BFO Based Optimized Positioning For Black Hole Attack Mitigation in WSN

Manvi Arya
Student, BBSBEC, Fatehgarh Sahib
Punjab, India

Er. Jatinder Pal Singh Raina
Asst. Professor, BBSBEC, Fatehgarh Sahib
Punjab, India

***Abstract*—Wireless Sensor networks are always susceptible to attacks by malicious behavior of external adversary which could negatively affect the secured routing and QoS and hence, vital wireless applications. In recent times, a lot of severe attacks have been proposed which make such networks highly vulnerable. One such attack is black hole attack that can be easily employed against routing in sensor networks. In this attack, a set of nodes in the network are being captured and reprogrammed by the external adversary so that these nodes do not transmit the data packets to the destination, which they generate or receive from other sensor nodes. In this paper, we 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. Our simulation results show that our technique can achieve more than 99% packet delivery success using one or two base stations and also, the success rate increases with three or more base stations even if there is increase in the radius of the black hole region. The proposed scheme can be used to identify 100% black hole nodes with almost negligible false positives.**

***Index Terms*—**WSN, black hole attack, multiple base stations, successful data delivery, bacteria foraging optimization, false positives**.**

I. INTRODUCTION

A WSN can be defined as a network consisting of hundreds or thousands of low power, low cost nodes, possibly mobile but more likely to be at fixed locations, deployed to monitor physical and environmental conditions like temperature, pressure, humidity, illumination intensity, pollutants etc. at different locations. WSN is emerging as a prevailing technology in future due to its wide range of applications in military and civilian domains including industrial control process and monitoring, environment and habitat monitoring, healthcare monitoring and so on. These networks are easily prone to security attacks, since once deployed, these networks are unattended and unprotected. Secure routing in sensor networks presents challenges due to several factors like low computing power, small memory, limited bandwidth, low processing capability and above all, very limited energy of SNs

[5]. There are a lot of attacks on these networks which can be classified as routing attacks and data traffic attacks. Some of the data attacks in sensor nodes are wormhole, sinkhole attack, selective forwarding, and black hole attack. A black hole attack is a type of denial of service attack in which a malicious node spuriously announces a short route to the destination to attract the additional traffic towards it and then drops all the data packets received by it.

The techniques proposed in literature for black hole attacks used the concepts of watch dog nodes [6], mobile agent [10], non-dispersive multipath routing [2], [3] and randomized routes [9]. These techniques though better, but are still not very effective.

In WSN, the requirement of successful packet delivery to the BS is more essential than the requirement of prevention of data captured by an adversary. With the use of efficient data algorithms such as AES [16], and data anonymity techniques [17], the information that an adversary derives from the captured packet can be made inconsequential. Consequently, our main objective is to deliver the packet to the BS in the presence of black hole nodes.

Our Contribution: In this paper, we propose a novel solution that uses Bacteria Foraging Optimization (BFO) technique for optimizing the positions of multiple base stations randomly in the entire network to help in improving the likelihood of packets from sensor nodes reaching at least one BS in the network in the presence of large black hole regions, thus ensuring high success rate. We demonstrate by simulation results that our scheme can achieve more than 99% successful packet delivery rate using one or two BSs only inspite of deploying more BSs in the network. But, if more than two BSs are deployed using our approach, then success rate is still more than 99% even if there is the increase in percentage of black hole nodes. This scheme can also be used to identify 100 % black hole nodes. Given that in a WSN, a BS is a laptop class device, so the idea of deploying multiple BSs is inexpensive. So, in case, there is increase in percentage of black hole nodes with an increase in the radius of black hole region then, three or four BSs can be deployed randomly in the network using our technique to help in increasing the success delivery rate. Use of multiple BSs have been proposed in the literature to handle the flow of large amount of heterogeneous data from the network and several optimization techniques have been designed for query allocation and base station placement. Here, use of multiple BSs is proposed for improving data delivery in the presence of black holes.

II. RELATED WORK

Various algorithms have been proposed to solve sinkhole attacks, selective forwarding attacks and black hole attacks in WSN. Here, we note that selective forwarding attack is a

special case of black hole attack only. In selective forwarding attack, malicious nodes behave like black hole and may refuse to forward some messages ensuring that they are not propagated further. In black hole attack, a malicious node simply drops all the packets received by it. The relevant work related to various types of attacks can be studied in the literature [1],[7],[8],[11].

