ISSN: 2321-7782 (Online)

Volume 2, Issue 9, September 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

BHDP Using Fuzzy Logic Algorithm for Wireless Sensor Network under Black Hole Attack

Jaspreet Kaur[1]
Research Scholar
Department of Computer Science & Engineering
SUSCET, Tangori
Mohali, Punjab – India

Bhupinder Kaur[2]
Assistant Professor
Department of Computer Science & Engineering
SUSCET, Tangori
Mohali, Punjab – India

Abstract: Wireless sensor networks are popular to today, the security in wireless sensor networks (WSNs) is a main issue due to the naturally limitations of computational capacity and power usage. The Black Hole attack is one of the main attacks that challenge the security of WSN. Any information that enters to the black hole region is captured and re-programs a set of nodes in the network to block the packets instead of forwarding them towards the base station due to this attack the performance of network is affected. The proposed BHDP (Black Hole Detection And Prevention) using fuzzy logic algorithm successful helps to detecting and prevent the black hole attack in WSN However, this techniques is very effective and efficient when used with multiple base stations to deployed the impact of black holes on data transmission in WSNs. The BHDP algorithm is more secure, reliable to improve the security in defense sector and civilian domains. In this paper the solution of black hole attack which is based on fuzzy rule. The fuzzy rule based solution identifies the infected node as well as provide the solution to reduce data loss over the wireless sensor networks.

Keywords: Black Hole, WSNs, BHDP (Black Hole Detection and Prevention) using fuzzy logic algorithm, multiple Base station, Fuzzy rules.

I. INTRODUCTION

A Wireless Sensor Network is a self-configuring network. It is popular in, science, civil infrastructure, military and home Commercial applications. The security is the main issue in WSN due to the limitation of the computational capacity and power usage. Wireless sensor network has much stronger and effective methods of Security to control the attacks caused by the malicious nodes in the network. From Previous research on wireless sensor network shows that they are more vulnerable to attacks than static networks. Therefore, any security solutions that are applicable for static routing network but don't work well on wireless sensor network. Some of the attacks caused by the malicious nodes are Black hole attack, wormhole attack, hello flood attack, gray hole attack, denial of service, Sybil Attack and Selective Forwarding attack and many more attacks.

In this paper, we focus on the detection and prevention of black hole attack by using multiple base stations. A black hole attack is an active attack in which a compromised node consumes all the data from the network. In black hole attack, an intruder captures and re-programs a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station due to attack the more usage of battery consumption and slow the speed of the networks. [3]

The proposed algorithm is used for detecting and preventing the black hole attack by using fuzzy rules. It makes the network more secure for communication. The result shows that our proposed algorithm works better. It also evaluate, the effect of attack on the following parameters *i.e* Total packet Drop, Packet Delivery ratio, actual packet loss, routing over head and Theoretical packet loss. The analysis shows that our BHDP algorithm is much more effective than other thus it makes the network security stronger and finds the attacks.

The rest of the paper is organized as follows. Section II gives the related work that has been carried out in the area of black hole attack. Section III explains the working of black hole attack Section IV carry multiple base stations Section V about the proposed approach in detail. Section VI provides the experimental and results. Section VII, VIII concludes the paper with a brief overview of their future work

II. Related Work

There are number of mechanism are proposed for detection and prevention of black hole attack. Some of them are explain below briefly:

Virmani et al. (2014) proposed an exponential trust based mechanism to detect the malicious node. In this method a Streak counter was deployed to store the consecutive number of packets dropped and a trust factor was maintained for each node. The trust factor drops exponentially with each consecutive packet dropped which helps in detecting the malicious node. The method showed a drastic decrease in the number of packets dropped before the node being detected as a malicious node. [1]

Baviskar et al. The security in wireless sensor network is a main issue due to the limitations of power usage. Several techniques based on secret sharing and multi-path routing have been proposed in it However, these techniques are not very effective, and when demonstrate, they may even end up making black hole attacks more effective. Propose an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission and performance compare with multiple base stations and without multiple base station to prevent black hole attack. [2]

Wazid et al. proposed an algorithm used for detection and prevention of black hole attacks which is harmful for the wireless sensor networks. Black hole is just like as DOS attack. Black hole attacks degrading in the performance of network parameters are affected *i.e* end- to- end delay and throughput**.** [3]

Dighe et al. proposed a technique based on secret sharing and multipath routing to overcome black hole attacks in the network. However, these techniques were not very effective. The efficient technique that uses in multiple base stations deployed in the network to reduce the impact of black holes on data transmission. [4]

Wazid et al. Proposed the comparative performance analysis of two WSN's topologies i.e. Tree and Mesh under black hole attack is done. If there is a WSN prone to black hole attack and requires time efficient network service for information exchange then Tree topology is to be chosen. If it requires throughput efficient and consistent service in the network then Mesh topology is used. An algorithm named as Topology Based Efficient Service Prediction (TBESP) algorithm was proposed depending upon the analysis done which will helped in choosing the best suited topology as per the network service requirement under black hole attack. [5]

Athmani et al. proposed the energy efficient intrusion detection system, to protect sensor networks from black hole attacks. The simple approach is based on control packets exchange between sensor node and the base station. [6]

Zhang et al. the location of each node in randomly deployed wireless sensor networks, and the detection of coverage holes. An improved hole detecting algorithm was proposed based on the Boolean sensing model .The algorithm used for hole boundary node by using diagram [7]

