Blackhole Attack Detection And Prevention Mechanism Using Ns2 Simulation

Ashwini V. Jatti and V.J.K. Kishor Sonti

Abstract:— Wireless Sensor Networks (WSNs) are susceptible to several attacks. Attack in which an intruder captures the nodes and change the programming of group of nodes and instead of forwarding packets to the base station, they are blocked is called blackhole attack. Due to this data entered in the attack area is seized and unable for reaching its end point which tend to low throughput and delay from end to end. Blackhole attack effect in this paper is determined on different parameters of network and mechanism for blackhole attack detection and prevention in AODV routing protocol. With proposed scheme the dropping ratio under attack is around 4 percent less than in comparison to AODV protocol and number of packet loss is also decreased. Under proposed scheme PDR is 39.4057 and under normal flow PDR is 43.2935. Under normal flow, end to end delay is 10.5026 msec and by this proposed scheme is 9.4160. Throughput under normal flow is 13.8578 bps and under proposed scheme is 12.6133 bps. Total energy consumption under normal flow is 79.5844 mJ and under proposed scheme is 79.8618 mJ. Due to this technique, there is increase in packet delivery ratio and delay is also decreased. Proposed mechanism discovers new route to destination by avoiding the attacker nodes.

Index Terms:— Blackhole attack, AODV, Routing Table, Backbone network, Packet delivery ratio, End-to-end delay, Throughput.

1 INTRODUCTION

Noteworthy progress has been made in sensor network security, ensuring resilience to malicious nodes. But there is always threat of attacks in WSN such as Blackhole, grayhole, sinkhole attacks. A security system must be able to tackle with persistence of attacks. Protocols developed till now deals with single attacks. Mostly, a security protocol developed for countering a particular threat is not suitable for defending different types of threats. A malicious node is a black hole which misguides the nodes to answer for any Route Requests (RREQ) which do not have active route to definite destination and all the received data is dropped. The nodes which are malicious can prove to be very dangerous if they all form a group and work together. Such attack types are called as cooperative blackhole attack. Blackhole attack different type is grayhole attack, where nodes are not attacker before and it becomes malicious later on.

Solution to this will be integration of all protocols but not for sensors networks due to their low storage capacity and processing capabilities. Attack analysis is itself a challenging problem. A smart attack can use different types of attacks for testing wireless sensor networks. This paper presents a technique of detecting and eliminating of grayhole and blackhole attack. Our proposed method works as follows, a backbone network of reliable nodes is established, at first over the ad hoc network. Later on, sometime request for a restricted new IP address which are not used, source node send for one of the backbone nodes. RREQ is sent by the node for search of destination node when it needs to make a broadcast, and at the same time search for restricted IP. When attacker nodes for any RREQ send RREP, then nodes also send a reply with RREP for the RIP (Restricted IP). Detection process of these attacker nodes is started by the source nodes, when this attacker node route replies certainly to any of the restricted IP with a RREP [10].

- *Ashwini V. Jatti is currently pursuing PhD degree from Sathyabama Institute of Science and Technology, Chennai - 600 119, India. E-mail: koti.ashwini@gmail.com*
- *V.J.K. Kishor Sonti is working as Associate Professor in Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai - 600 119, India. E-mail: kishoresonti.ece@sathyabama.ac.in*
- *kishoresonti.ece@sathyabama.ac.in*

2 LITERATURE REVIEW

This section deals with the review of previous researcher's findings and their views. Bhargava et al. [4] has presented an Intrusion detection and Response model for detection of any malicious activity in a routing protocol and responses if any node anomalously using Intrusion Detection Model. Ramaswamy et al. [1] proposed a technique in ad hoc network for prevention of the co-operative black hole attacks. Their method is created on a trust relationship between the nodes, therefore they failed to tackle grayhole attacks. This method process for long time for completion, even though attacker had not attacked the network due to intensive cross checking. Shurman et al. [5] presented two methods for detection of blackhole attack. This method had drawbacks of related time delay due to hops sharing with the route and usage of additional two tables where every node update frequently. Due this, these methods could not work for set of malicious nodes in network. Deng et al. [2] has presented a technique for prevention of black hole attacks in ad hoc network. When node gets the RREP packet from another path, it cross checks with the next hop on the route to the destination in this method. When the hop which is next neither have a route to the sink node and nor have a connection with node that transmit the route response, then which node transmit the route responses is detected as attacker node. When the nodes which are malicious unite together, this method fails.