In [10], secure routing algorithm is proposed against black hole attacks using multiple base stations deployed in network by using mobile agents. Routing through multiple base stations algorithm is activated only when there is chance of black hole attack in the network which is detected by mobile agent. If it doubts that a particular node is a black hole node, then only it triggers the routing process algorithm through multiple base stations for time t. If the node is a black hole node, then it revokes that node and triggers routing process algorithm through the nearest base station.

In [3], multiple routes were computed for transmission of shares of different packets using multipath routing algorithms like DSR, AODV. These routes were node-disjoint. But this approach was no longer valid if adversary could compute the set of routes for any given source and destination as the route computation was deterministic in the sense that the same set of routes were always computed by the routing algorithm. Secondly, when the node density was moderate, the scarcity of enough routes significantly undermined the security performance of multipath approach and last, the routes were not spatially dispersive enough to circumvent a moderate size black hole.

In [9], a randomized multipath routing algorithm has been proposed that could overcome the problems in [3]. Multiple paths were computed in a randomized way, each time a packet needed to be sent. So, the routes may no longer be node-disjoint and were as dispersive as possible such that they have the highly likelihood of not simultaneously passing through a black hole. And it was almost difficult for the adversary to jam all the possible routes from source to the destination. But, this technique was only effective if there were a small number of black holes in the WSN. In case, a stronger attack was made by compromising a large number of sensors, then no secret share could escape from being intercepted by the adversary. Under such circumstances, this technique proved to be worse with only one BS when attributed to the capture of atleast N-T+1 shares by the black hole nodes.

In [12], an efficient technique BAMBi was proposed that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission (Fig 1). Here, despite the presence of large black hole regions in the network, more than 99% packet delivery success is achieved with deployment of three or more BSs. At the same time, since the base stations deployed in this scheme were at fixed location, the success rate was only 60% using one BS. With the increase in the radius of black hole region, the success rate decreased. Moreover, this scheme couldn't identify 100% of the black hole nodes. This technique was very effective when compared with MTRP with the use of multiple base stations, the failure percentage using BAMBi is always lower than 7% while in MTRP, the failure percentage could be more than 60% with only one base station. We compare our technique with BAMBi as it is the best in literature.

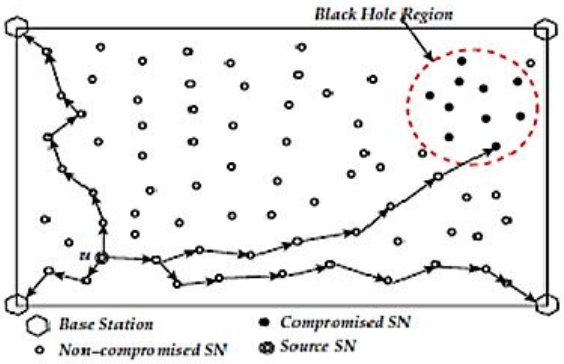


Fig 1: Success rate using fixed Multiple BSs in BAMBi

III. PROPOSED ALGORITHM

In this algorithm, bacteria foraging optimization technique is used to optimize the best locations of the multiple base stations to be deployed randomly in the network using quadrant method.

Here, the SNs used for optimization are considered as bacterial SNs. The basic steps involved in the process are:

a. Population initialization
b. Swimming and Tumbling
c. Selection
d. Elimination

