International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

# A Framework to Detect Black Hole Attack in WSN Using Multi Base Stations Based Mechanism

**Dr. Ajay Jangra, Rajesh Choudhary**
Department of Computer Science & Engineering, University Institute of Engineering & Technology, Kurukshetra University, Kurukshetra, Haryana, India

## ABSTRACT

WSN (Wireless Sensor Network) is wireless network in which nodes can transmit messages between them through base station. A base station is a node that provides connectivity between other odes or it can be a centralized node. When a balckhole node performs attack on base station node then it destroy whole network and to avoid this kind of problem is a difficult problem. The detection of black hole attack and prevention of network from black hole is a critical problem. In this paper a multi base station based mechanism to detect black hole attack in WSN is proposed. In proposed mechanism check agents will used to detect black hole attack. The proposed mechanism is implemented in netbeans and analyzed using delivery probability performance metric.

**Keywords :** WSN(Wireless Sensor Network), Base station, check agent, black hole, Malicious Node and Netbeans

## I. INTRODUCTION

WSN is a fast emerging technology in the today's world which has applications in many fields. As WSN is a wireless technology and worked in an infrastructure-less environment. Hence, these networks can be easily prone to several types of attacks. Black-hole attack is one of the major attacks among them and is an active attack. In this attack, an attacker can re-programmed the sensor nodes so that they behave as normal nodes but disrupts the normal functioning of these networks. These nodes are black-hole nodes and the region affected by these nodes is called as the black-hole region. So, when the source node starts the route discovery process to find the shortest route to the destination node. At that time, these black-hole nodes advertise a wrong path as the shortest path including itself to the destination node. So when the source node uses this path to send data to the destination node, the black-hole node starts dropping the packets in all or by selecting some important packets. Although some authors proposed different solutions to detect black hole attack in WSN and prevent network from this attack.

Alattas[14] proposed a mechanism to detect black hole nodes in WSN using multiple base stations. In this mechanism, whenever a base station is destroyed by black hole node then next base station was worked as current base station but drawbacks was that the author didn't provide any attribute or parameter on the basis of black hole nodes are detected also how a new base station is selected as current base station was not described in this paper. The energy consumption of this mechanism was high and detection rate was low so to solve these kinds of issues in this thesis, propose a framework to successful data transmission in the presence of black hole attack in network.

## II. PROPOSED FRAMEWORK

The objective here is to proposed a technique to detect the black-hole attack using multiple base-stations and a check agent based technology. The proposed technique is more efficient than the previous techniques and gives better results. This technique is energy efficient, fast, lightweight and also reduces message complexity.

Check agent is a software program which is self-controlling and it moves from node to node and checks the presence of black-hole nodes in the network.

CSEIT172578 | Received : 01 Oct 2017 | Accepted : 13 Oct 2017 | September-October-2017 [(2)5: 716-720]

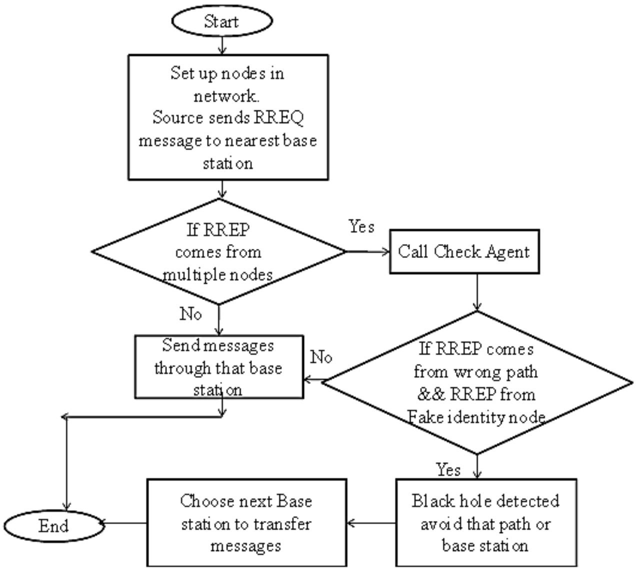

Start
Set up nodes in network. Source sends RREQ message to nearest base station
If RREP comes from multiple nodes
Yes
Call Check Agent
No
Send messages through that base station
No
If RREP comes from wrong path && RREP from Fake identity node
Yes
Black hole detected avoid that path or base station
Choose next Base station to transfer messages
End

