of control activity by utilizing just chose hubs, called MPRs, to retransmit control messages.

This method essentially decreases the quantity of retransmissions needed to surge a message to all hubs in the system. Besides, OLSR requires just incomplete connection state to be overflowed so as to give briefest way courses. The negligible arrangement of connection state data needed is, that all hubs, chose as MPRs, MUST proclaim the connections to their MPR selectors. Extra topological data, if present, MAY be used e.g. for repetition purposes. OLSR is composed to work in a totally disseminated way and does not rely on upon any focal substance. The convention does NOT REQUIRE dependable transmission of control messages: every hub sends control messages occasionally, and can thusly maintain a sensible loss of some such messages. Such misfortunes happen habitually in radio systems because of crashes or other transmission issues. Additionally, OLSR does not require sequenced conveyance of messages. Every control message contains a grouping number which is increased for every message. Hence the beneficiary of a control message can, if needed, effortlessly recognize which data is later - regardless of the fact that messages have been re-requested while in transmission.

II. RELATED WORK

Table: 1 Literature Survey

Author Name	Paper Name	Technique
Wang Yunwu [1]	Using Fuzzy Expert System based onGenetic Algorithm for Intrusion Detection System	Fuzzy based Genetic Algorithm approach.
Wei Li [2]	Using Genetic Algorithm for Network Intrusion Detection	Genetic Algorithm based intrusion detection system which was tested with TCP/IP networks
AnupGoyal and Chetan Kumar [4]	GA-NIDS: A Genetic Algorithm based Intrusion Detection System	Suggested a systematic learning method known as Genetic Algorithm (GA), to identify illegitimate nodes
YutengGuo [5]	Feature Selection based on Rough Set and modified Geneticprogramming for Intrusion Detection	Method based on Rough Sets and improved Genetic Algorithms is proposed
Akansha Saini and Harish kumar [8]	Effect of Black hole attack on AODV Routing Protocol In MANET.	Use of AODV routing process because of the cooperative Black Hole Attack.
[13] C. Karlof and D. Wagner	Secure routing in wireless sensor networks: Attacks and countermeasures	Multiple routes were computed for transmission of shares of different packets using multipath routing algorithms like DSR, AODV. These routes were node-disjoint.
[14]Manvi Arya	BFO Based Optimized Positioning For Black Hole Attack Mitigation in WSN	Propose an efficient technique that uses multiple base stations to be deployed randomly in the network to counter the impact of black holes on data transmission using BFO.
[15]1Harmanpreet Kaur, 2P. S. Mann	Prevention of Black Hole Attack in MANETs Using	proposed a scheme to detect Black hole attack in a network using DSR.S
	Clustering Based DSR Protocol	

III. PACKET DROP ATTACK

A packet drop attack is also known as black hole attack in the network layer [9]. In black hole attack node drops packets at each step, then high loss of data takes place in the network. The node that drops the packet is malicious node. This attack can be viewed as following:

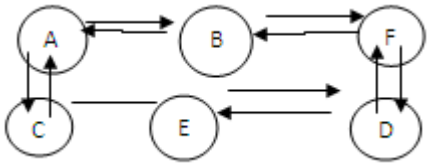

Figure.1.3 Black Hole Attack/ Packet Drop Attack

Above figure shows that node A wants to send data to node D. So 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 A node. As soon as node A starts to send the packet the node C drops packet in the middle of the data sending process [10].

IV. BFO(BACTERIA FORAGING OPTIMIZATION ALGORITHM)

Through foraging of the real bacteria, locomotion is achieved by a set of tensile flagella. Flagella help an *E.coli* bacterium to trip up or swim, which are two basic operations perform by a bacterium at the time of foraging [16]. When they spin the flagella in the clockwise route, each flagellum heave on the cell that fallout in the moving of flagella separately and to finish the bacterium tumbles with smaller number of tumbling whereas in a damaging place it tumbles often to find a nutrient gradient. Moving the flagella in the counter clockwise course helps the bacterium to swim at a very fast speed. In the above mentioned algorithm the bacteria undergoes chemo taxis, where they like to move towards a nutrient incline and avoid noxious surroundings. A usually the bacteria move for a longer coldness in a welcoming environment. Figure 1.4 depicts how clockwise and counter clockwise association of a bacterium take place in a nutrient explanation.