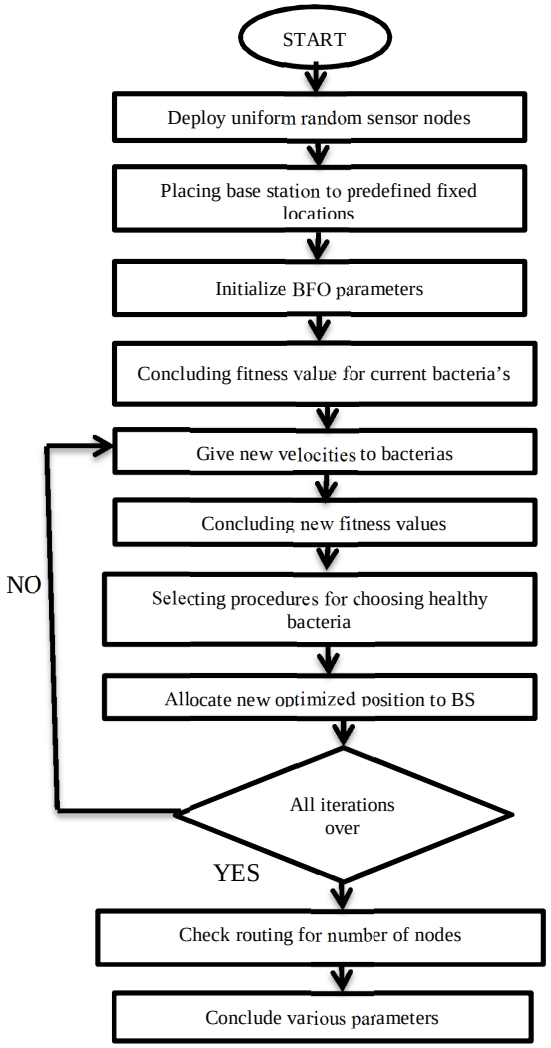
ALGORITHM FOR OPTIMIZATION OF BASE STATION'S LOCATION USING BFO

for i=1 to i=n
F_i=Fitness (B_i)
end for
for i=1 to i=t
for j=1 to j=n
B_{ti}=B_i+R(SS);
if (B_{ti}>S_x & B_{ti}<S_y)
B_{ti}=B_{ti} ;
else
B_{ti}=B_i ;
end if
F_{ti}=Fitness (B_{ti})
end for
for i=1 to i=n
if (F_{ti}>F_i)
B_i=B_{ti};
F_i=F_{ti}
end if
end for
end for
B_o=B_i(max(Fi));

B_o : optimized location of BS
B_i : position for i^{th} bacterial node

B_{ti} : new position for i^{th} bacterial node
n : number of nodes
t : number of iterations
R() : a random function for adding new velocity with Step size (SS) range
S_x, S_y: search limits for location of BS

IV. FLOWCHART



First, for n parent bacterial SNs deployed randomly in network, fitness values (F_i) are computed. Secondly, swimming and tumbling process takes place according to random function R(SS). If the new locations of bacterial SNs are within the limits S_x and S_y, then they are stored in B_{ti}, otherwise the older ones stored in B_i are considered. Now, the fitness values of child bacterial SNs (F_{ti}) are computed. Selection of healthy bacterial SNs is done on the basis of their fitness values. The remaining n nodes again act as parent bacterial SNs. The entire process repeats itself for t iterations as mentioned in the algorithm. After t number of iterations, the bacterial node with highest fitness value is selected as the best position for deployment of the base station.

Note that, if more than one BS is to be deployed, then the network is divided into quadrants. This is one of the many possible ways of placing a set of BSs.

V. MATHEMATICAL EQUATION

In this work, an important term taken into consideration for optimization of BS's location is *FITNESS VALUE*. Fitness value of a SN refers to the density of nodes present in its neighborhood. Fitness value is computed by using the following formula:

$$dis = \sqrt{(X-B_{i1})^2+(Y-B_{i2})^2}$$

if $dis_i > 0$ & $dis_i < tx$; $dis\_L_i = 1$
else ; $dis\_L_i = 0$

$$fitness\_value = \sum_{i=1}^{n} dis\_L_i;$$

X & Y : locations of sensor nodes
B_i : bacterial node's location
dis_i : distance vector of all nodes from current bacterial node location
n : number of nodes
dis_L_i : a logical vector

VI. IDENTIFICATION OF BLACK HOLE NODES

The proposed technique can be used to identify black hole nodes after optimizing the location of BS and then transmitting data packets to that SN in its neighborhood which can actually send the data further to the BS. We make use of control packets including encryption key for this task. First, RREQ is broadcasted in the network. As, black hole nodes use tiny OS beaconing protocol like other normal nodes to form the part of routing tree, they are the first one to send reply without checking their routing table, advertising that they have the shortest route towards the destination. So, in the broadcasting mode, reply comes from both black hole and non-black hole nodes present in its neighborhood. Now, control packets with encryption keys are sent to the preferable nodes. If RRPLY comes from any node, then data packet is transmitted to it. In case, nodes do not respond to source SN, then they can be considered as black hole nodes. It is to be noted that, the data packet is dropped only when there is no non-black hole node available in the neighborhood of the source SN. This procedure is performed in the network at regular intervals of time to identify the presence of a black hole region.

We do not deal with revocation in detail, but revocation of the black hole nodes can be performed by having the BSs broadcast a revocation list. We find that it is easy to prove that this procedure can identify all the black hole nodes in the network. This is because a black hole node does not transmit/forward any packet to the BSs. As a result, no black hole node is going to be a part of the path from any nonblack

hole SN to a BS. This proves that our scheme will be able to identify all the black hole nodes.

