INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

SECURE AND ENERGY EFFICIENT PROTOCOL USING BFO & FUZZY LOGIC IN WSN

Renu Dahiya[1], Navneet Verma[2]

[1]Geeta Engineering College
Naultha, Panipat, Haryana (132103), India
renudahiya23@gmail.com
[2] Geeta Engineering College
Naultha, Panipat, Haryana (132103), India
navneet.cse@geeta.edu.in

Abstract*: A Wireless sensor network is a temporary network set up by wireless mobile computers (or nodes) moving arbitrary in the places that have no network infrastructure. Since the nodes communicate with each other, they cooperate by forwarding data packets to other nodes in the network. Thus the nodes find a path to the destination node using routing protocols. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. There is lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. We have used multiple base station approach to prevent the black hole attack. Since, black hole doesn't let go the data which passes through its region, so best solution is that data should avoid the path of black hole. On this basis we used multiple base station concepts which considers the message delivered if any of base station received that. The positions of base stations are optimized with the bacterial foraging optimization (BFO) and fuzzy logic, so that all base stations are at minimum distance from the nodes and nodes have to spend less energy in transferring data packets to base station.*

Keywords: *WSN, TinyOS, BFOA, Black Hole Attack.*

1. INTRODUCTION

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. If minimum two stations in a BSA communicate with each other, they are members of the BSS. The 802.11 standard has two BSS modes. These are ad-hoc and Infrastructure networks. **Infrastructure Network:** This network is called as Infrastructure Basic Service Set (Never called IBSS). Stations in a same BSA communicate with each other over access points. Thus, a station communicates with another at two hops. **Ad-Hoc Network:** This network is called Independent Basic Service Set (IBSS) Stations in an IBSS communicate directly with each other and do not use an access point. Because of the mobility associated with ad-hoc networks, they are commonly called MANET (Mobile Ad-hoc Network). There are many type of attack in WSN basically Black hole attack. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. Black hole akin to real meaning which swallows all objects and matter.

To succeed a black hole attack, malicious node should be positioned at the center of the wireless network. Black hole attack affects the whole network.

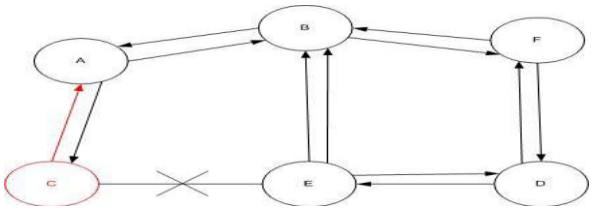

Figure 1: Black Hole Problem

2. LITERATURE REVIEW

In the wireless networks, radio communication is the medium of choice. A wireless network is any type of computer network that uses wireless data connections for connecting network nodes. It enables people to access and communicate to other devices without any need of wires. MANET is a collection of various mobile nodes. . In the MANET, different types of attacks are possible. These attacks are categorized as: active attacks and passive attacks. The most common attack in MANET is black hole attack. The black hole attack comes under the category of denial of services attack [16]. There proposed the algorithm that will help to successfully deliver the packets in the presence of black hole attack by using multiple base stations with optimized position using genetic algorithm (GA)[17]. There also a method to detect and prevent black hole attacks by notifying other nodes [7] in the network of the incident. 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 [18][3]. There is also an

