Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Implementation of Black Hole Attack Detection and Mitigation in MANET Using Advance BFO Algorithm

Ashwini Hosgouda[*]
Dept. of ISE, NHCE,
Bangalore, India

M S Shobha, Asst. Prof.
Dept. of ISE, NHCE,
Bangalore, India

Akshay S Aspalli, Asst. Prof.
Dept. of EEE, DBIT,
Bangalore, India

Abstract— ***A MANET (mobile ad hoc network) is an infrastructure-less network of mobile devices, which are decentralised and are composed of continuously self-configuring nodes. Due to the various flexibility provided by MANET they are prone to attacks. One of the major attacks is the Black hole attack. In this the attacker node does not forward packets to the destination which leads to loss of packet delivery. In this paper we provide an efficient method which uses advance BFO algorithm to increase the success packet delivery ratio even in the presence of black hole reason. For the implementation of black hole attack detection and mitigation we use java netbeans IDE and performance is evaluated.***

Keywords—MANET, Black Hole Attack, BFO

I. INTRODUCTION

Wireless ad hoc networks are group of autonomous nodes that can be self managed with no infrastructure. MANET's are spontaneous and dynamic in nature so any node can join or leave the network at any given time. Due to this they are widely used in military and rescue areas where communication among soldiers in battlefield and in areas where new temporary network is required because the network might be collapsed due to some disaster. Ad hoc networks are temporary networks which are established in place where no fixed infrastructure is required.

Apart from nodes acting as host they also act as router in discovering nodes and forwarding packets to the correct node in the network. As wireless ad hoc networks have no fixed infrastructure they are more open to attacks. One of the major attacks is the black hole attack. In which the malicious node absorbs all the packets in it like a hole which sucks in everything, hence it is named as black hole attack.

A. Overview of Black hole attack in MANET

A black hole attack is a kind of denial of service attack in which a malicious node absorb all packets in itself by falsely claiming a fresh route to the destination and drop them without forwarding them to the destination. In this kind of attack the faulty node advertise itself for having a fresh route and shortest path to the destination without even checking its routing table information.

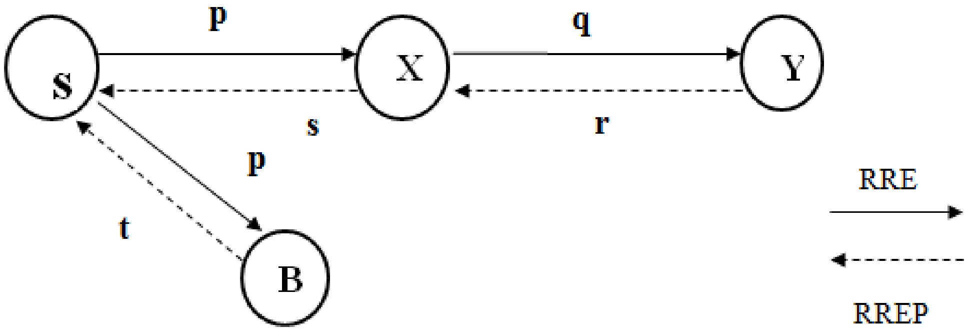


Figure 1: Black Hole Attack

In the above figure 1.1, S is the source node which wants to send packets to Y the destination node. Every node has two types of packets to be sent to the destination, one is routing packet and other is data packet. When node S wants to send data packets to node Y it sends the route packets also called as (RREQ) route request packet to its neighbouring nodes.

Let us assume that nose B is faulty node, after getting the RREQ packet from S it immediately reply back stating that it has fresh path to the destination without even checking its routing table. Once node S has got the (RREP) route reply packet from B it sends all data packets to B thinking it has the shortest and fresh path to the destination. But node B does not forward packets to the destination instead drops all packets. Node B reply back with minimal hope count value and highest destination sequence number so source node S sends all its packets to the malicious node B. With this attack all the data packets are falsely taken from the source node and are dropped without sending to the destination.