Amoli et al. studied the detection of the attack in very high speed networks by using the software network intrusion detection system .In this analyzing statistics of network flows increases feasibility of detecting intrusions within encrypted communications they had found the weaknesses and limitations of current unsupervised NIDS(Network Intrusion Detection System) [8]

Sheela .D et al. proposed a lightweight, fast, efficient and mobile agent technology based security solution against black attack for wireless sensor networks (WSNs). WSN has a dynamic topology, intermittent connectivity, and resource constrained device nodes. The scheme was used to defend against black hole attack using multiple base stations deployed in network by using mobile agents. The attack can be accomplished either selectively (e.g. by dropping packets for a particular network destination, a packet every n packets or every t seconds, or a randomly selected portion of the packets, which is called "Gray hole attack") or in bulk (by dropping all packets). Mobile agent is a program segment which is self-controlled. They navigate from node to node not only transmitting data but also doing computation. The benefit of using this mechanism is that it does not require more energy. [9]

Schaffer et al. reviewed the state-of-threat of clustering protocols in WSNs with special emphasis on security and reliability issue. They define taxonomy of security and reliability for cluster head election and clustering in WSNs. They propose a counter measures against typical attacks and show how they improve the discussed protocols. [10]

III. Blackhole Attack

The black hole attack is one of the simplest routing attacks in WSNs. The black hole attack is the routing attack in the sensor which act on the network layer are called routing attacks. The attacks that happen while routing the messages send. The adversary captures these nodes and re-programs them so that they do not transmit any data packets forward. In a black hole attack, the attacker transitive *i.e.* receives but does not forward) all the messages to the receive A black hole is a just like as Denial of Service (DoS) attack which is very difficult to detect and remove . The black hole attack is a active attack .In a black hole attack all the packets are consecutively dropped which leads to the decrease in the efficiency of the network and unnecessary wastage of battery life.

Working of Black Hole Attack

Any information that enters the black hole region is captured and not able to send the data from source to destination and this causing more power usage of the battery. In this technique a coordinator is responsible for authentication, checking of the failure of intermediate node and detection of Black hole attack.

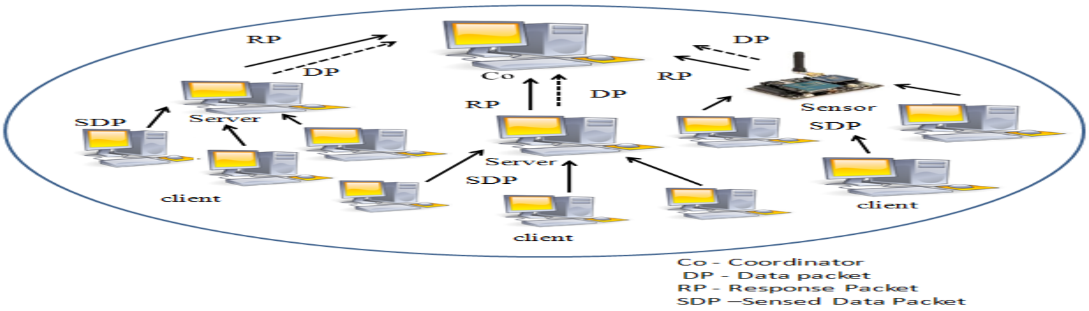


Fig.1 Normal flow of packet [3]

The client sense physical phenomenon converts this into information and passes that information to the server in the form of Sensed Data Packet (SDP) as shown in fig1 Server further processes this information and passes it to the coordinator in the form of Data Packet (DP) depicts that the server doesn't reply with the Response Packet (RP) and Data Packet (DP) to the Coordinator. The coordinator waits for a fixed period of time. If here sensor doesn't send any of these packets even after this time period, it means the sensor has failed

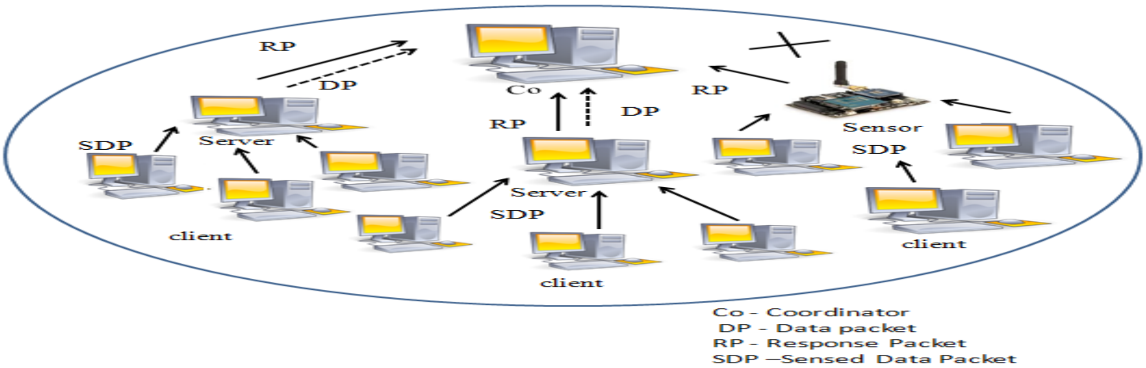


Fig. 2: Traffic Flow under Black hole Attack [3]

Show as fig.2 becomes the black hole node as it consumes all the Sensed data Packets (SDPs) coming from the Sensor nodes without forwarding them to the Coordinator. In this way normal flow of traffic is achieved in the network.