VII. PERFORMANCE EVALUATION

For evaluation, we perform simulation of our protocol in a realistic setting. The WSN is deployed in a square field of dimensions 100 × 100 m^2. The SNs are deployed randomly in the network, with the number of SNs being 200.

Table 1: Assumed parameters for simulation

1.	Number of bacterial sensor nodes	10
2.	Number of iterations	1000
3.	Step_Size (SS)	[-1 0 1]
4.	SEARCH LIMITS	
4(a)	One BS	[(0 100) ; (0 100)]
4(b)	Two BSs	[(0 100) ; (0 50) (0 100 ; (50 100)]
4(c)	Three or Four BSs	[(0 50) ; (0 50) (0 50) ; (50 100) (50 100) ; (0 50) (50 100) ; (50 100)]

The transmission range of the SNs was chosen to be 20m. For our simulation, the numbers of BSs deployed in the network were one, two, three, or four, with the positions being selected randomly in the entire network using quadrant method. The following table represents the parameters assumed in optimization process.

To simulate different sizes of black hole (hence number of black hole nodes), we chose 3 different radii for the black hole region, namely 20m, 30m, and 40m. To make the simulation more realistic, we considered two randomly placed black hole regions in the network.

We averaged our results over 100 topologies. For a network topology, we ran our result for two different sets of random placement of the two black hole regions. For each topology, we considered 50 transmitting SNs, chosen randomly from the 200 randomly placed SNs. We compared our work with that of BAMBi proposed in [12]. In BAMBi, the positions of BSs were fixed, being at the four corners of the square field, namely (0, 0), (100, 100), (0, 100), and (100, 0) respectively. Using BFO, positions are randomly selected. Among other analysis, we compared the results on the basis of percentage of packets successfully delivered to the BS(s) and also the percentage of packets captured by the black hole nodes. We also took into consideration other performance aspects for our technique.

VIII. SIMULATION RESULTS

Fig. 3.1 illustrates the super-linear increase in the percentage of black hole nodes with an increase in the radius of the black hole region. When the radius of the black hole region was 20m, the percentage of nodes in black hole region was around 20% of the total nodes, when the radius was 30m it was around 35%, and when the radius was 40m it was around 50%. This implies that a linear increase in the black hole region radius may result in a disproportionate decrease in the probability of successful packet delivery.

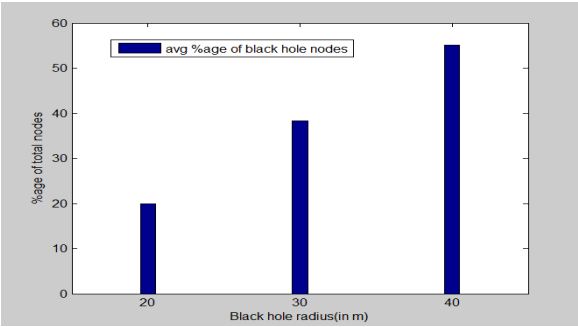


Fig 3.1 Black hole nodes %age in BFO & BAMBi

Fig. 3.2.1 illustrates the percentage of packets successfully delivered in the network for our technique with one or two BSs only and BAMBi, where the same percentage was achieved after deploying three or more BSs (radius of black hole is less), as depicted in Fig. 3.2.2. BAMBi technique performs worse than our technique with one BS. This can be attributed to the capture of data packet by the black hole nodes if they form the part of routing tree. As expected, the success rate falls, in general, with an increase in the radius of the black hole region with one BS. Despite the presence of two large black holes in the network, with one or two BSs, greater than 99% of the data is delivered successfully by our technique. Also, there is high increase in the success rate with the further increase in radius of black hole when compared with previous results.