II. PROPOSED METHOD FOR DETECTION AND MITIGATION OF BLACK HOLE ATTACK

We propose a new method for the mitigation and detection of black hole attack in which sink placement places an important role. In a wireless ad hoc network black hole attack is one of the major attack that is to be detected and removed. We use BFO (Bacteria Foraging Optimization) sink placement algorithm for the placement of the base stations randomly in the entire network. The below figure 2 shows the system architecture in which the node transfers packets to its nearest base station, whose position is given by the BFO algorithm. Black hole attacker node drops all the packets coming to it. The base station after being placed in the correct position it detects the black hole and sends its report.

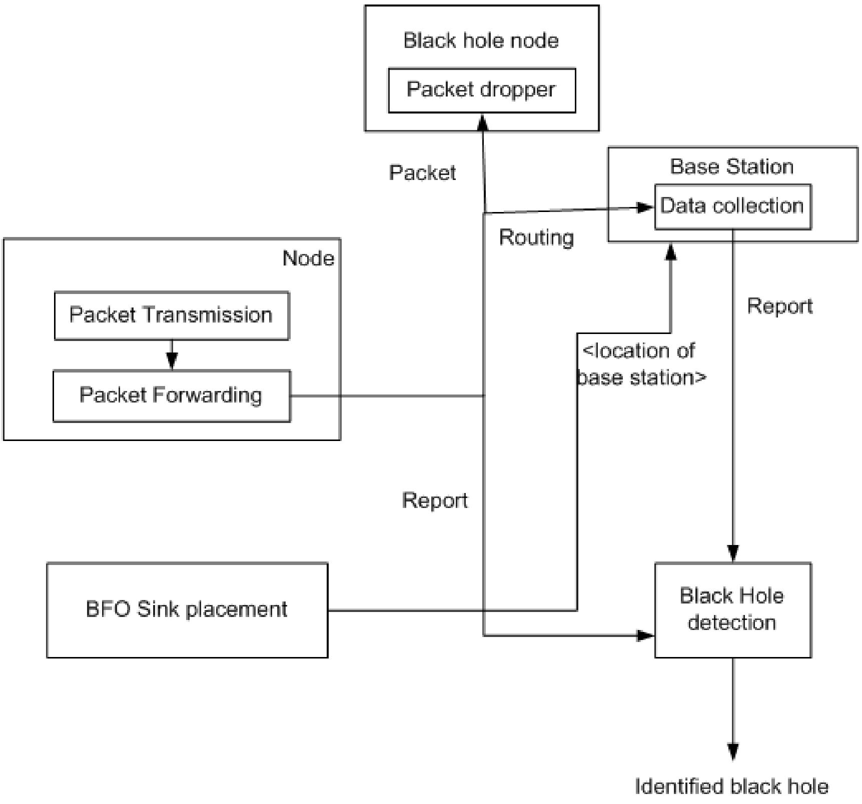


Figure 2: Black Hole Attack Detection and Sink Placement Architecture

Advance BFO (Bacteria Foraging Optimization) Algorithm is used for the mitigation of black hole attack in MANET. Here our main aim is for delivery of packets from the source node to at least one base station in the presence of black hole. In this method we optimize the position of four base stations randomly in the network at the same time. After little iteration the base stations are placed at the most fittest position among all. The fitness value is calculated by the density of nodes around the base station. Once the base stations are placed according to their fitness value the source node sends packets, the packet is transferred to the nearest base station. If a black hole or a black hole region is present in between the source node and the base station, we can change the position of the base station itself and move to a new location based on their fitness value. So that the packets are delivered to at least one base station in presence of black hole attack.

Figure 3 shows the packet delivery from source to nearest sink, after the sinks are optimized at the same time. Here no black hole attack is present in the network.