Haung et al. [9] implemented a Cooperative Intrusion Detection System in adhoc network for attacks of different types which affected routing protocol and IDS also. But the detection results of blackhole attack were not so good and it was economy high. Agarwal et al. [6] had presented a mechanism of creating strong node network as a backbone

network. Strong nodes network called as Backbone network help the sink and source nodes to carry the checking determination for an end to end, if destination receives all the data packets. Backbone network starts a procedure to detect the attacker nodes, if checking results fails. Using backbone nodes concept, an algorithm is having been designed. Indrasinghe et. al. [7] and Mohsin et al. [8]. has discussed the idea of state full approach in ad-hoc networks of IP addresses allocation.On basis of the literature review it can be seen that variety of techniques were implemented for detection and prevention in wireless sensor networks of the black hole attacks, however there is no single solution available to detect and prevent attacks. Some or other limitations are observed in the intrusion detection systems developed by researchers in the past. Hence there is a scope to develop an IDS (intrusion detection system) for detection and prevention of the attack in the wireless sensor networks. Packet delivery ratio increases and end-to-end delay reduces, reduce energy consumption and throughput increase under blackhole attack using NS2 simulation was the aim of study.

3 NETWORK MODEL

By selecting few nodes, the problem is approached so they can be reliable and must be powerful in terms of battery power. A BB network is created by these nodes which are stated as BBN (Back Bone Nodes) and has some unusual function different from usual nodes. The system is separated into many networks where Normal Nodes and the Back Bone Nodes (BBN) for the co-ordination are expected. Initially the nodes are expected to be capable of finding their particular grid locations after entering the network. It is also supposed at any point of time the black/gray nodes numbers are less than number of normal nodes.Stateful classification – formation of the IP address can be divided into-

1. Stateless method
2. Stateful method.

1. Stateless method: In this method, by self-assignment unconfigured host must obtain its own IP address. Random address task is approved by this method and followed by duplicate address detection technique is used to achieve address uniqueness. There is no allocation table in Stateless method.

2. Stateful method: In this method, an host which is unconfigured to acquire IP address asks to work as proxies its neighbor nodes. New type of state-full approach is created viz. Core Maintenance of the Allocation Table.

4 BLACKHOLE ATTACK IN WSN

Black hole attacks are attack in which an intruder captures the nodes and change the programming of group of nodes and instead of forwarding packets to the base station, they are blocked. Due to this, data is captured which arrives in the attacker (black hole) region. These attacks can be created simply and are able to decrease system efficiency by dividing the network, thus base stations will not get the important dat. Throughput and end-to-end delay of network performance like parameters can get affected due to occurrence of blackhole nodes end- to- end delay increases and throughput decreases Blackhole attack occurs as follows:Regular packets flow:Regular packets flow is shown in the figure 1. In figure 1 sensor nodes which are labeled as SN1 to SN2, two nodes which are router nodes which are R1 and R2 and a node as coordinator are shown. Physical phenomenon is sensed by sensor nodes which is then converted into data and then this sensed and processed data is transmitted to R1 and R2 router nodes. SN1, SN2 and SN3 sensor nodes data is transmitted to R1 router and remaining sensor nodes data is transmitted to R2 router. Coordinator node receives the information from routers [11].