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

intrusion detection system for MANET against black hole attack using fuzzy logic and fuzzy rule [4][13][10]. Fuzzy rule based solution identify the infected node as well as provide the solution to reduce data loss over network [19]. Almost all of the EA and SI algorithms perform with heuristic population-based search procedures that incorporate random variation and selection [8]. In a black hole attack, a malicious node answers each route request with a fake reply claiming to have the shortest and freshest route to the destination. However, when the data packets arrive, the malicious node discards them. Several detection methods are described and their strengths and weaknesses discussed. Ad hoc networks are an increasingly promising area of research with lots of practical application [14]. For sensor networks with re-newable energy sources, analysis shows that the maximum sustainable throughput in the network scales much worse than the capacity predicted based on interference among concurrent transmissions, if the growth of the physical network size is not exceedingly slow compared to the growth of **n [1].** For dis we are having a novel cluster based distributed routing algorithm for heterogeneous WSNs [2]. Hierarchical Energy Efficient Reliable Transport Protocol (HEERTP) for the data transmission within the WSN. This protocol maximises the network lifetime by controlling the redundant data transmission with the co-ordination of Base Station (BS) [21]. We analysed impact of changing the initial energy parameter on the proposed multihop routing protocol as well as Assisted LEACH so that its exact effect could be understood and interpreted in terms of performance parameters like throughput, average energy consumption [11][20]. The black hole attack, under the AODV routing protocol and its effect are elaborated by stating how this attack disrupt the performance of MANET. And also studied of the impact of black hole attacks in MANET using both reactive and proactive protocols [12] [22]. Methods of integration of autonomic computing principles into WSNs. PSO based clustering for self-optimization and watch mechanism based method for self-protection from black hole attack has been presented [15]. An energy efficient maximum lifetime routing algorithm. It is based on a greedy heuristic technique to maximize lifetime of the system. For achieving maximum system lifetime proposed algorithm uses the energy cost of links for constructing energy efficient path [6]. Finally we can conclude that data packet delivery in EEMLR routing is more than that using AODV routing.

3. PROPOSED WORK

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. 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. Figure 2 depicts how clockwise and counter clockwise movement of a bacterium take place in a nutrient solution.

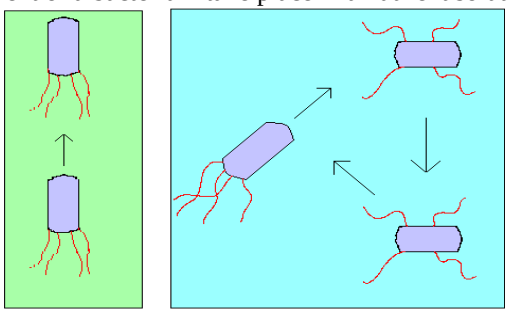

Figure 2: Swim and tumble of a bacterium

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.

The pseudo algorithm is given as:

Parameters:
[Step 1] Initialize parameters p, S, Nc, Ns, Nre, Ned, Ped, C(i)(i=1,2…S),
Algorithm:
[Step 2] Elimination-dispersal loop: l=l+1
[Step 3] Reproduction loop: k=k+1
[Step 4] Chemotaxis loop: j=j+1
[a] For i =1,2…S take a chemotactic step for bacterium i as follows.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

[b] Compute fitness function, J (i, j, k, l).
Let, J (i, j, k, l) = J (i, j, k, l)+ J_{cc} (θ(j, k, l),P(j, k, l)) (i.e. add on the cell-to cell attractant–repellant profile to simulate the swarming behaviour)
[c] Let Jlast=J (i, j, k, l) to save this value since we may find a better cost via a run.
[d] Tumble: generate a random vector D(i)ÎÂp with each element (i),m 1,2,..., p, m D = a random number on [-1, 1].
[e] Move: Let

$$\theta^i(j+1,k,l) = \theta^i(j,k,l) + c(i)\frac{\Delta(i)}{\sqrt{\Delta^t(i)\Delta(i)}}$$

This results in a step of size C(i) in the direction of the tumble for bacterium i.
[f] Compute J (i, j +1, k, l) and let
J (i, j 1, k, l) = J (i, j, k, l) +J_{cc} (θ(j 1, k, l), P(j 1, k, l))
[g] Swim
i) Let m=0 (counter for swim length).
ii) While m< s N (if have not climbed down too long).
• Let m=m+1.
• If J (i, j +1, k, l) <Jlast(if doing better), let Jlast = J (i, j +1, k, l) and let

$$\theta^i(j+1,k,l) = \theta^i(j,k,l) + c(i)\frac{\Delta(i)}{\sqrt{\Delta^t(i)\Delta(i)}}$$