**Figure 1.** Proposed Framework

### Description of proposed framework

The proposed work describes the mechanism to detect blackhole attack from WSN.In this work the main focus should be given on the successful delivery of the packets to the base station to improve the delivery of the packets from the sender nodes nearby at least one base station in the network. In this mechanism, initially generate nodes in the network after that sender nodes and receiver nodes are selected among these nodes.
Now sender node chooses shortest path from various number of available paths towards destination. After that check agent is applied on all the nodes considered in selected paths. The purpose of check agent is to check each nodes separately and if it detects black node then it display a triggered message that blackhole is encountered and ignore this path. For effective solution, if a base station is destroyed by blackhole node then select next base station from multiple base stations to improve the delivery of the packet from the sender nodes reaching at least one base station in the network. If blackhole is encountered then it is necessary for sender node to rescan the path and avoid that particular node to get better throughput and less packet droop-rate in network. The proposed mechanism is helpful to avoid blackhole attack in WSN.

## III. RESULTS

### A. Metrics used

- **Total number of packets dropped:** It show total number of packets drops in the network during data transmission in between nodes.
- **Total number of packet delivered:** It show total number of packets delivers in the network during data transmission in between nodes.
- **Delivery probability:**It show delivery probability of total number of packets delivers in respective of total number of packets created in the network during data transmission between nodes.

**Table 1.** Parameters Used

| | |
|---|---|
| Network scale | 200 X200 |
| No. of nodes | 100;150;200;250 |
| No. of base stations | 6 |
| No. of check agent | 1 |
| Operating System | Windows 8 |