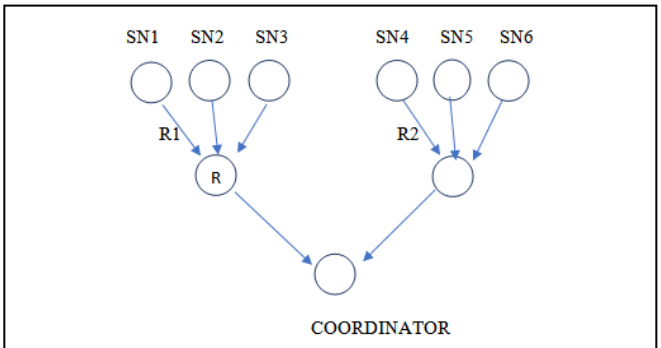

Fig. 1 *Regular flow of data packets*

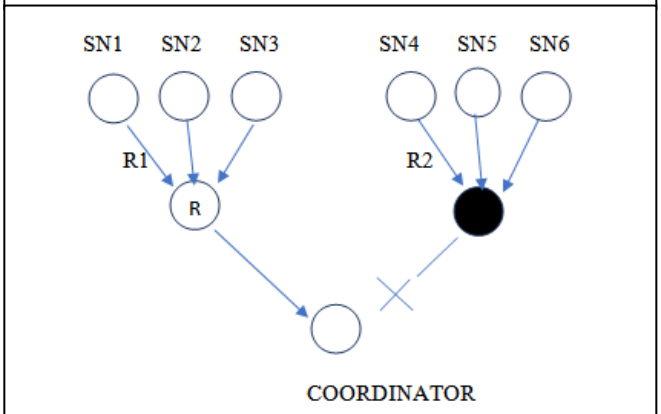

Fig. 2 *Blackhole attacker situation where R2 router converts a blackhole attacker node*

Figure 2 shows blackhole attacking on nodes. Here a coordinator, two nodes which are router nodes (R1, R2) and six nodes which are sensor nodes (i.e. SN1, SN2, ----- SN6) are present figure 2. Physical phenomenon is sensed by the sensors, translate it in data and this sensed and processed data is transmitted to R1 and R2 router node. SN1, SN2 and SN3 sensor nodes broadcast their data to R1 router and remaining sensors broadcast to R2 router. Coordinator node receives the information from R1 router. Since now the R2 router becomes a blackhole attacker and captures whole data received by it without further transmitting it to coordinator. R2 router as black background here denotes the blackhole node. As blackhole attacker R2 absorbs of all the data packets, delay rises and throughput reduces. Hence the network performance is degraded [11].

5 BLACKHOLE ATTACK DETECT ION AND REMOVAL

MECHANISM

Data packets are not allowed to reach its sink node by blackhole attacker node. So here a method is being proposed for blackhole attack detection and prevention. In this method

the blackhole is detected before it attacks the node and reprogram its data and prevents from data loss.

Mechanism

An AODV which is on-demand vector routing protocol is a source originated. Each single node which is mobile has a table named routing table, where there is data of route for sink node from the node of next hop. Source node makes the use of the definite route which is available from its routing table to the sink node, but if the source node wants to send to a sink node a data packet. It is if unavailable, then by propagating the Route Request (RREQ) message to its neighbors, a route discovery process is started, which is then further transmitted till an intermediate node receives it with a new adequate path to the sink node definite in the RREQ, or the sink node itself.

Entry of the node that transmits the RREQ message further which RREQ and source node is made by the intermediate node. Route Response (RREP) message to the next neighboring node from which it received the RREQ with a new adequate route toward the sink node is unicasted by intermediate or sink node. The RREP is forwarded in the reverse direction after an intermediate route makes an entry for the neighboring node from which it received the route response. Source node with an entry for the sink node updates its routing table, and the node from which it got the route response, on receiving route response. Through neighboring node which responded first with a route response, data packet is started transmitting from the source node towards the sink node.This method gives list of the set of attacker nodes when they turn as a source node locally at every node. Concept of Core Maintenance of the Allocation Table is used in our protocol uses i.e., a new node for IP address has to send a request of a transmission message, as a request for IP address, it sends a broadcast message, when it joins the network. IP addresses which is free is selected by backbone nodes after getting this message. BBN receives an acknowledgement from the new node once it receives the allotted IP address. Only BBN knows unused/restricted IPs of the network from the active pool at any point of time because Back Bone Nodes (BBN) controls the allocation. Firstly, when source node wishes to communicate the information, for a restricted IP (RIP) it sends a request to the BBN which is nearest to it. Source node receives an answer with one of the unused IP addresses from BBN after randomly selecting from the pool of unused IP addresses. At same time source node transmits the route request for destination and the RIP also.In a normal case, only sink node transmits an RREP to source node and not from restricted IP (RIP), that means at that time the local network is having normal node and free from attacker nodes. For certain period of time the RIP is reused by source node for further data transmissions. This recently sent RIP is not assigned to any other node by BBN until that period of time. However, the source node receives an RREP for the RIP, when there is an attack in that route. Then the attack detection process is started by source node. The SN firstly transmits to the neighbors of the node an alerts message to enter into promiscuous mode from where it received RREP to RIP. So that neighbor nodes would listen to the packet assigned to them and also to the packet designed to the defined sink node. Then next SN transmits to the destination some dummy data packets, meanwhile nodes from neighboring start the monitoring of packet flow. Neighboring nodes transmits this monitored message further towards the next hop of the dummy packet of data & so on. Now, if it comes to know that more dummy packet of data is lost extra than loss of the normal packets expected network, by the monitoring nodes then it informs about this particular IN (Intermediate Node) to the source node. The location of the attack (Black Hole) with the help of information received by the various nodes which monitors is detected by source node. Throughout the network this information is broadcasted, leading to its labelling as black hole and their records are canceled. Then each and every node reject further any black hole responses and looks for a valid changed route to the sink node [10].