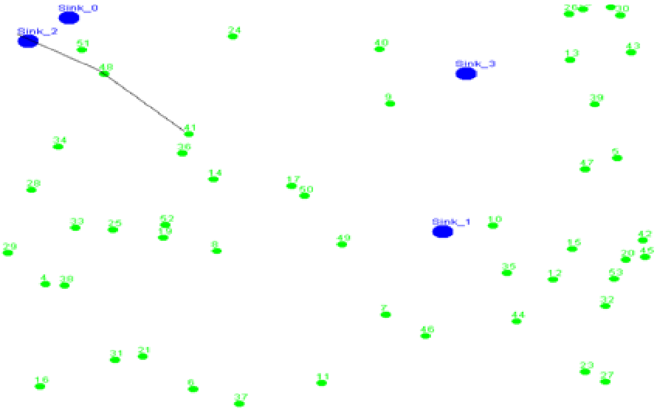


Figure 3: packet delivery from source to sink without black hole attack

In Figure 4 it shows what happens if black holes are present in between the source and the sink node, the affected node just drops all the packets coming to it as shown in the figure.

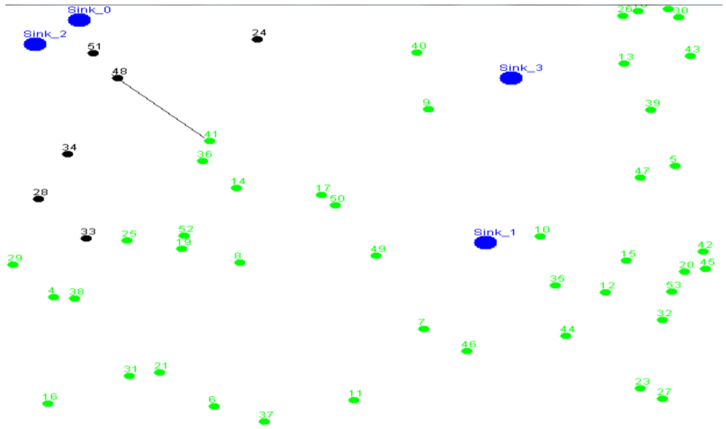


Figure 4: black hole attack

So to reduce the mitigation created by black hole nodes, we optimize the position of sink once again. As shown in the figure 5, sinks are moved to another position by calculating the fitness value. Once the sinks are moved to new location, the source node can send packets again with new route to its nearest sink as shown in the figure.

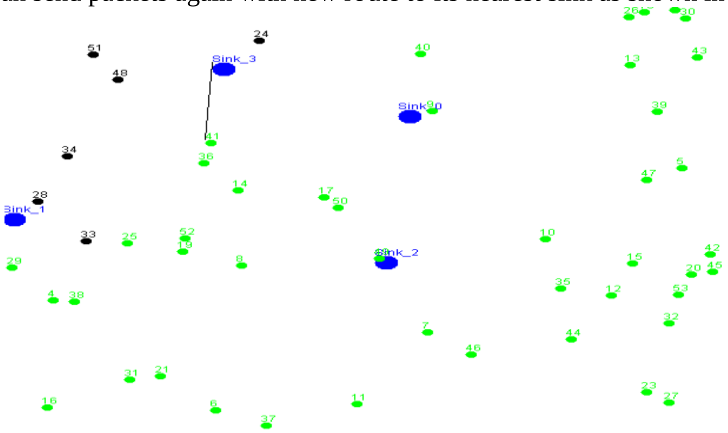


Figure 5: successful delivery of packets in presence of black hole attack by applying BFO sink placement algorithm.

III. EVALUATION

For evaluation, we perform simulation in java Net Beans IDE 7.0.1. Wireless sensor network is created in a square field with sensor nodes deployed randomly in the entire network.