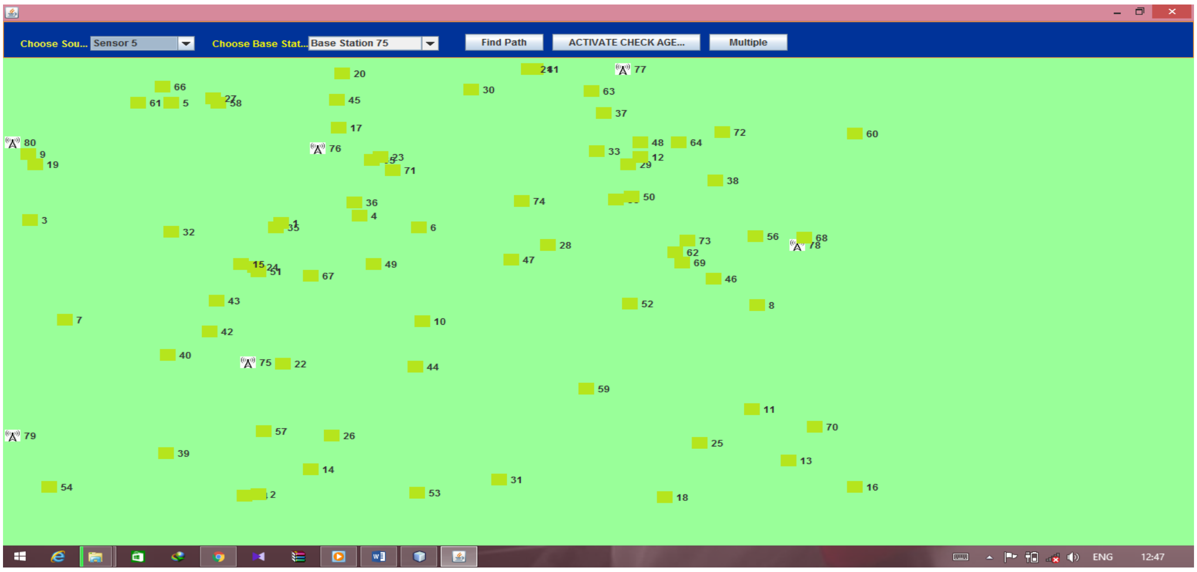
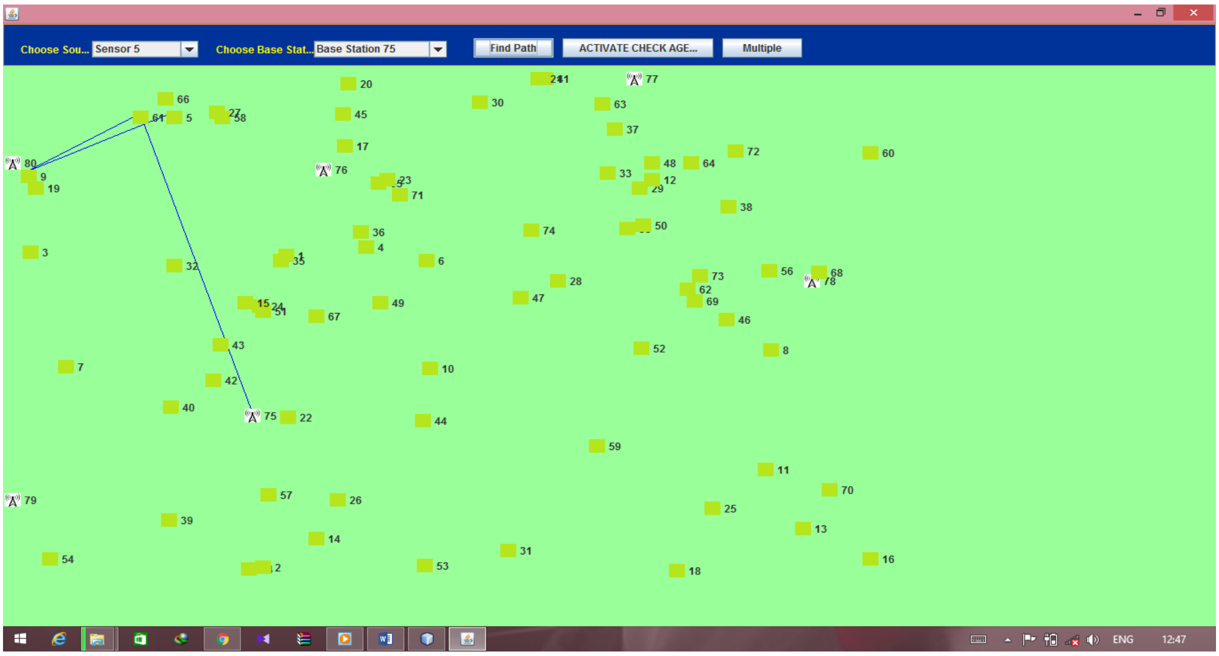


