Jaya *et al*, International Journal of Computer Science and Mobile Applications,
Vol.3 Issue. 9, September- 2015, pg. 42-52 **ISSN: 2321-8363**

Wireless Sensor Network: Black Hole Attack Detection Using BFO-FUZZY

Miss. Sunita Rani
School of Engineering & Sciences,
BPS Mahila Vishwavidyalaya Khanpur Kalan, Sonepat, Haryana-(India)

Jaya
School of Engineering & Sciences,
BPS Mahila Vishwavidyalaya Khanpur Kalan, Sonepat, Haryana-(India)

Abstract: Security is an essential feature in wireless networks. Wireless sensor network is a dynamic network with large number of mobile nodes. As the traffic increases over the WSN, it will lead to a number of problems like network congestion and packet loss. This congestion and packet loss occurs due to the attack in WSN. One of the profound attacks is black hole attack. As a result some packets are lost over the network which eventually slows down the communication process. With the help of a rigorous literature review we tend to suggest the solution against black hole attack which is based on fuzzy rule. BFO-fuzzy rule based solution identifies the infected node as well as it provides the solution to reduce data loss over network. We also provide a detailed performance evaluation based on various network parameters. The proposed scheme can be used to identify 99% black hole nodes with almost negligible false.

Keywords: WSN, Fuzzy logic, Black hole attack, Packet loss, Data rate, AODV, bacteria, fuzzy functions.

1) Wireless sensor Network: This type of Wireless communication is used to transfer data among users without a wired infrastructure. Using electromagnetic waves, mobile users transmit and receive data over the air. Wireless communication spreads from home RF to satellites, from cellular phones to walkie-talkies. Its mobility, simplicity and cost saving installation advantages make the wireless communication more popular, especially in recent decades Increasing user mobility needs and developments in the use of laptop computers and PDA's is one of the main reasons of the popularity of wireless networks ***et al*** **[6]**

1.1) Black Hole Attack : In black hole ***et al*** **[1] [8]** 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. 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 ***et al*** **[2].** 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 ***et al*** **[3].**

The method how malicious node fits in the data routes varies. Fig. 1.1 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.

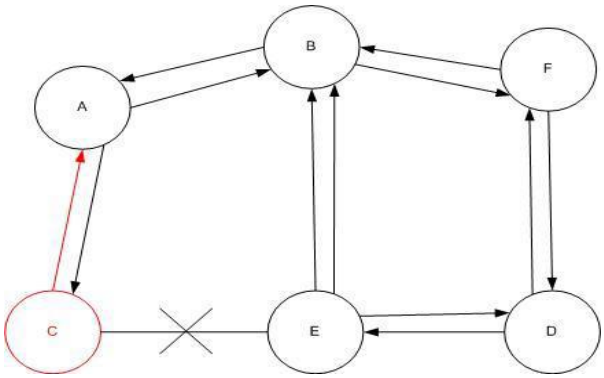


Fig. 1.1 Black Hole Problem

1.2) Black hole attack in AODV :Two types of black hole attack can be described in AODV in order to distinguish the kind of black hole attack ***et al*** **[5] [9].**

Internal Black hole attack: This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route

External Black hole attack: External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

2) Objective: In mobile networks day by day problem of call dropping is increasing because of black hole attack. Data packets are either dropped in to black hole or altered. According to survey of DTE India around 35% call dropping problem still exists. Many methods have been suggested for this. One of them is using multiple base stations which are further connected to single head. In this, signals reaching

to any base station are considered as received signal. Base station positions are kept fixed. But those signals passing through black hole region will also get dropped. To avoid this base station position can be such that all signals reaches to them. Optimization technique can be used to find out the optimal position of base station so that maximum signals avoid the path of black hole region and reach to base station. Considering theses problems, following will be our key objectives :

- Multiple base station (MBS) approach will be adopted to reduce the effect of black holes
- Positioning of multiple base station will not be fixed at four corners as was in some previous work found, rather than a bio inspired optimization technique named firefly optimization will be used which will optimally locate the position of base stations.**et al [7]**
- Fuzzy logic approach will be used to identify the black hole attack and comparison with various number of base stations will be shown.