Algorithm for detection Blackhole attacks

Step 1: Network of backbone nodes is created. A request to backbone network for new restricted IP is sent by source node. Backbone network search for new unused IP address and source node receives new restricted IP address.

Step 2: Request is being sent by source node to sink node for further transmission and to restricted IP also waits for a limited time.

Step 3: Destination node on receiving request from source node, in routing table enters its IP address. If it is sink node or route towards the sink node then sends a response to source node for further transmission.

Step 4: When the node that accepts request from source node is not a sink node, then it becomes intermediate node and forwards the request to next node in the network.

Step 5: Intermediate node again makes an entry of the IP address of the node which sends a reply to its request and transmits IP address of its neighbor node to source node.

Step 6: If source node receives a response from only sink node then it transmits the data packets to the sink node. But when it receives response from both sink node and restricted IP, then it sends a dummy message and starts the detection process.

Step 7: Source node sends a request to neighbor nodes to enter in safe area and keep monitoring other nodes whether they are normal nodes or attacker node. When dummy message loss is more than the threshold value, intermediate nodes transmits IP of attacker node to the source node.

Step 8: on receiving information from intermediate node, source node halts the data transmission to that node and transmits the data from new route to the sink node.Thus, the data loss due to attacker node can be overcome. Throughput can be increased and end to end delay can be decreased.

6 RESULTS AND DISCUSSIONS

In this study a wireless sensor network with 100 nodes under blackhole attack has been simulated in NS2 simulation tool.

6.1 Simulation Design

Different parameters for simulation are considered. They are as follows shown in table.

Figure 3 shows the formation and motion of the nodes. 100 nodes are created for simulation. One node is created as source and one as sink node. Two nodes are created as attacker nodes. Node 5 is made as a source node and node 9 as destination node. Node 12 and node 35 are created as an attacker node. Nodes in brown color are intermediate nodes as shown in figure 4. Intermediate nodes keep monitoring the nodes behavior and packet flow. Intermediate node also response to the source node by transmitting restricted IP. Till

TABLE 1

SIMULATION PARAMETER SETUP

Sr. No.	*Parameters Description*	*Type*
1	*Channel*	*Wireless*
2	*Radio propagation model*	*Two ray ground model*
3	*Network interface type*	*Wireless/phy*
4	*Mac type*	*Mac/802_11*
5	*Interface queue type*	*Drop tail / Pri -queue*
6	*Link layer*	*LL*
7	*Antenna model*	*Omni antenna*
8	*Maximum packet in queue*	*50*
9	*Number of nodes*	*100*
10	*Routing protocol*	*DRCBC*
11	*X Dimension of topography*	*1000*
12	*Y Dimension of topography*	*1000*
13	*Time of simulation end*	*200ns*

TABLE 2

COMPARISON OF PARAMETERS UNDER NORMAL FLOW AND PROPOSED SCHEME

Parameters	*Under normal flow*	*Under blackhole attack with proposed scheme*
Number of packets send	*3601*	*3601*
Number of packets received	*1559*	*1419*
Packet delivery ratio	*43.2935*	*39.4057*
Delay(msec)	*10.5026*	*9.4160*
Throughput (bps)	*13.8578*	*12.6133*
Number of packets dropped	*2042*	*2182*
Dropping ratio	*56.7065*	*60.5943*
Total energy consumption(mJ)	*79.5844*	*79.8618*
Total residual energy(mJ)	*9820.42*	*9820.14*

now all the nodes are normal nodes and there is no loss of packet.Figure 5 shows the flow of data between the nodes. Until all the nodes are normal, Source node transmits data packets. Intermediate node is transmitting the data packets and simultaneously monitoring the neighboring nodes.