Table 1: parameters for the simulation

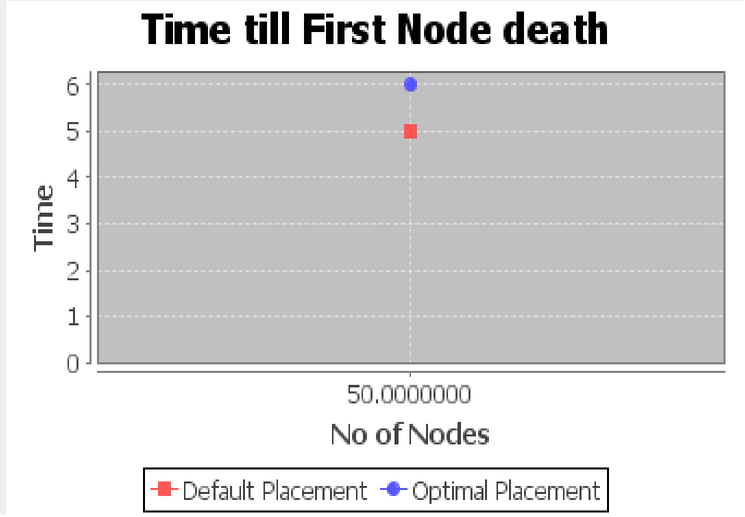
Number of sensor nodes	50
Number of sink node	4
Communication range	150

During simulation, 50 sensor nodes are deployed in the network with communication range between the nodes as 150.four sink nodes are optimized at the same time and located using their fitness value. We have compared our work with that of the existing system where the sink nodes are placed at fixed positions, we are comparing by four parameters like time till first node death, time till last node death, energy consumption and packet delivery ratio.

The detection of black hole attack is done by the checking the routing table by base stations. If black hole nodes are present in the path from source node to its nearest base station, it is identified as black hole node and a revocation list is sent to all the nodes.

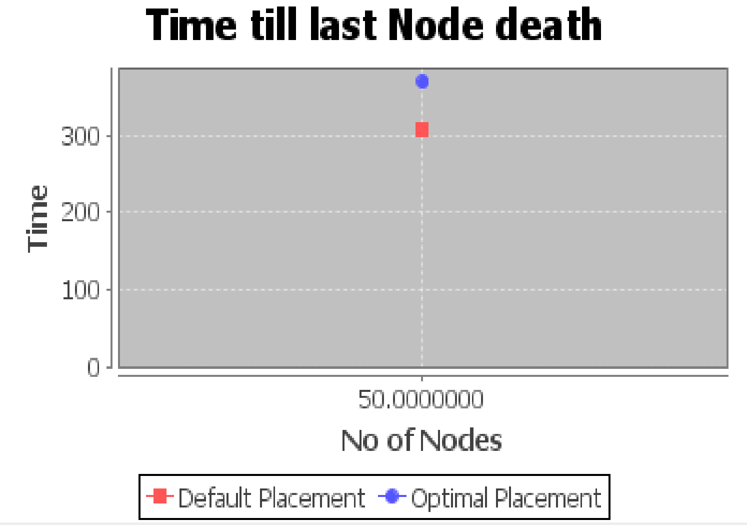
IV. SIMULATION RESULT

Simulation is carried out taking four parameters into consideration. In graph 1 Time till first node death is the time taken for the first node to die in the network of 50 nodes. It shows the life time of the network. Were x-axis indicates number of nodes and y-axis indicates the time .For the default sink placement method time taken was 5 and for our optimal placement method time taken is increased to 6.