IV. Multiple Base Stations

The use of multiple BSs is used for improving data delivery in the presence of black hole attacks. For WSN proposed a technique in which transmitting of sensor node performs power control to transmit a packet to more than one sensor nodes in the direction of the base station If the sensor node that is on the forwarding path does not forward a packet, then its next hop neighbor on the forwarding path will identify this event and report to the sensor node as a black hole. This scheme is very expensive for a network with n number of black hole nodes.

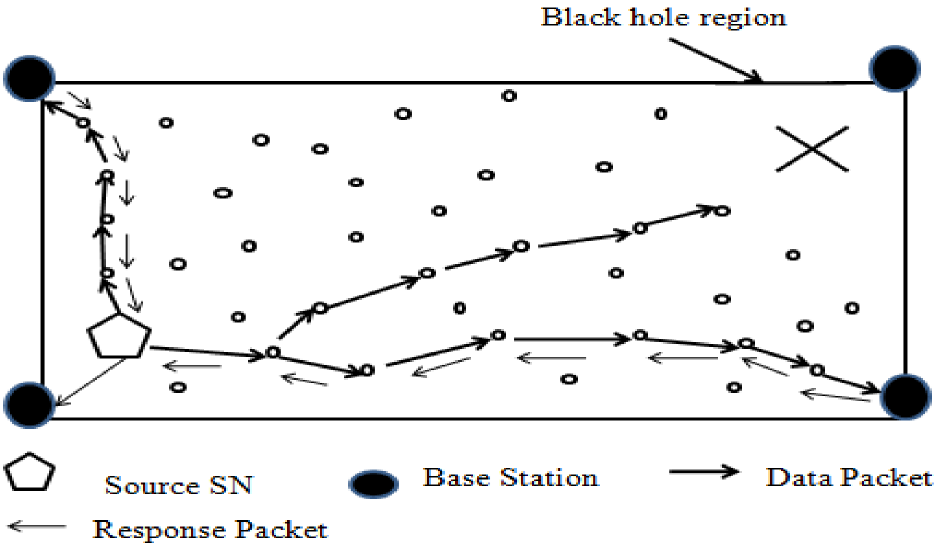


Fig.3: Data Delivery Success improves with Multiple Base Stations [4]

In fig.3 Sensor Node transmits the data towards the Base Stations using three nodes disjoint paths. The fig shows that none of the packet traversing the three paths reaches the Base Stations. This demonstrates that multi-path based routing can perform arbitrarily bad in the presence of black hole attack. By using multiple base stations placed in different end and detect black hole attack in path of different base station. In multipart base station technique, black hole region close to the Base Station can capture all packets with high probability also all the routes directed towards a single base station. The use of multiple base stations for improving the data transmission. The following show the steps of the algorithm.

V. Proposed Approach

BHDP (BLACK HOLE DETECTION AND PREVENTION) USING FUZZY LOGIC ALGORITHM

In the BHDP (black hole detection and prevention) using fuzzy logic algorithm involves following steps:

Algorithm BHDP using fuzzy logic

Step1: Create a wireless sensor network of N nodes

Step2**:** Define the member nodes of four base stations according to given range

Step 3: Select the nearest member of nodes which is nearest to the base station.

Step 4: Send the packets from one base station to anther base station.

Step5**:** Analysis the parameters such as total packet drop, Packet delivery ratio, Theoretical packet loss, Actual packet loss and routing overhead for each neighbor parameters