**Figure 2.** Deployment of nodes

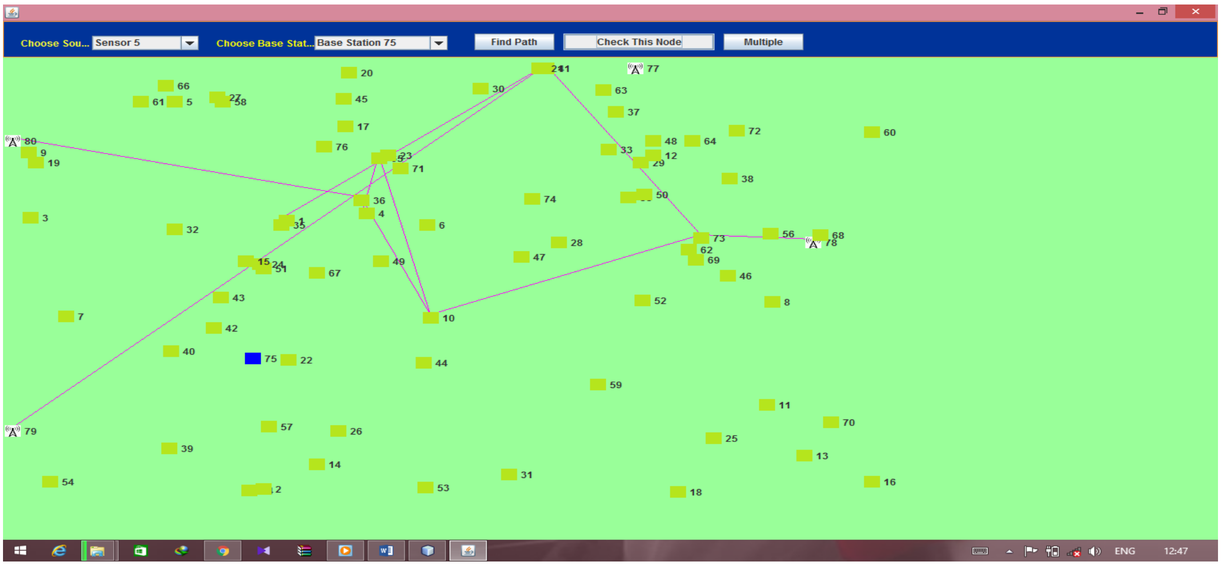
Figure 2 shows deployment of nodes in network. Sender and receiver nodes are chosen from these nodes.


Choose Sou... Sensor 5

Choose Base Stat... Base Station 75

**Figure 3.** path between nodes

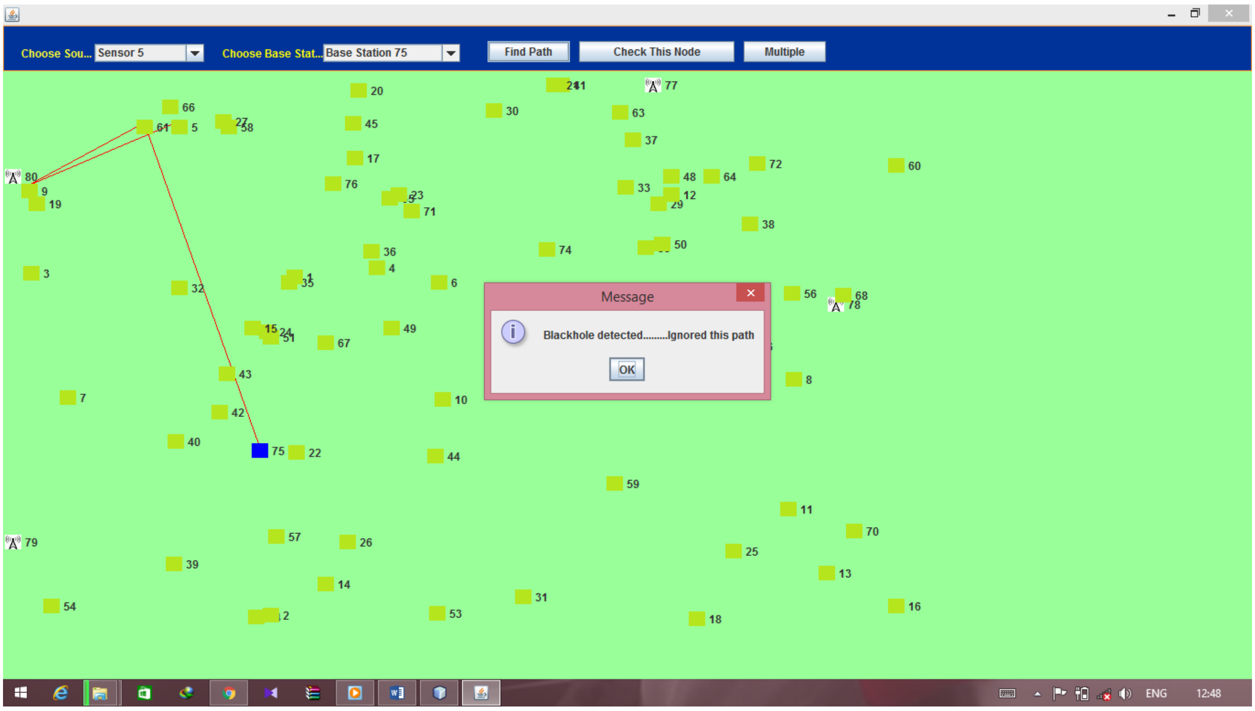
Figure 3 shows shortest path between nodes in network.