And use this θ(j +1, k, l) to compute the new J (i, j +1, k, l) as we did in [f]
• Else, let m= s N. This is the end of the while statement.
[h] Go to next bacterium (i+1) if i ≠ S (i.e., go to [b] to process the next bacterium).
[Step 5]If c j <N, go to step 3. In this case continue chemotaxis since the life of the bacteria is not over.
[**Step 6**] Reproduction:
[a] For the given k and l, and for each i = 1,2,..., S , let

$$J_{health} = \sum_{j=1}^{N+1} J(i,j,k,l)$$

be the health of the bacterium i (a measure of how many nutrients it got over its lifetime and how successful it was at avoiding noxious substances). Sort bacteria and chemotactic parameters C(i) in order of ascending cost health J (higher cost means lower health).
[b] The r S bacteria with the highest J_{health} values die and the remaining r S bacteria with the best values split (this process is performed by the copies that are made are placed at the same location as their parent).
[**Step 7**] If k <N_{re} , go to step 3. In this case, we have not reached the number of specified reproduction steps, so we start the next generation of the chemotactic loop.
[**Step 8**] Elimination-dispersal: For i = 1,2..., S with probability ed P , eliminate and disperse each bacterium (this keeps the number of bacteria in the population constant). To do this, if a bacterium is eliminated, simply disperse another one to a random location on the optimization domain. If l <N_{ed} , then go to step 2; otherwise end.
Thus search for food of E.Coli can be categorised into four steps: Chemotactic, Swarming, Reproduction and Killing/ Dispersion. Mathematically these can be represented step by step as:
Chemotactic:

$$\theta^i(j+1,k,l) = \theta^i(j,k,l) + c(i)\frac{\Delta(i)}{\sqrt{\Delta^t(i)\Delta(i)}}$$

Where $\theta^i(j,k,l)$represents *i*-th bacterium at *j*th chemotactic, *k*-th reproductive and *l*-th elimination-dispersal step. *C*(*i*) is the size of the step taken in the random direction specified by the tumble (run length unit).
Swarming
J (i, j, k, l) = J (i, j, k, l)+J_{cc}(θ(j, k, l),P(j, k, l)
where*J (i, j, k, l)* is the fitness function.

The matlab code for objective function for our case is shown below:

```
function
fposition=Live_fn(x,nodepos)
x=limitchk(x);
tx=20;
for jj=1:(size(x,1)/2)
    bspos(jj,:)=[x(2*jj-
1),x(2*jj)];
end
     len=size(bspos,1); %  number
of base sattion nodes
    for ii=1:len
        for kk=1:size(nodepos,1)

dis(ii,kk)=sqrt((nodepos(kk,1)-
bspos(ii,1))^2+(nodepos(kk,2)-
bspos(ii,2))^2);
            if dis(ii,kk)>0 &&
dis(ii,kk)<=tx
                dis_L(ii,kk)=1;
            else
                dis_L(ii,kk)=0;
            end
        end
    end
    fposition=sum(sum(dis_L));
end
```

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. The input signals are fuzzified and represented in fuzzy set notations by membership functions. The defined 'if ….. and 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 fuzzy logic controller, the energy consumed and packet loss are defined by linguistic variables such as low, medium and high characterized by memberships. The memberships are

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

curves that define how each point in the input space is mapped to a membership value between 0 and 1. The user interface module of fuzzy logic is shown in Figure 3. The membership functions belonging to the other phases are identical Membership functions for the inputs are shown in Figure 4 and Figure 5. The membership function are of output variable is shown in Figure 6.

The surface viewer of our fuzzy logic is shown in Figure 7. It is a three dimensional representation of mapping of energy consumed, packet loss and output of fuzzy logic. Because this curve represents a two-input one-output case, you can see the entire mapping in one plot. Packet loss is along x axis and energy consumed is drawn along y axis. Z axis represents the trust value. Defining only membership function doesn't complete fuzzy logic designing. Rule sets for taking decision have to be designed also. You see a single figure window with 9 plots nested in it. The three column plots represent energy consumed, packet loss rate and output. Each rule is a row of plots, and each column is a variable. The rule numbers are displayed on the left of each row. You can click on a rule number to view the rule in the status line. The first two columns of plots (the six yellow plots) show the membership functions referenced by the antecedent, or the if-part of each rule. The third column of plots (the three blue plots) shows the membership functions referenced by the consequent, or the then-part of each rule. This decision will depend on the input values for the system. The defuzzified output is displayed as a bold vertical line on this plot. The Rule Viewer allows you to interpret the entire fuzzy inference process at once. The Rule Viewer also shows how the shape of certain membership functions influences the overall result.