Step6: Apply fuzzy logic to do detect under the network under attack or not

Step7**:** Remove the attack

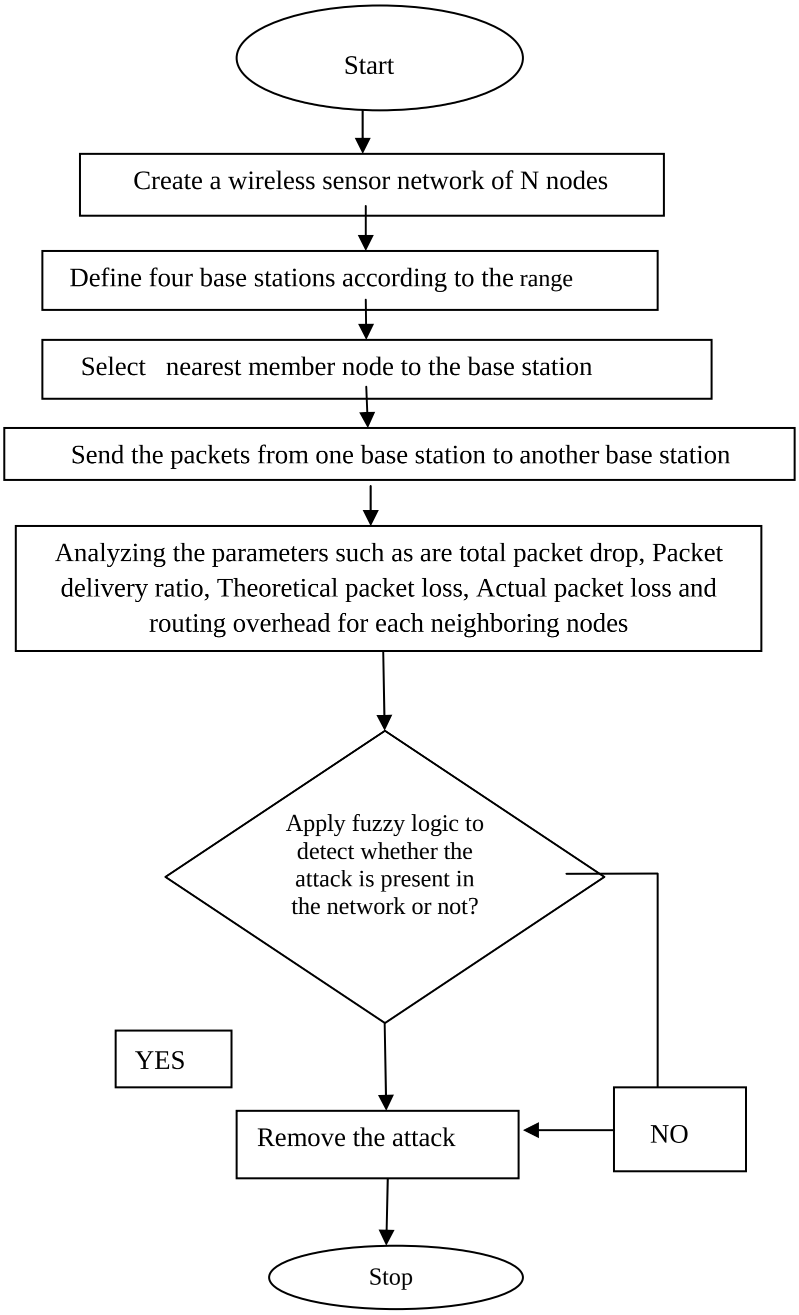

Start
Create a wireless sensor network of N nodes
Define four base stations according to the range
Select nearest member node to the base station
Send the packets from one base station to another base station
Analyzing the parameters such as are total packet drop, Packet delivery ratio, Theoretical packet loss, Actual packet loss and routing overhead for each neighboring nodes
Apply fuzzy logic to detect whether the attack is present in the network or not?
YES
NO
Remove the attack
Stop

Fig. 4: Flowchart representations of proposed work

VI. EXPERIMENTAL RESULTS

To evaluate the behavior of simulated based black hole attack, to observe the network under the attack or not so, we considered the performance parameters of networks are Total packet Drop, Packet Delivery Ratio, Routing Over head, Actual packet loss, Theoretical Packet loss.

A. Packet Delivery Ratio:

Packet Delivery Ratio (PDR) is the ratio of number of delivered data packets to the total number of packets sent. The greater value of packet delivery ratio means the better performance

B. Routing Overhead:

Routing overhead is the amount of information needed to describe the changes in the dynamic topology.

C. Total Packet Drop:

The total number of packets dropped during the sending of the packets lower value of the packet lost means the better performance of the protocol.

D. *Theoretical Packet Loss:*

This number is closely related to the channel capacity of the system and is the maximum possible quantity of data that can be transmitted under ideal circumstances.

E. *Actual Packet Loss:*

The loss according to the calculation to the formula.

Creating a Wireless Sensor Networks

Creating a wireless sensor network according to the given range with four mulitple base stations with N number of nodes.

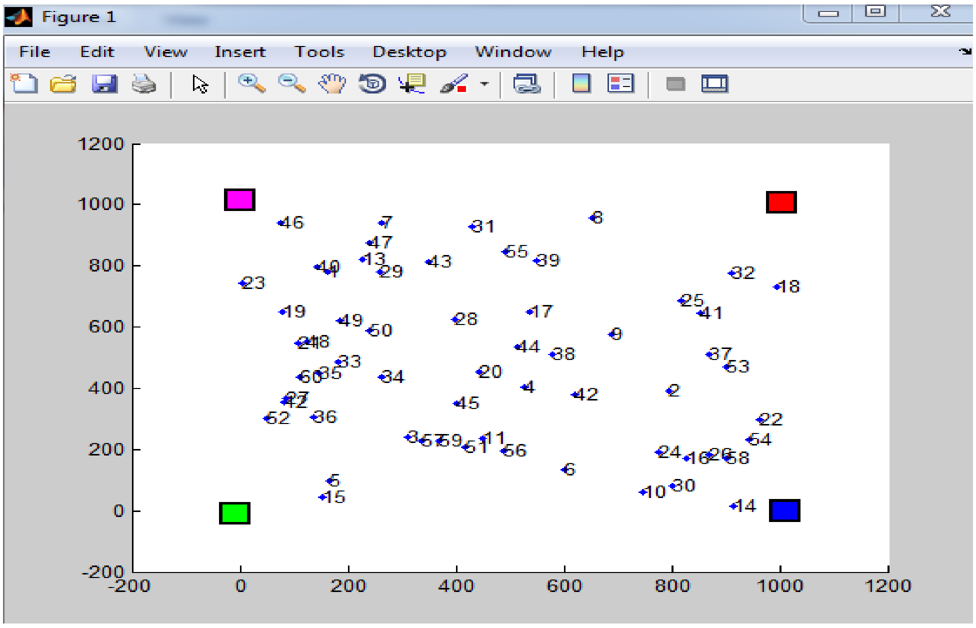


Fig -5: Creating a WSN

The fig.5 shows that packet traveling green,blue,red,pink are the four base stationand blue dots with number shows the sensor nodes that demonstrates the multiple-path base routing can perform arbitrarily bad in presence of black hol attack

Nodes transmits the data towards the base station using four nodes disjont paths as shown in fig.6