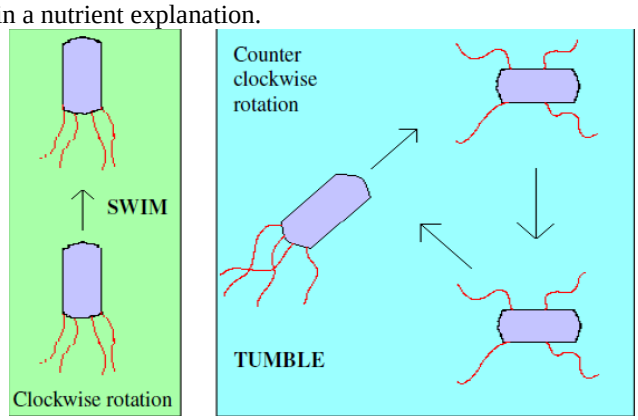

Figure 1.4 Swim and tumble of a bacterium

When they get food in adequate, they are enlarged in length and in attendance of appropriate temperature they

break in the center to from an accurate replica of itself. This phenomenon inspired passing to initiate an event of imitation in BFOA. Due to the incidence of sudden ecological changes or attack, the chemo tactic progress may be shattered and a group of bacteria may move to some other places or some other may be introduce in the swarm of concern. This constitutes the event of removal dispersion in the real bacterial population, where all the microorganisms in a region are killed or a group is discrete into a new part of the surroundings.

V. PROPOSED METHODOLOGY

Following flowchart shows the working of BFO algorithm approach and the parameters like packet drop, request forwarding rate, route request receive that has been taken to implement BFO algorithm [11] based approach for prevention of black hole attack in the network.

a. For Each Node Blackhole=0;
b. ReceiveReply (Packet P){
c. if(BALCKHOLE~=1 AND P has an entry in Route Table){
d. selectDest_Seq_No from routing table
e. if(P.Dest_Seq_No>Dest_Seq_No){
f. If (Rrep Not Sent)
g. Then Blackhole=1;
h. ELSE
i. update entry of P in routing table
j. unicast data packets to the route specified in RREP
k. BLACKHOLE=0;
l. }
m. else {
n. discard RREP
o. }
p. }
q. else {
r. if(P.Dest_Seq_No>= Src_Seq_No){
s. Make entry of P in routing table
t. }
u. else {
v. discard this RREP
w. }}}

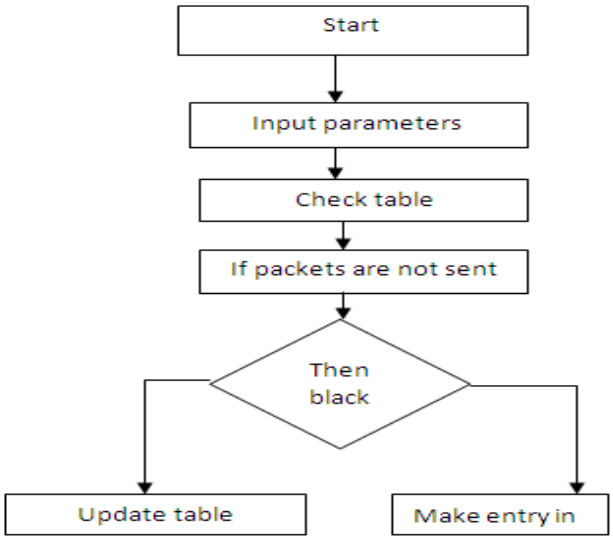

Figure. 1.5 Proposed flowchart

VI. SIMULATED RESULTS

Below Figure shows the black hole detection rate and the procedure to detect the black hole attack in the MATLAB environment.