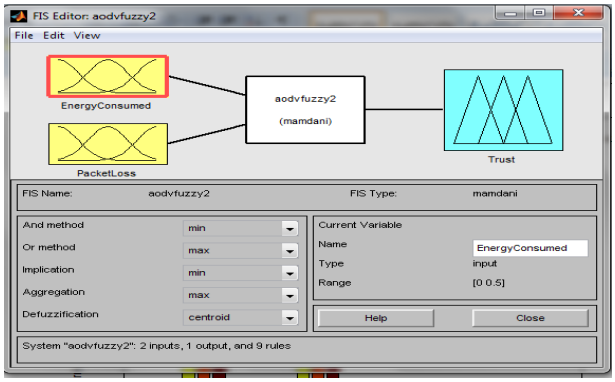

Figure 3: User interface of fuzzy logic in MATLAB

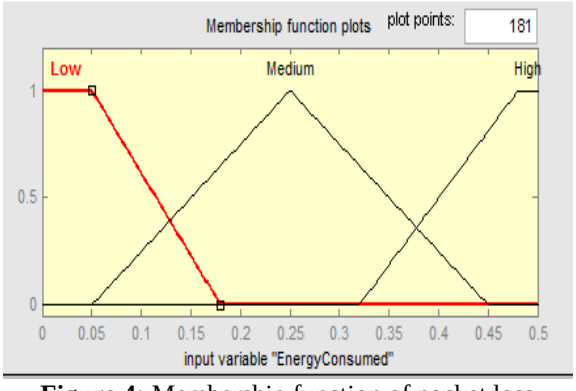

Figure 4: Membership function of packet loss

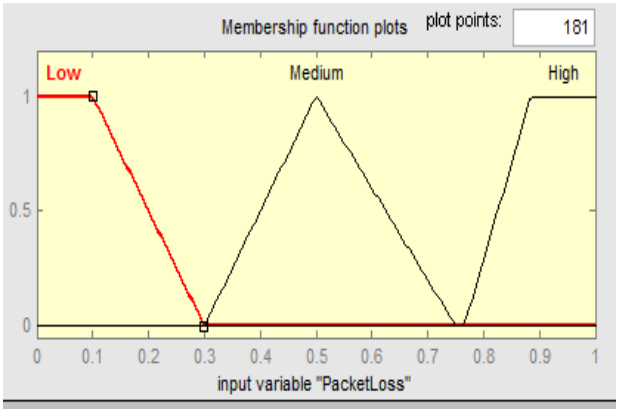

Figure 5: Membership function of energy consumed

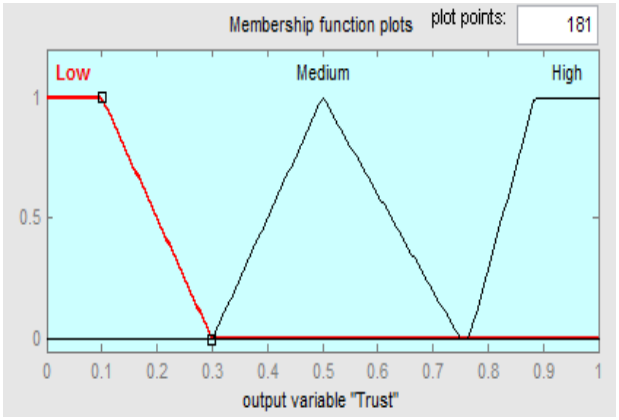

Figure 6: Membership function of output trust value

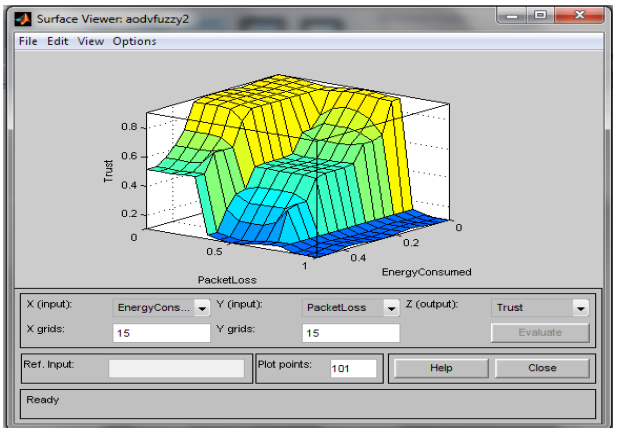

Figure 7: Surface viewer plot of fuzzy logic

4. RESULT AND DISSCUSSION

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. 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 regions. The statistics used for simulation of WSN are used in Table 1 below.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Table 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 8. Route form source node to base station is found out by using AODV protocol which is shown by colored path in Figure 8. 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. 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.

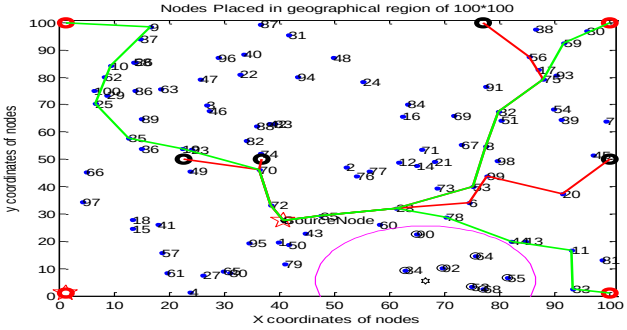

Figure 8: AODV path made form source to base stations

Figure 9 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.