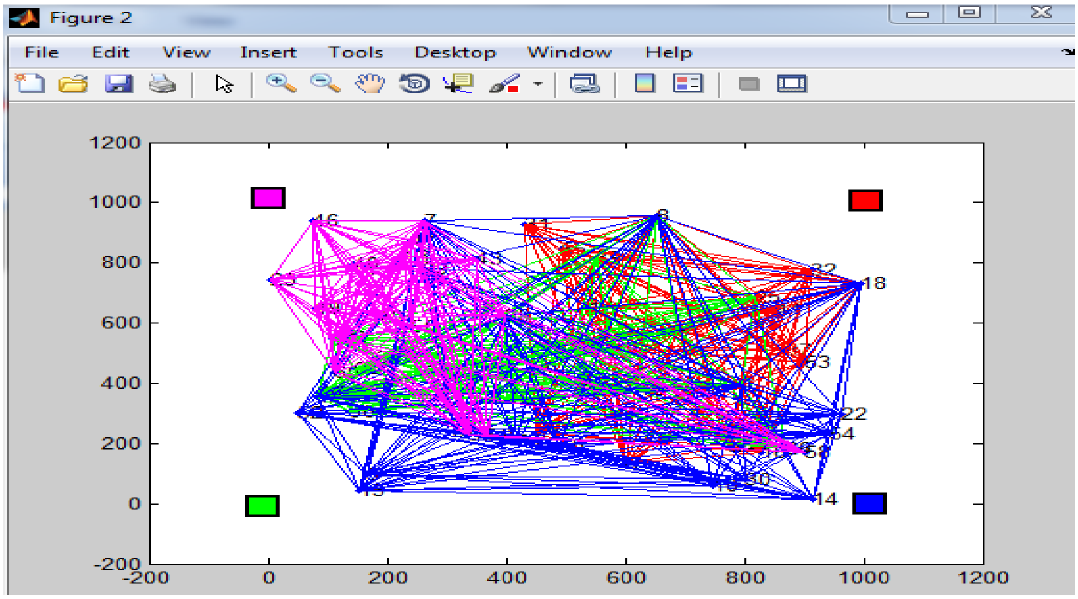


Fig. 6: Member of WSN Connect nearest neighboring base stations

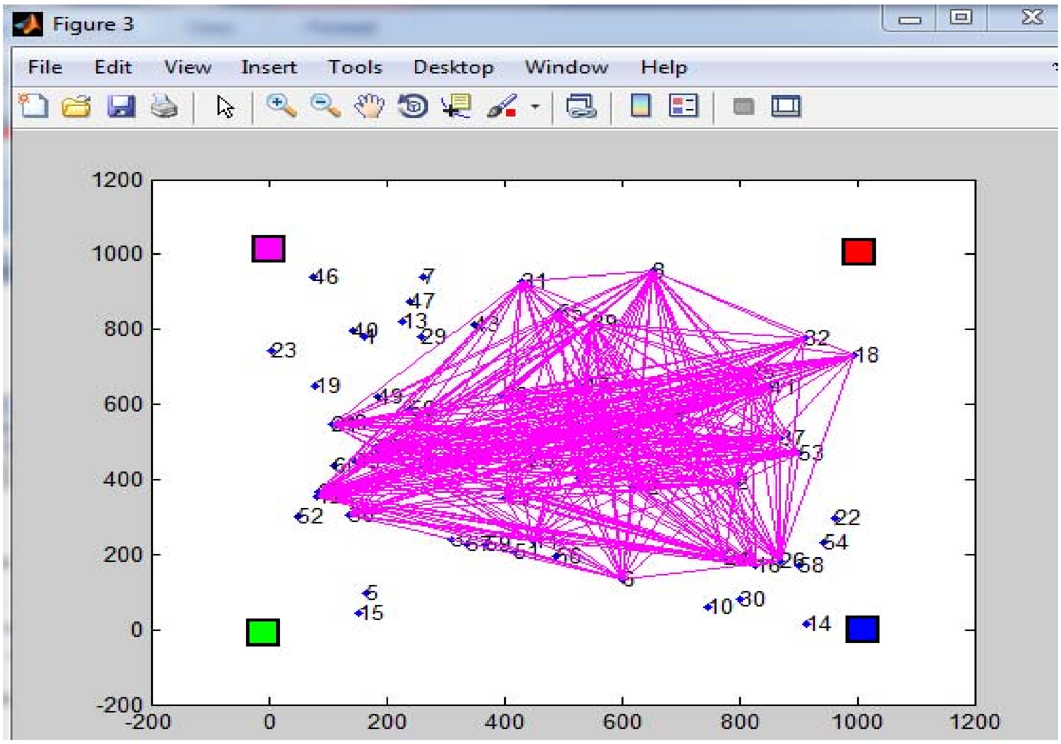


Fig -7: base station send data to other base station and check the black hole attack

Network Not Under Black Hole Attack

The network not under attack when normal flow all the sensor nodes are sending packets to the base station. When one base station become sends data to anther base station without the time delay and report to the other base station that it receives the packet and the data called the network not under the black hole attack the packet sending calculates the given parameters and the nodes report to source that the data is send then the dialog box appears which tells the network under attack or not In this way normal flow of traffic is achieved in the network. as shown in the figure 8