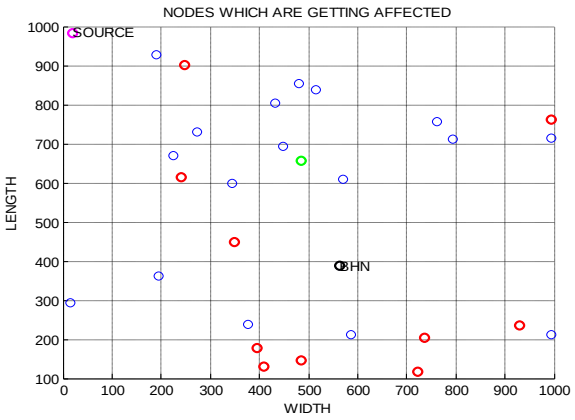

Figure 1 Vehicular Network nodes

The above figure shows the VANET that shows the Black Hole node in black color and the red color nodes which are affected by the black hole node. The network is configures in 1000*1000 area.

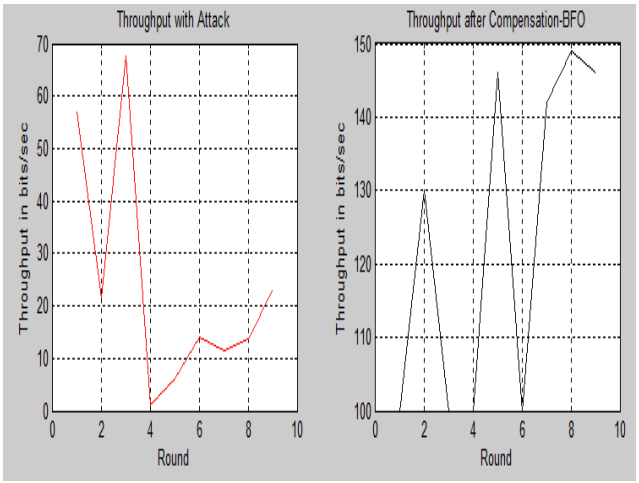

Figure 2 Throughput graph

The above figure shows the network throughput performance with attack and compensation using Bacteria foraging optimization with respect to the number of rounds and throughput is increased after applying BFO which increases the network lifetime.

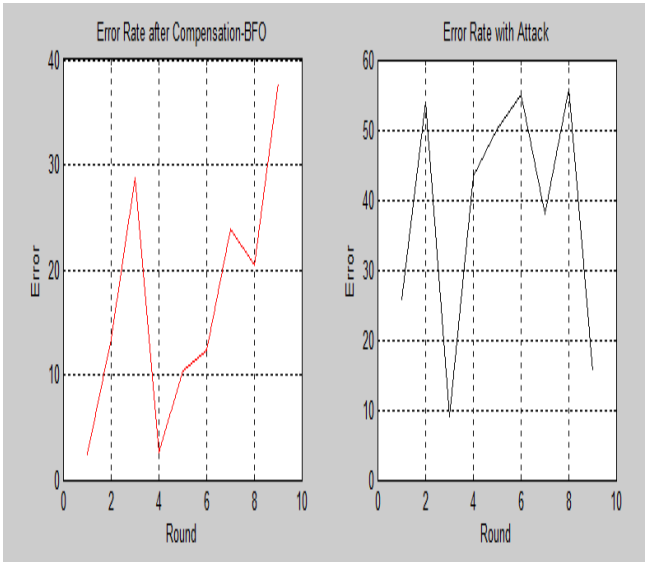

Figure 3 Error rate

The above figure shows the error rate in the presence of attack and compensation using Bacteria Foraging optimization. The Error rate is more with attack which is compensated less after applying optimization algorithm

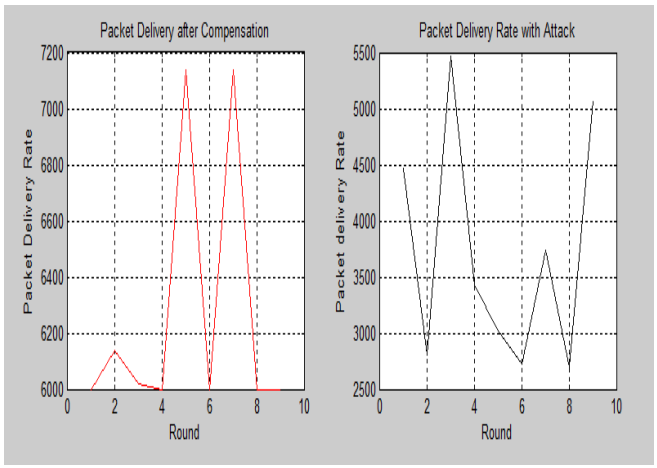

Figure 4 Packet Delivery Rate

The above figure shows the packet delivery rate with attack which is less i.e. the packet delivery to the destination is less due to black hole attack and after applying BFO the rate is increasing which should be high to increase the network lifetime.