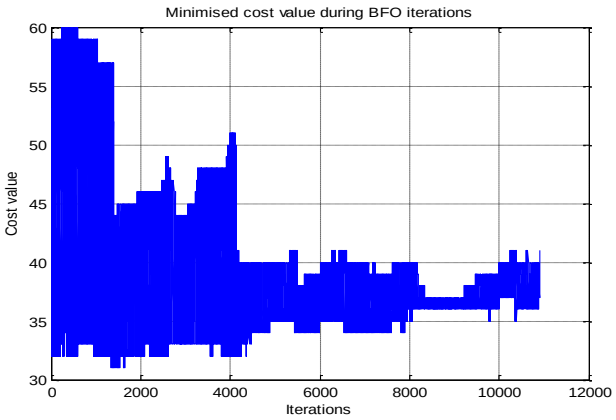

Figure 9: Fitness function plotting of BFO

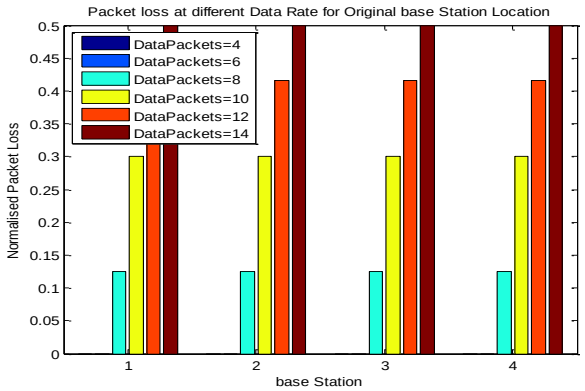

Figure 10: Packet losses for all base stations before optimization

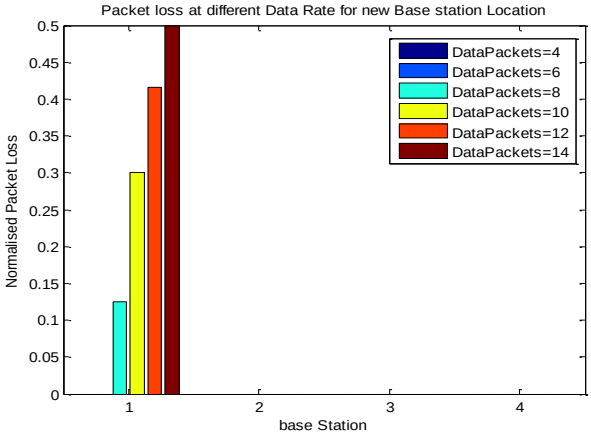

Figure 11: Packet losses for all base stations after optimization

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

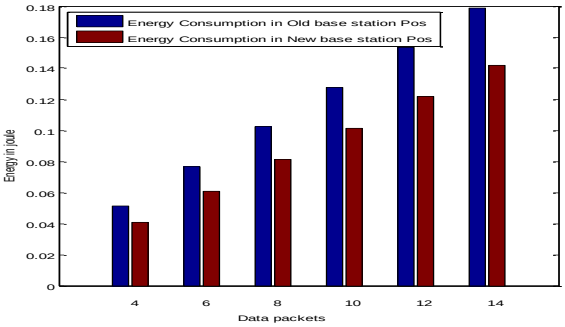

Figure 12: Energy Consumption Bar graph for 20 m black hole radius

5. CONCLUSION AND FUTURE WORK

In this study, we analyzed effect of the Black Hole in an AODV Network. For this purpose, we implemented an AODV protocol that behaves as Black Hole in MATLAB. We simulated four scenarios with different black hole radius and different data rates, where each one has100 nodes that use AODV protocol and also simulated the same scenarios after introducing one Black Hole Node into the network. Moreover, we also implemented a solution that attempted to reduce the Black Hole effects in MATLAB using 4 base stations in the geographical region of 100 nodes and simulated the solution using the same scenarios. Our simulation results are analyzed below: 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. We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used the AODV routing protocol. But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Black Hole attack. They can be categorized on the basis of how much they affect the performance of the network. Black Hole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Black Hole attack as well as the elimination strategy for such behavior has to be carried out for further research.

REFERENCES

[1] ZHIHUA HU, "Fundamental Performance Limits Of Wireless Sensor Networks" IEEE, 2006.

[2] Mahanth K Gowda, "Energy and Throughput Optimized, Cluster Based Hierarchical Routing Algorithm for Heterogeneous Wireless Sensor Networks" Int. J. Communications, Network and System Sciences, 2011, 4, 335-344.

[3] Satyajayant Misra, "Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks"IEEEE, 2011.

[4] Kulbhushan, "Fuzzy Logic based Intrusion Detection System against Blackhole Attack on AODV in MANET" IJCA Special Issue on "Network Security and Cryptography" NSC, 2011.

[5] Marjan Radi, "Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges" Sensors 2012, 12, 650-685.