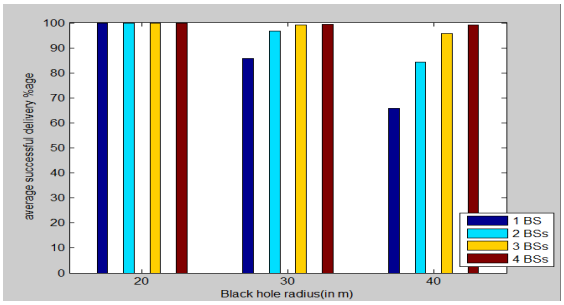


Fig 3.2.1 Packet Delivery Success %age in BFO

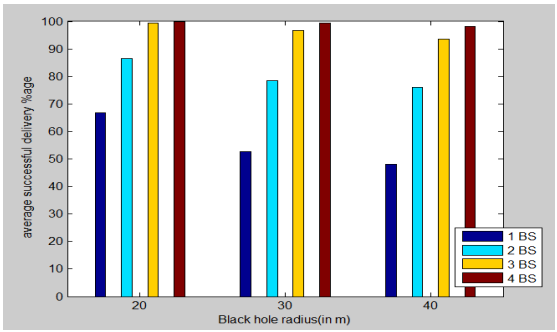


Fig 3.2.2 Packet Delivery Success %age in BAMBi

Fig. 3.3 illustrates the failure percentage of the transmitted packets. As expected, with an increase in the radius of the black hole region, the failure percentage for BAMBi increases with one or two BSs, shown in Fig. 3.3.2. It should be noted that the failure in BAMBi implies that the BS is unable to receive the packets from sensor nodes due to disruption by the black hole nodes in their path. And in our technique, if there is no non-black hole node in the neighbourhood of communicating SN, we count it as a failure. With one BS, the failure percentage is less than 5% using our technique (Fig. 3.3.1), whereas, with BAMBi, the failure percentage could be more than 30%. Using two BSs, failure rate is lower than 2% in our approach, while in BAMBi, it could be less than 15%.

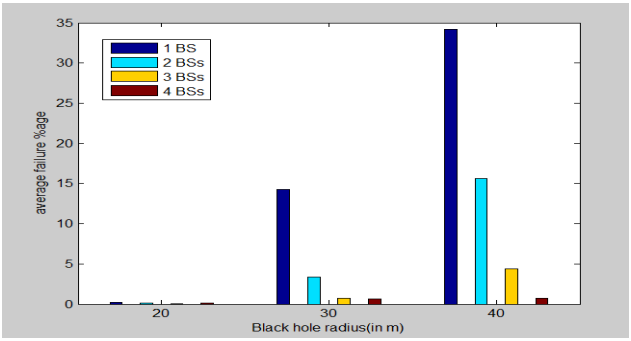


Fig 3.3.1 Packet Delivery Failure %age in BFO

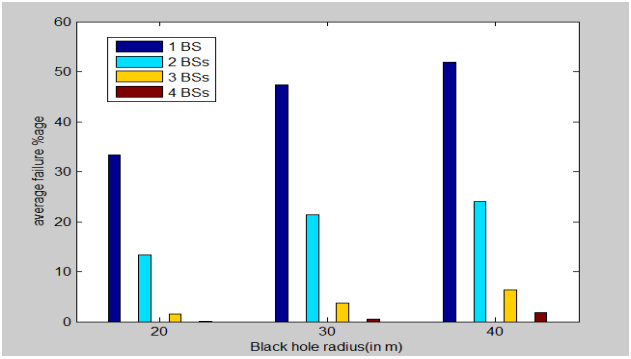


Fig 3.3.2 Packet Delivery Failure %age in BAMBi

Results show that BFO can be used to identify 100 % black hole nodes in the network without fail. This is expected as per the discussion in Section VI. An important aspect of the study is related to the percentage of false positives. Fig. 3.4.1 illustrates the false positives in our technique. In BAMBI (Fig. 3.4.2), with one BS the false positive values are high, because a large number of non-black hole nodes that are unable to reach the BS, due to disruption by the black hole nodes, are in turn identified as black hole nodes. The false positive value reduces with two or more BSs. In our technique, the false positive percentage is nearly negligible. The results demonstrate the effectiveness of our technique in both delivering data to the BSs with high probability as well identifying all the black hole nodes with negligible false positives.