2.2)Bacterial Foraging Optimization: Bacteria Foraging Optimization Algorithm (BFOA), is a new comer to the family of nature-inspired optimization algorithms. For over the last five decades, optimization algorithms like Genetic Algorithms (GAs), Evolutionary Programming (EP), Evolutionary Strategies (ES), which draw their inspiration from evolution and natural genetics, have been dominating the realm of optimization algorithms. Recently natural swarm inspired algorithms like Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO) have found their way into this domain and proved their effectiveness. Application of group foraging strategy of a swarm of *E.coli*bacteria in multi-optimal function optimization is the key idea of the new algorithm. Bacteria search for nutrients in a manner to maximize energy obtained per unit time. Individual bacterium also communicates with others by sending signals. A bacterium takes foraging decisions after considering two previous factors. The process, in which a bacterium moves by taking small steps while searching for nutrients, is called chemotaxis and key idea of BFOA is mimicking chemotactic movement of virtual bacteria in the problem search space. ***et al*** **[12] [13]**

During foraging of the real bacteria, locomotion is achieved by a set of tensile flagella. Flagella help an *E.coli*bacterium to tumble or swim, which are two basic operations performed by a bacterium at the time of foraging. When they rotate the flagella in the clockwise direction, each flagellum pulls on the cell. That results in the moving of flagella independently and finally the bacterium tumbles with lesser number of tumbling whereas in a harmful place it tumbles frequently to find a nutrient gradient. Moving the flagella in the counter clockwise direction helps the bacterium to swim at a very fast rate. In the above-mentioned algorithm the bacteria undergoes chemotaxis, where they like to move towards a nutrient gradient and avoid noxious environment. Generally the bacteria move for a longer distance in a friendly environment. Figure 4.1 depicts how clockwise and counter clockwise movement of a bacterium take place in a nutrient solution When they get food in sufficient, they are increased in length and in presence of suitable temperature they break in the middle to from an exact replica of itself. This phenomenon inspired Passino to introduce an event of reproduction in BFOA. Due to the occurrence of sudden environmental changes or attack, the chemotactic progress may be destroyed and a group of bacteria may move to some other places or some other may be introduced in the swarm of concern. This

constitutes the event of elimination-dispersal in the real bacterial population, where all the bacteria in a region are killed or a group is dispersed into a new part of the environment.

2.2) FUZZY LOGIC CONTROLLER: The fuzzy logic controller for the proposed black hole region detection has two real time inputs measured at every sampling time, named energy consumed and packet loss and one output named trust ***et al* [10] [11].** The input signals are fuzzified and represented in fuzzy set notations by membership functions. The defined 'if … then …' rules produce the linguistic variables and these variables are defuzzified into control signals for comparison with a carrier signal to generate PWM inverter gating pulses. Fuzzy logic control involves three steps: fuzzification, decision-making and defuzzification. Fuzzification transforms the non-fuzzy (numeric) input variable measurements into the fuzzy set (linguistic) variable that is a clearly defined boundary. In the proposed controller, the energy consumed and packet loss are defined by linguistic variables such as low, medium and high characterized by memberships. The memberships are curves that define how each point in the input space is mapped to a membership value between 0 and 1.

3) PERFORMANCE EVALUATION: Our work is detecting the black hole in the network. We used multiple base stations for this and data packet reached at any base station is considered as successful delivery ***et al* [4].** The motto of using multiple base stations is to increase delivery rate of packets. We used MATLAB as a tool to simulate the proposed work as it provides an easy to use interface and wide range of functions which can be used directly. Initially a wireless sensor network is simulated in MATLAB using 100 numbers of nodes which are displaced in 100*100 region. The statistics used for simulation of WSN are used in table 3.1 below.

Table 3.1: Parameters considered for simulation

Parameters	Values
Node number	100
Geographical area	100*100
Base station	4
Black hole radius(m)	20,30,40,50
Node's transmission range	16 m
Packet size	64 bytes
Data rate	4,6,8,10,12,14 packets/sec
Energy consumption per bit in the transmitter or receiver circuitry	50 nJ
energy consumption for multipath fading	0.0015 pJ
Data aggregation energy consumption	5 nJ

Initially base stations are placed at four corners of geographical area and source node is chosen randomly amongst given nodes. The black hole node is knowingly assigned to any node other than

source node. it will affect all nodes which come under its circular area made by its radius as shown in figure 3.1. Route form source node to base station is found out by using AODV protocol which is shown by colored path in figure 3.1. four routes for four base stations will be identified and if any route passes through black hole affected area which is shown by magenta color in the same figure, data packets will not be transferred further as these will trap into black hole and no packet will move further on that path and a complete loss of data packets will occur. So base stations positions are optimized to avoid this path and new locations are searched using bacterial foraging optimization as discussed in previous chapter. The objective function defined, minimizes the total distance of source node to each base station and effectiveness of correct optimization can be checked by plotting the fitness function value.