[6] Sourabh Jain, "ENERGY EFFICIENT MAXIMUM LIFETIME ROUTING FOR WIRELESS SENSOR NETWORK" International Journal Of Advanced Smart Sensor Network Systems, Vol 2, No. 1, January 2012.

[7] Sowmya K.S, "Detection and Prevention of Blackhole Attack in MANET Using ACO" International Journal of Computer Science and Network Security, VOL.12 No.5, May 2012.

[8] 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.

[9] Rudranath Mitra, "Secure and Reliable Data Transmission in Wireless Sensor Network: A Survey"International Journal Of Computational Engineering Research,May-June 2012.

[10] Naveen Kumar, "A Fuzzy Based Approach to Detect Black hole Attack" International Journal of Soft Computing and Engineering ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[11] MEENAKSHI SHARMA, "Transmission Time and Throughput analysis of EEE LEACH, LEACH and Direct Transmission Protocol" Advanced Computing: An International Journal Vol.3, No.5, and September 2012

[12] Savita Shiwani, "Detection of Black Hole Attack In MANET Using FBC Technique" International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 2, March – April 2013

[13] Kiran Narang, "Black Hole Attack Detection using Fuzzy Logic" International Journal of Science and Research, Volume 2 Issue 8, August 2013.

[14] 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.

[15] Rajani Narayan, "Self-optimization and Self-Protection in AODV Based Wireless Sensor Network"International Journal of Computer Science and Mobile Computing, Vol.3 Issue.1, January- 2014, pg. 244-254.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

[16] 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.

[17] Anurag Singh Tomar, "Optimized Positioning Of Multiple Base Station for Black Hole Attack" International Journal of Advanced Research in Computer Engineering & Technology Volume 3 Issue 8, August 2014.

[18] 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.

[19] 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.

[20] 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.

[21] Prabhudutta Mohanty, "A Hierarchical Energy Efficient Reliable Transport Protocol for Wireless Sensor Networks" Ain Shams Engineering Journal, June 2014.

[22] 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.