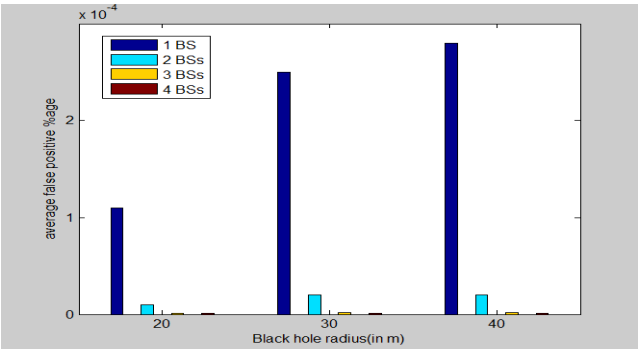


Fig 3.4.1 False Positives %age in BFO

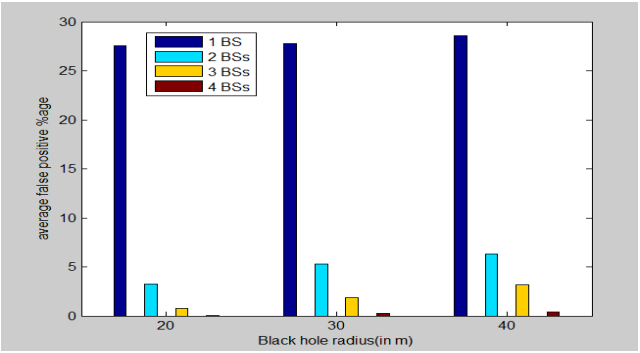


Fig 3.4.2 False Positives %age in BAMBi

IX. CONCLUSION AND FUTURE WORK

In this paper, we propose BFO technique, used to optimize the locations of multiple BSs and thus, help in increasing the success delivery rate. Results showed that our technique is highly effective in reducing the effect of black hole nodes on the successful delivery rate of data packets and, thus decreasing the failure percentage to a large extent. In future, one may use optimization for all the base stations at a time using some optimized technique like Ant Colony optimization (ACO), BAT colony optimization or Particle Swarm optimization (PSO). We are optimizing the BS one by one and using quadrant method. One may use to find all the base station's optimized locations within the full area.

X. REFERENCES

[1] I. Khalil, S. Bagchi, and C. Nina-Rotaru. DICAS: Detection, diagnosis and isolation of control attacks in sensor networks. In *Proceedings of IEEE SECURECOMM*, pages 89–100, 2005

[2] Z. Karakehayov. Using REWARD to detect team black-hole attacks in wireless sensor networks. In *ACM Workshop on Real- World Wireless Sensor Networks*, 2005.

[3] 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.

[4] I. Khalil, S. Bagchi, and C. Nina-Rotaru. DICAS: Detection, Diagnosis and isolation of control attacks in sensor networks. In *Proceedings of IEEE SECURECOMM*, pages 89–100, 2005.

[5] M. Tubaishat, J. Yin, B.Panja, and S. Madria, A Secure Hierarchical Model for Sensor Network, ACM SIGMOD Record, Vol. 33. No. 1, March 2004

[6] Mukesh Tiwari, Karm Veer Arya, Rahul Chaudhari, Kumar Sidharth Chhoudhary. *Designing Intrusion Detection to detect Black hole and selective forwarding attack in WSN based on local information, 2009.*

[7] H. Al Nahas, J. Deogun, and E. Manley. Proactive mitigation of impact of wormholes and sinkholes on routing security in Energy-efficient wireless sensor networks. *Wireless Networks*, 15(4):431–441, 2009.

[8] E. Ngai, J. Liu, and M. Lyu. An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks. *Computer Communications*, pages 2353–2364, 2007.

[9] T. Shu, S. Liu, and M. Krunz. Secure data collection in wireless sensor networks using randomized dispersive routes. In *IEEE INFOCOM*, pages 2846–2850, 2009.

[10] Sheela.D, Srividhya. V.R, Asma Begam, Anjali and Chidanand , G.M. *Detecting black hole attack in WSN using Mobile Agent.*

[11] B. Xiao, B. Yu, and C. Gao. CHEMAS: Identify suspect nodes in selective forwarding attacks. *Journal of Parallel and Distributed Computing*, pages 1218–1230, 2007.

[12] Satyajayant Misra, Kabi Bhattarai, and Guoliang Xue. BAMBi: Blackhole Attack Mitigation with Multiple Base Stations in Wireless Sensor Networks, 2011 IEEE.

[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), September 2003.

[14] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cyirci. Wireless sensor networks: A survey. *Computer Networks*, 38(4):393 – 422, 2002.

[15] Satish Salem Ramaswami and Shambhu Upadhyaya "*Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing*" 2006 IEEE.

[16] S. Didla, A. Ault, and S. Bagchi. Optimizing AES for Embedded devices and wireless sensor networks. In *Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities (Trident)*, pages 1–10, 2008.

[17] S. Misra and G. Xue. Efficient anonymity schemes for clustered wireless sensor networks. *Intl. Journal of Sensor Networks*, 1(1):50–63, 2006.

[18] N.Bhalaji, Dr. A. Shanmugam "*Association between nodes to combat blackhole attack in DSR based* MANET,2009,IEEE.