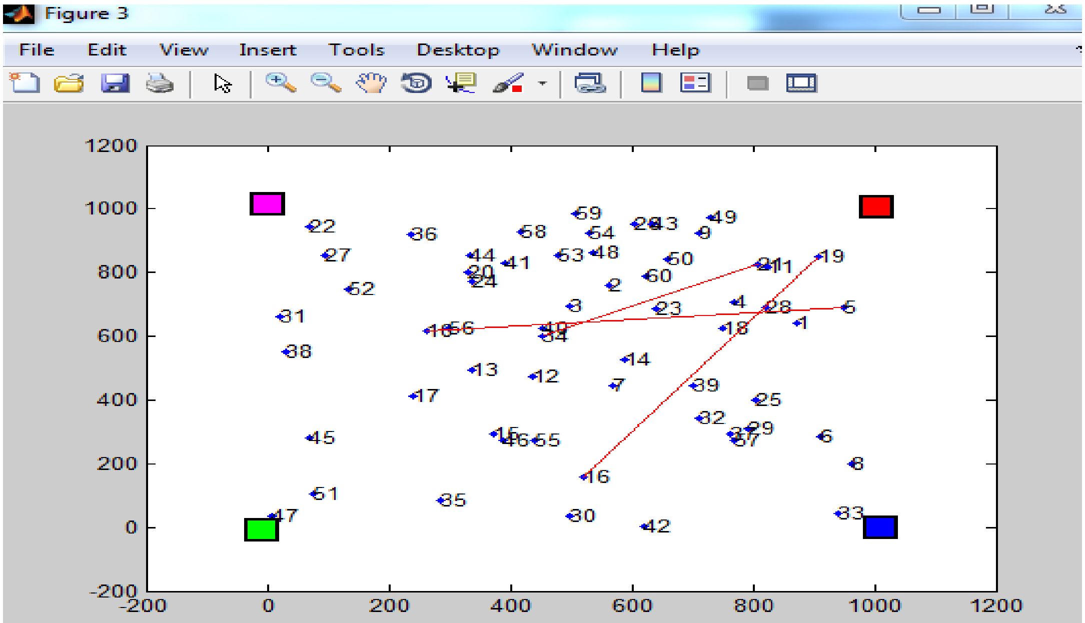
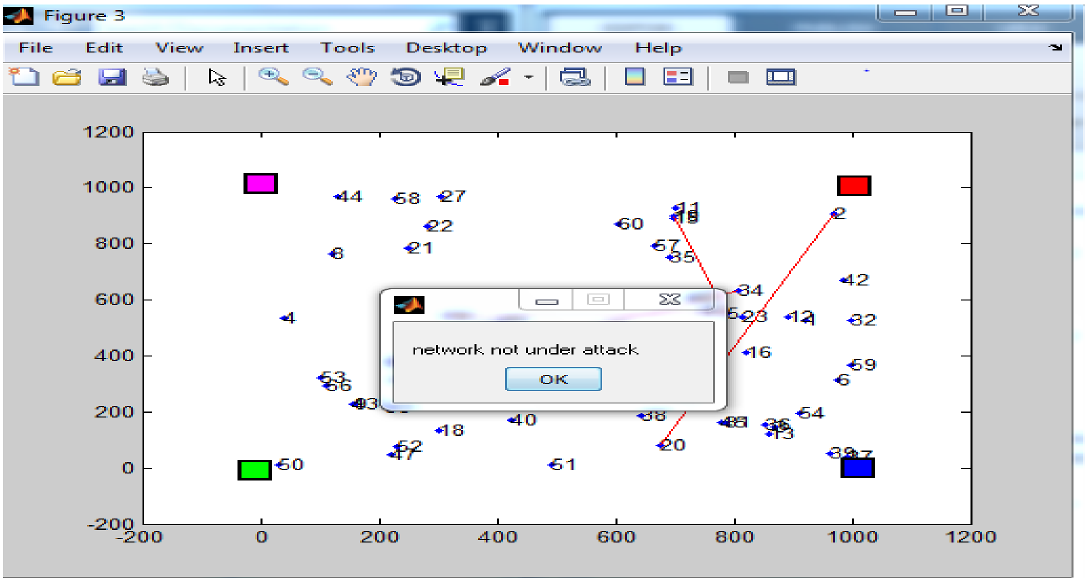


Fig 8: packets sending for parameter calculation

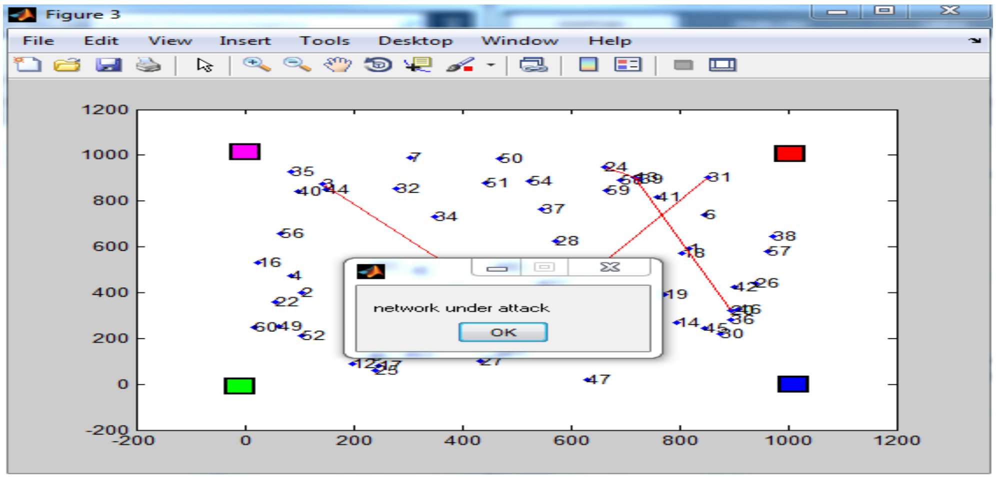


network not under attack

Fig 9: the message box the network not under the attack

Network under Attack

The network under attack when normal flow all the sensor nodes are not sending packets to the base station. When one base station becomes black hole attacker it consumes all received traffic and doesn't report to the other base station because it is sending the Response of the Packets but not the Data Packets are called the network under the black hole attack then the packet sending calculates the given parameters and the nodes report to source that the data is send then the dialog box appears which tells the network under attack or not as shown in the figure 10