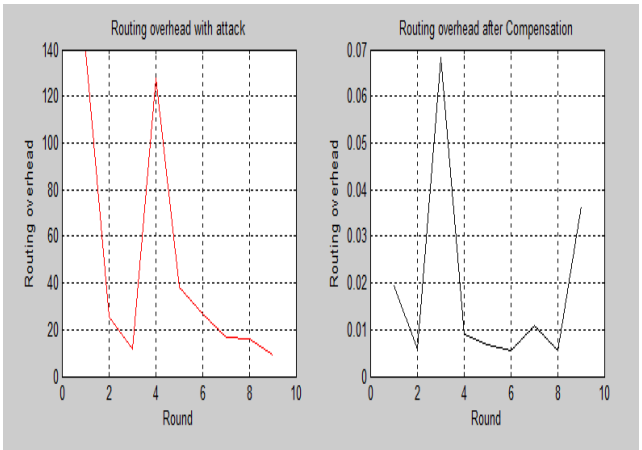

Figure 5 Routing overhead

The above figure shows the routing overhead in the presence of the black hole attack and after apply Bacteria foraging the routing overhead is compensated which should be less for appropriate communication

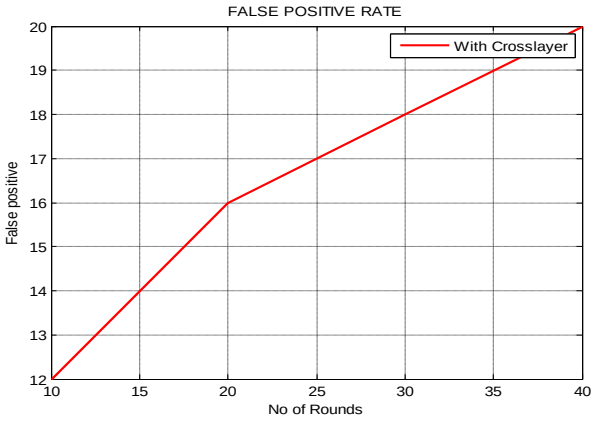

Figure 6 False positive rates (previous technique)

The above figure shows the false positive rate using cross-layer technique with respect to number of rounds and it is compensated using bacteria foraging optimization to get efficient output

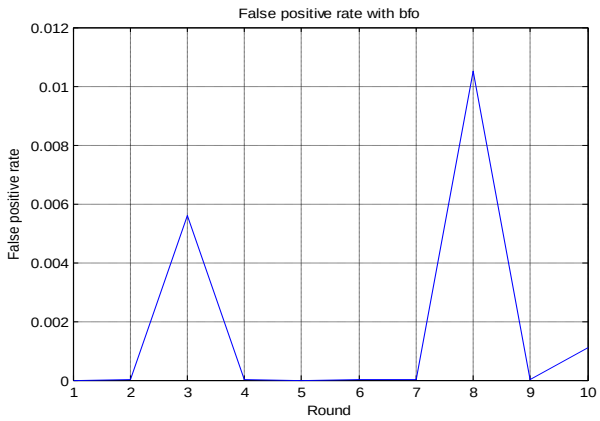

Figure 7 False positive rates

The above figure shows the false positive rate using bacteria foraging optimization which is very less as compared to cross layer previous technique

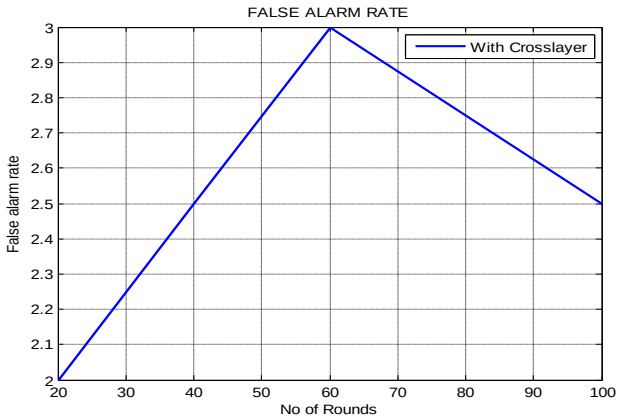

Figure 8 False alarm rates (previous approach)