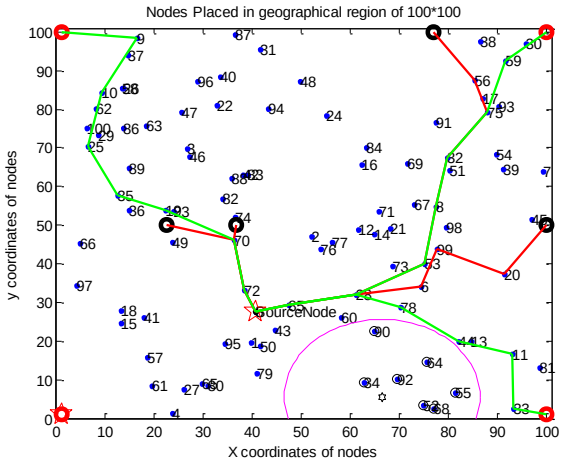


Figure 3.1: AODV path made form source to base stations

An animation window for bacteria's movement is displayed when script is executed and all bacteria set to a minimum optimal position as shown in figure 3.2 below. This minimal position attained by all bacteria proves our optimization is correct. The minimized objective function plot is shown ii figure 3.3.

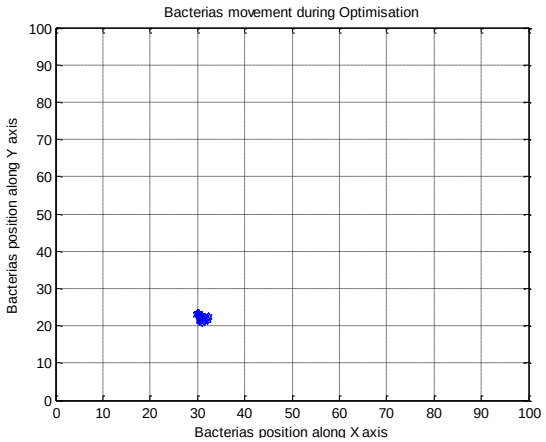


Figure 3.2: minimal position attained by bacteria

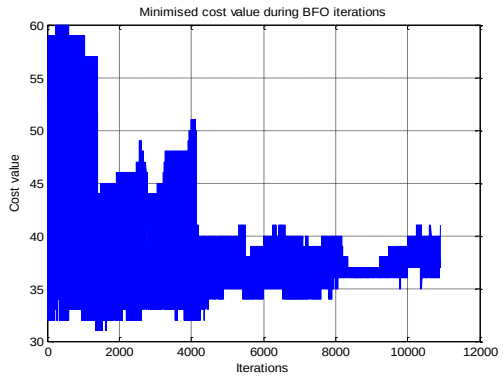


Figure 3.3: fitness function plotting of BFO

Figure 3.3 shows that fitness function is decreasing with iterations and around 11000 iterations are done in our work. Correct optimization depends upon the fact that fitness function value should decrease with iteration. After optimization network gets new locations for all base stations from which nodes are at minimum distance. A new path for packet transfer is constructed by AODV protocol and that path is usually avoided by black hole radius. Some cases may also be observed with new path also passing through black hole radius. In such cases again optimization is the solution as in every new optimization, new locations of base stations will be obtained. ***et al*** **[14]**.

An animation window for bacteria's movement is displayed when script is executed and all bacteria set to a minimum optimal position as shown in figure 3.2 below. This minimal position attained by all bacteria proves our optimization is correct. The minimized objective function plot is shown ii figure 3.3. As discussed in previous chapter we have used fuzzy logic to find out whether route followed is black hole route or not. The energy consumed in transmission and reception of packet is calculated on the basis of distance using radio model for energy consumption and packet loss on the basis of energy is calculated