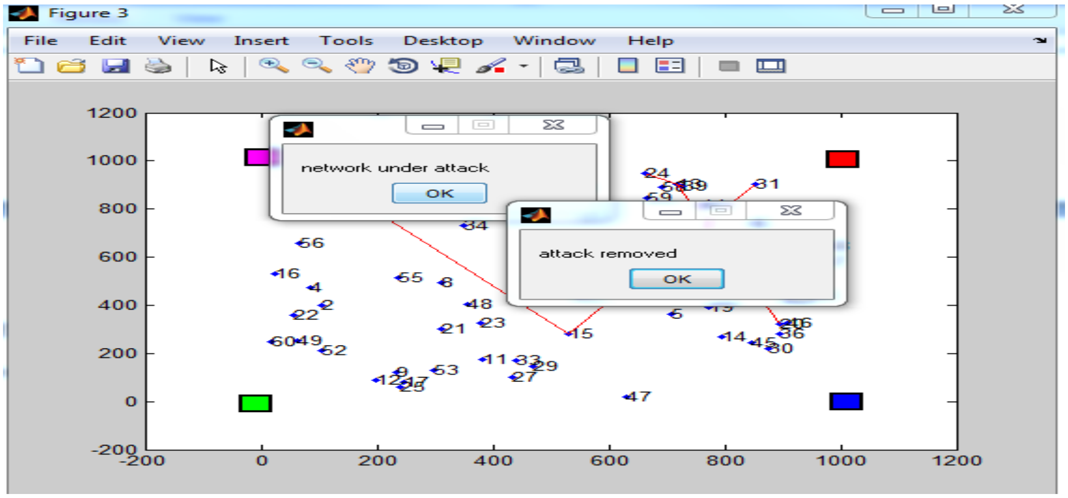


network under attack

Fig. 10: the network under the attack

Removal of Black Hole Attack

After the detection of the black hole attack node, is reformed by removing node. Sensor nodes are which were initially reporting to the base station now are sending data packet to other base station. Inform its previous nodes via beacon signal for the node with which now they have to communicate. Continue detection process. In this way normal flow of traffic is achieved in the network.



network under attack

OK

attack removed

OK

Fig.11. the message box that the attack is removed

Performance Parameters with network not under Black Hole attack. P is for good packet and R is for bad packet.

TABLE 1: Network not Under Black Hole Attack

P	R	PDR	ROVH	TPD	APL
0.235	0.02	0.4974	0.0051	0.0268	5.5026
0.335	0.03	0.4976	0.0061	0.0045	5.5024
0.45	0.04	0.5146	0.0175	0.0248	5.4854
0.535	0.055	0.5748	0.0145	0.0154	5.4252
0.635	0.06	0.5367	0.0188	0.0188	5.4633
0.735	0.07	0.5301	0.00098	0.0084	5.4699
0.835	0.08	0.5666	0.0282	0.042	5.4334
0.93	0.09	0.538	0.0136	0.0086	5.462

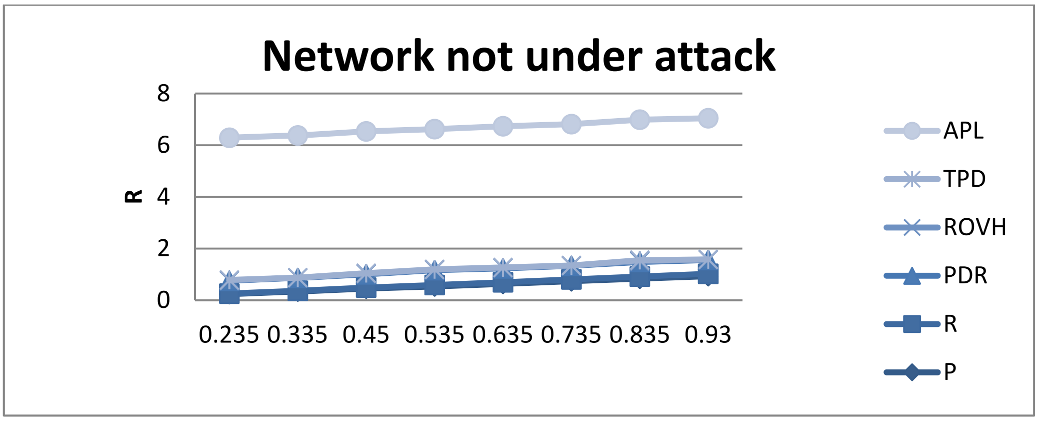


Fig -12: total drop packets, routing overhead, packet delivery ratio, actual packet loss not under attack

The fig12 shows the parameters when the normal flow of network. The fig13 shows the parameters affect when the network under the black hole attack Performance Parameters with network under Black Hole attack P is for good packet and R if or bad Packet.