The above figure shows the false alarm rate with respect to number of rounds and it refers to the probability

of falsely rejecting the null hypothesis for a particular test which is approaching to 2.5

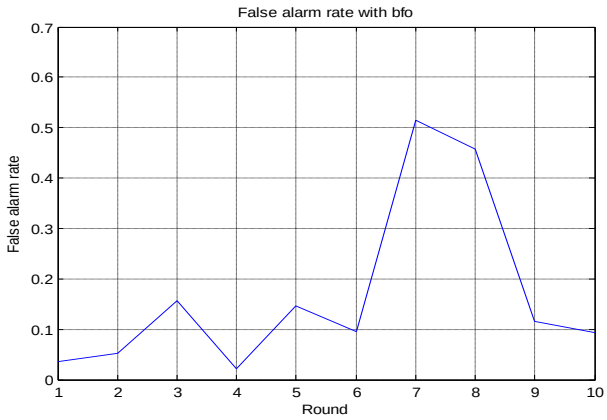

Figure 9 False Alarm rate using proposed technique

The above figure shows the False alarm rate which should be less to get the appropriate output than the crossbreed technique used as previous approach. Lesser the false alarm rate more will be the accuracy of the system.

VII. CONCLUSION AND FUTURE SCOPE

In this paper, the issues related to packet drop attack has been studied and then an intrusion detection system has been implemented using BFO algorithm. The proposed algorithm has been tested with various parameters as well as with various network configurations. This algorithm has led to enhancement of the accuracy rate of the network. Future scope lies in the use of malicious node in which malicious node can be used to prevent the routing problem via attacker.

VIII. REFERENCES

[1]. Wang. Yu , "Using Fuzzy Expert System based onGenetic Algorithm for Intrusion Detection System", April 2009.

[2]. Wei Li, " Using Genetic Algorithm for Network Intrusion Detection", 2010.

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

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

[5]. Yuteng Guo, Beizeng Wang, Xingxing Zhao, XiaobiaoXie, Lidalin and QindaZhou,"FeatureSelection based on Rough Set and modified Geneticprogramming for Intrusion Detection", In proceedings of 5th International Conference of Computer Science and Education. August 2010.

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

[7]. Sheenu Sharma and Roopam Gupta, "Simulation Study of Black hole Attack in Mobile Adhoc Networks", In proceedings of Engineering Science and Technology. 2009.

[8]. Akansha Saini and Harish Kumar "Effect of Black hole attack on AODV Routing Protocol In MANET", International Journal of Computer Technology, Volume1, Issue 2, December 2010.

[9]. Rajib Das, Dr.BipulSyamPurkayastha and Dr.Pradipto Das "Security Measures for Black hole Attack in MANET: An Apporach" InternationslJournal of Engineering Science and Technology,2009.

[10]. P. Michiardi, R. Molva. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks". European Wireless Conference, 2002.

[11]. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black hole Attack in Mobile Ad Hoc Networks" Proceedings of the42nd annual Southeast regional conference ACM-SE 42, APRIL 2004, pp. 96-97.

[12]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Department of Computer Science, IACC 258 North Dakota State Universities, Fargo, ND58105.

[13]. C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier's Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, September 2003.

[14]. Manvi Arya, "BFO Based Optimized Positioning For Black Hole Attack Mitigation in WSN", International Journal of Engineering Trends and Technology (IJETT) – Volume 14 Number 1 – Aug 2014.

[15]. Harmanpreet, "Prevention of Black Hole Attack in MANETs Using Clustering Based DSR Protocol", IJCST Vol. 5, Issue 4, Oct - Dec 2014.

[16]. Das, Swagatam, et al. "Bacterial foraging optimization algorithm: theoretical foundations, analysis, and applications." Foundations of Computational Intelligence Volume 3. Springer Berlin Heidelberg, 2009. 23-55.