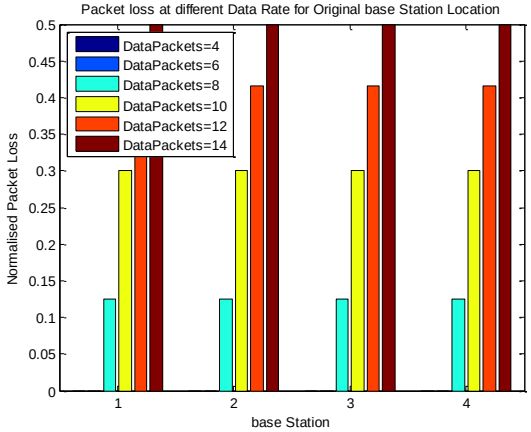
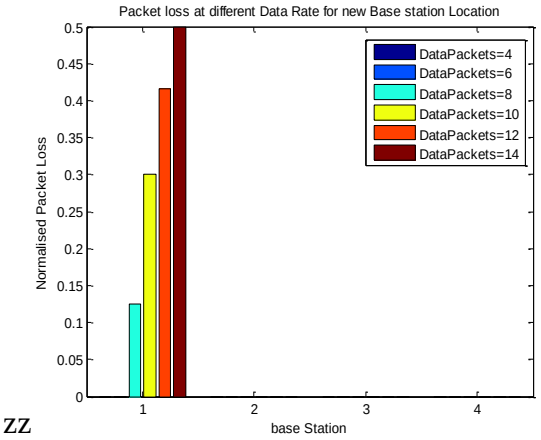


Figure 3.4: packet losses for all base stations before optimisation



ZZ

Figure 3.5: packet losses for all base stations after optimization

Figure 3.4 and 3.5 shows the packet loss before and after optimization. These are normalised packet loss. In figure 3.5 for base station 1 and base station 2, packet loss is zero, it means these are nearby source node and not much energy losses are visible. `These losses are checked for a radius of 20 meter. Losses in the packet depend upon the packet size too. Small is the packet size losses are less and larger is size, higher are losses.

Figure35.5 shows the losses for data packets 4 and 6 are zero but as it increases to 8 packets, 0.13 packets are lost or 13% packets are lost, which increases with increase in number of packets and for 14 data packets, it is 100%. Same can be checked with the case with unoptimized base station position. Figure 3.5 shows the losses for data packets 4 and 6 are zero but as it increases to 8 packets, 0.13 packets are lost or 13% packets are lost, which increases with increase in number of packets and for 14 data packets, it is 100%. Same can be checked with the case with unoptimized base station position. The new path discovered using AODV protocol for which losses are less is shown in table 5.2 below.

Table 3.2: new path assigned by AODV protocol for all base stations

To Base station 1	88 -> 52 -> 25 -> 22 -> 2 -> 93 -> 34 -> 46 -> 9 -> 38 -> 24 -> 6 -> 57 -> 102
To Base station 2	88 -> 17 -> 94 -> 97 -> 103
To Base station 3	88 -> 52 -> 25 -> 22 -> 2 -> 93 -> 14 -> 58 -> 56 -> 53 -> 3 -> 104
To Base station4	88 -> 52 -> 25 -> 22 -> 2 -> 1 -> 51 -> 50 -> 71 -> 12 -> 105

Packet losses increase with increase in the black hole radius as shown in figures 3.6-3.8 and ahead and table for them as per base station losses is shown in table 3.3-3.6.