TABLE 2: Network under attack

P	R	PDR	ROVH	TDP	APL
0.25	0.2	2.76675	0.0031	0.01008	3.2325
0.355	0.3	2.7898	0.0013	0.0417	3.2102
0.44	0.4	2.8704	0.0017	0.0133	3.1246
0.55	0.5	1.6464	0.0227	0.0464	4.3536
0.655	0.6	2.9119	0.0053	0.0116	3.0881
0.75	0.7	2.9078	0.0027	0.0113	3.0922
0.85	0.8	2.9119	0.0053	0.0116	3.0881
0.95	0.9	2.9265	0.0018	0.0076	3.0735

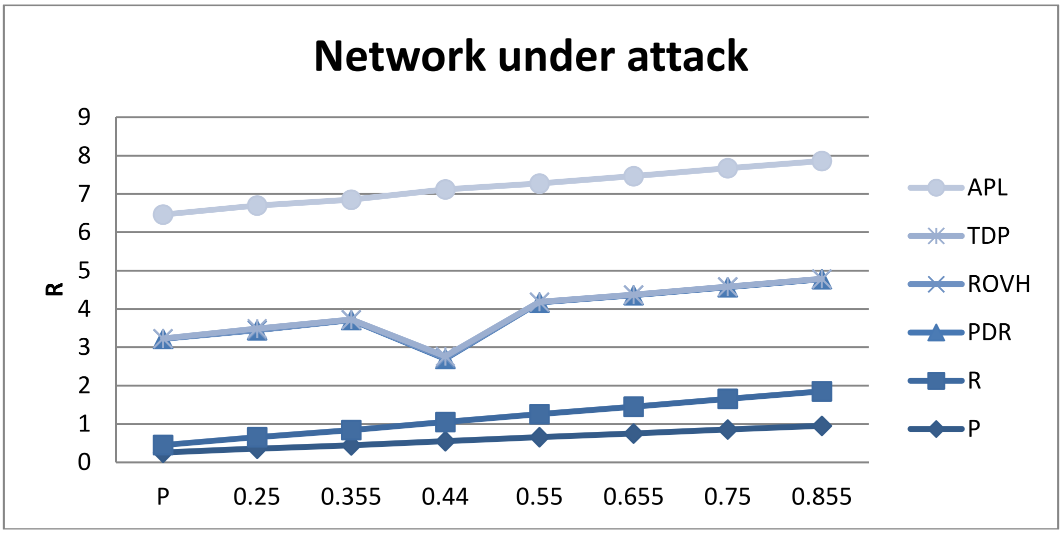


Fig 13 total drop packets, routing overhead, packet delivery ratio, actual packet loss under attack

Finally this research has shown the improvement done by proposed work in graphs with respect to parameters like actual packet loss, total packet drop routing overhead, packet delivery ratio

VII. Conclusion

The proposed BHDP (Black Hole Detection and prevention using fuzzy logic algorithm) that used detects and prevents the black hole attack in WSN. The advantage of the proposed algorithm is that it does not make any modification to the packet. Hence the multiple base stations receive the same packet despite of the presence of black hole. The parameters (such as packet delivery ratio, total packet drop, routing over head, theoretical packet) used in this work to help in determine the consequence of black hole attack effectively on the wireless sensor network.

VIII. Future Work

The Future work includes comparing of the proposed algorithm with another algorithm. The propose algorithm has been used for detecting and preventing the black hole attack, as future work the proposed algorithm can be use for detecting the preventing other types of security attacks such as Grey hole or Wormhole attack etc also used other parameters like total data rate, network load, throughput, end to end delay etc.

References

1. Dr. Deepali Virmani,, Manas Hemrajani and Shringarica Chandel., "Exponential Trust Based Mechanism to Detect Black Hole attack in Wireless Sensor Network " Bhagwan Parshuram Institute of Technology,vol.1 Jan(2014).
2. B.R. Baviskar and V.N.Patil "Black hole Attacks Prevention in Wireless SensorNetwork by Multiple Base Station Using of Efficient Data Encryption Algorithms" International Journal of Advent Research in Computer & Electronics, Vol.1, No.2, (2014).
3. Mohammad Wazid , Avita Katal ,Roshan Singh Sachan , R.H Goudar and D.P Sing.,"Detection And Prevention Mechanism For Black hole Attack" in Wireless Sensor Network IEEE,(2013)
4. Pranjali G Dighe , and Milind B Vaidya "Counter Effects of Black Hole Attack on Data Transmission in Wireless Sensor Network with Multiple Base Stations" International Journal of Engineering and Innovative Technology (IJEIT) Vol.3,Issue5, (2013)
5. Mohammad Wazid, Avita Katal, Rooshsn Singh, Sachan , R.H Goudar and D.P Singh, "TBESP Algorithm for Wireless Sensor Network Under Black Hole Attack" IEEE International Conference on Communications (ICC) (2013).
6. Samir.Athmani., Djallei Eddine Boubiche and Azeddine Bilami ," Hierarchical Engery Efficient Intrusion Detection System For Black Hole Attacks in WNS" IEEE International Conference on Communications (ICC) (2013).
7. Yunzhou Zhang, Xiaohua Zhang, Zeyu.Wang and Honglei Liu.," Virtual Edge Based Coverage Hole Detection Algorithm in Wireless Sensor Network" IEEE International Conference on Communications (ICC) (2013).
8. Payam vahdami Amoli , Timo Hamalainen , "A Real Time Unsupervised NIDS For Detecting Unknown And Encrypted Network Attacks in High Speed Network", IEEE International Conference on Communications (ICC) (2013).
9. D.Sheela, V.R Srividhya, A.Begam, Anjali and G.M Chidanand," Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent" International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012)
10. Peter.Schaffer, karoly.Farkas, Adam. Horvath Tamas Holczer and Levente. Buttyan, "Survey Secure and reliable clustering in wireless sensor networks: A critical survey", ACM, Computer Networks: The International Journal of Computer and Telecommunications Networking, (2012).