Choose Sou... Sensor 5

Choose Base Stat... Base Station 75

**Figure 4.** check agent activation

Figure 4 shows check agent activation activity for detecting the blackhole nodes from network.



Blackhole detected........Ignored this path

**Figure 5.** blackhole detection

Figure 5 shows detecting blackhole node after check agent activation and display message that blackhole is detected.

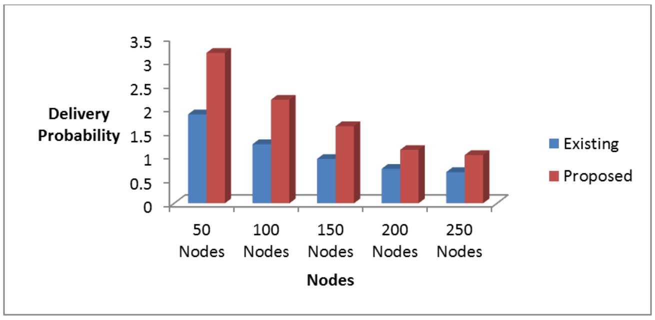


**Figure 6.** Nodes v/s delivery probability

Figure 6 shows bar graph of delivery probability of existing technique and proposed technique. In proposed technique delivery probability is high as compared to existing technique.

## IV. CONCLUSION AND FUTURE SCOPE

In this paper multi base station based mechanism is proposed that uses multiple base stations that concept improves delivery ration and network performance. In proposed mechanism if one base station is destroyed by black hole attack then another base station can be worked as previous base station. The proposed framework is implemented using netbeans and analyzed with performance parameter delivery probability. In proposed work delivery probability is high as compare to existing technique. This technique can be used in the real world application to handle such types of attacks in the sensor networks and thus proves more advancement in this field of sensors. The work can be done further to handle the message complexity and to use less number of base stations in the network for better delivery results in the wireless sensor networks.

## V. REFERENCES

[1]. Ajay Jangra & Rajesh Verma, "Analyzing Wlans Standards For Wireless Sensor Network", International Journal of Information Technology and Knowledge Management January-June 2011, Volume 4, No. 1, pp. 301-304.

[2]. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol. 38, pp: 393-422, 2002.

[3]. K. Sharma and M. K. Ghose; Wireless Sensor Networks, "An Overview on its Security Threats" IJCA Special Issue on Mobile Ad-hoc Networks, Vol.1, pp: 42-45, 2010.

[4]. Z. I. Khan and M. M. Afzal, "Security in Wireless Sensor Networks : DoS Perspective,"

International Journal of Engineering Research & Technology (IJERT) Vol. 6, pp. 311–316, 2017.

[5]. Ajay Jangra, Nitin Goel, Priyanka, Komal, "Security Aspects in Mobile Ad Hoc Network (MANETs): A Picture", International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196.

[6]. Ajay Jangra1,*, Priyanks2, Richa, "Cb-SDA: Cluster-based Secure Data Aggregation for Private Data in WSN", Wireless and Mobile Technologies, 2013, Vol. 1, No. 1, 37-41

[7]. Ajay Jangra, Richa, Swati, Rajesh Verma, "Vulnerability and security analysis of wireless sensor networks" Indian Journal of Applied Research and Engineering, 4 January, 2011.

[8]. D. Sheela, V. R. Srividhya, A. Begam, and G. M. Chidanand, "Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent," Volume 9, Issue 44, November 2016