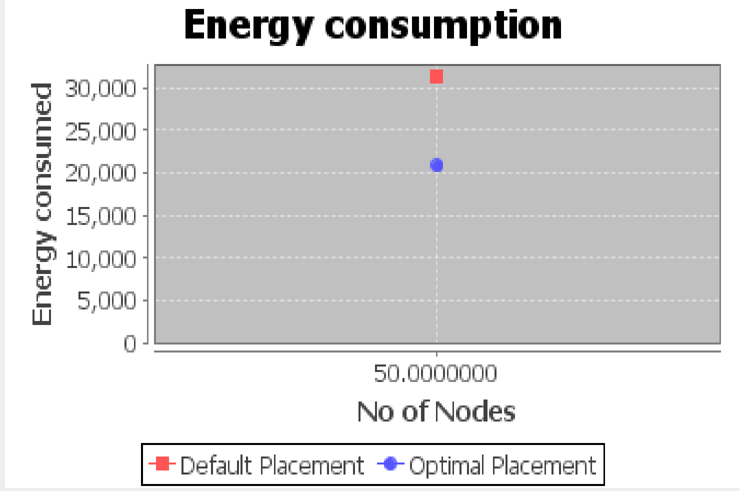
Graph 1: time till first node death

In graph 2 time till last node death shows the time taken for the last node to die in the network of 50 nodes. It shows the life time of the network. Were x-axis indicates number of nodes and y-axis indicates the time. For the default sink placement method time taken was 300 and for our optimal placement method time taken is increased to 400.



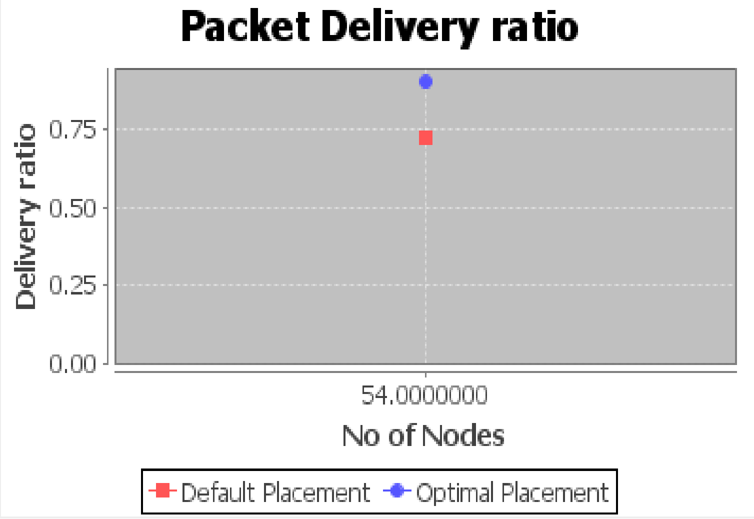
Graph 2: time till last node death

Third parameter is the energy consumption as shown in graph 3. It shows the amount of energy consumed by the nodes in the network. Were x-axis indicates number of nodes and y-axis indicates energy consumed. For the default sink placement method energy consumed was 30,000 and for our optimal placement method energy consumed was decreased to 20,000.



Graph 3: energy consumption

Last parameter is the packet delivery ratio as shown in graph 4. Packet delivery ratio is the ratio of number of packets delivered by number of packets sent. Were x-axis indicates number of nodes and y-axis indicates percentage of packet of delivery. For the default sink placement method the packet delivery ratio was 75% and in our optimal placement method packet delivery ratio was increased to 95%.



Graph 4: packet delivery ratio

V. Conclusion and Future Work

In this paper, we propose advance BFO (Bacteria foraging Optimization) technique, used to optimize multiple base stations at the same time in order to increase the percentage of packet delivery even in the presence of black hole attack. It also detects black hole attacker and send a revocation list as acknowledgment. Results showed that our method is effective in reducing the energy consumption, increase packet delivery and increasing the life time of the network. In future, one can work on improving black hole attack detection method and increase the percentage of detection.

ACKNOWLEDGEMENT

I express my gratitude to **Ms M.S.Shoba,** Assistant Professor, Dept. of ISE, New Horizon College of Engineering, Bangalore for constantly guiding the development of the project. I also thank **Mr Akshay S Aspalli**, Assistant Professor, Dept. Of EEE, Don Bosco Institute of Technology, Bangalore for his valuable suggestions which were the motivating factors in completing the work.

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 R EWARD 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 cont rol 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 routi ng 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.