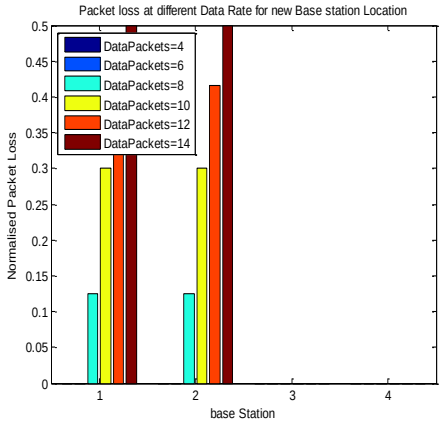


Figure 3.6: Packet losses with black hole radius=30 meter

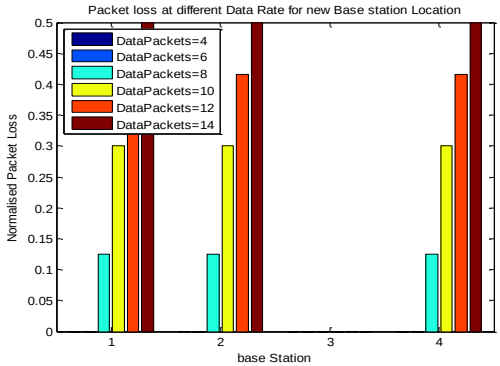


Fig 3.7: Packet losses with black hole radius=40 meter

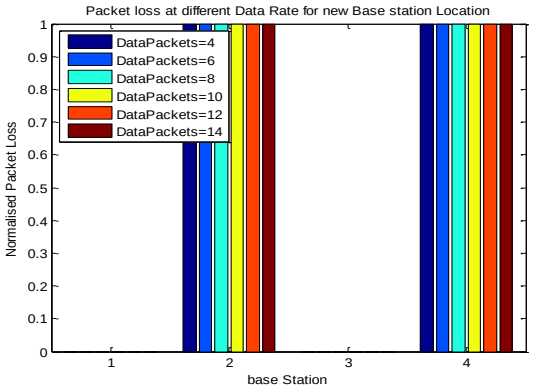


Figure 3.8: Packet losses with black hole radius=50 meter

Table 3.3: packet losses for base station 1

Black Hole Radius=20	Black Hole Radius=30	Black Hole Radius=40	Black Hole Radius=50
0	0	0	0
0	0	0	0
0	0.1250000	0.12500	0
0	0.3000000	0.3000	0
0	0.4166666	0.41666	0
0	0.5000000	0.50000	0

Table 3.3: packet losses for base station 2

Black Hole Radius=20	Black Hole Radius=30	Black Hole Radius=40	Black Hole Radius=50
0	0	0	1
0	0	0	1
0	0.1250000	0.1250000	1
0	0.3000000	0.3000000	1
0	0.4166666	0.4166666	1
0	0.5000000	0.500000	1

Table 3.3: packet losses for base station 3

Black Hole Radius=20	Black Hole Radius=30	Black Hole Radius=40	Black Hole Radius=50
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0
0	0	0	0

Table 5.3: packet losses for base station 4

Black Hole Radius=20	Black Hole Radius=30	Black Hole Radius=40	Black Hole Radius=50
1	0	0	1
1	0	0	1
1	0	0.12500000	1
1	0	0.30000000	1
1	0	0.41666667	1
1	0	0.0000000	1

4) Conclusion: Having simulated the Black Hole Attack, we saw that the packet loss is increased in the ad-hoc network. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the radius of Black Hole Nodes is increased then the data loss would also be expected to increase.

To avoid this instead of using single base station, 4 similar base stations are used. Initially packet loss for the fixed base station positions at the four corners of the region is checked. Then their positions are optimized rather than fixed corner position using BFO such that every base station has minimum distance form nodes and nodes have to consume less energy to transmit the data so that packet losses are decreased. Black hole is a problem in that as it doesn't let pass the message through its region. To detect the black hole path a trust value using fuzzy logic is used. That trust value will be calculated on the basis of energy of node and packet loss as input ion the fuzzy logic. In chapter 5, tables of simulation results show the difference between the number of packets lost in the network with and without black hole detection scheme.

References

[1] Harmandeep Kaur, "A Novel Approach To Prevent Black Hole Attack In Wireless Sensor Network" International Journal For Advance Research In Engineering And Technology, Vol. 2, Issue VI, June 2014.

[2] Namita Sharma, "Effect of Varying Initial Energy on Multihop Routing Protocol in Wireless Sensor Network" International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014.

[3] C. Kolias, "Swarm intelligence in intrusion detection: A survey." IJAFRC, Volume 2 Issue3, Nov 2011.

[4] Satyajayant Misra, "Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks"IEEEE, 2011
[5] C.V.Anchugam, " Detection Approach for Black Hole Attack on AODV in MANETs using Fuzzy Logic System" International Journal of Advanced Information Science and Technology Vol.33, No.33, January 2015.
[6] ZHIHUA HU, "FUNDAMENTAL PERFORMANCE LIMITS OF WIRELESS SENSOR NETWORKS"IEEE, 2006.
[7] Binitha S, "A Survey of Bio inspired Optimization Algorithms" International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-2, May 2012.
[8] Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic" International Journal of Science and Research, Volume 2 Issue 8, August 2013.
[9] Yash Pal Singh, "A Survey on Detection and Prevention of Black Hole Attack in AODV- based MANETs" journal of information, knowledge and research in computer engineering, nov 12 to oct 13 ,volume – 02, issue – 02.
[10] Poonam Yadav, " A Fuzzy Based Approach to Detect Black hole Attack"International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.
[11] Jaspreet kaur, "BHDP Using Fuzzy Logic Algorithm for Wireless Sensor Network under Black Hole Attack" International Journal of Advance Research in Computer Science and Management Studies Volume 2, Issue 9, September 2014 pg. 142-151.
[12] Marcelo H.T. Martins, "Decentralized Intrusion Detection in Wireless Sensor Networks." Q2SWinet'05, October 13, 2010.
[13] Ioannis Krontiris, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks."International Journal of Advanced Science and Technology Vol. 36, November, 2009.
[**14]** C. Kolias, "Swarm intelligence in intrusion detection: A survey." IJAFRC, Volume 2 Issue3, Nov 2011.