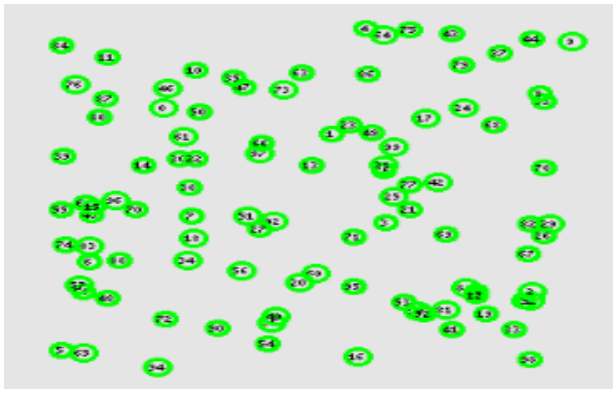

Fig. 3 *WSN with normal flow*

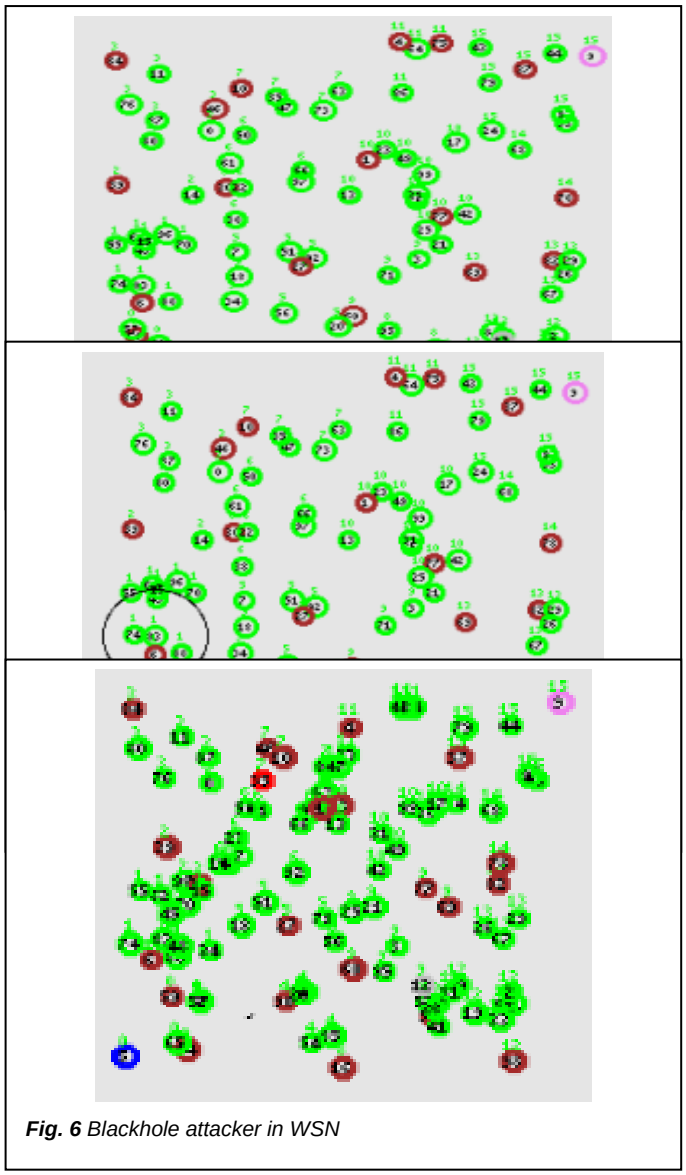

Fig. 6 *Blackhole attacker in WSN*

Node 12 and node 35 now becomes the attacker node. As shown in figure node 6 color changes from green to red. As the node becomes attacker, data transmitting towards the attacker nodes are discarded. Data packet changes its route. Intermediate nodes send an alert message to source node about the attacker nodes and changes the route of data packets.

6.3 Effect of Blackhole on Parameters

Parameter of nodes with attack and without attack is given depicted in table 2. As shown in table 2, due to this algorithm there is not much loss of data packets. Packet delivery ratio under attacker node is around 4% less and packets dropped are also less.

Output shown in form of graph is connections versus different parameters.

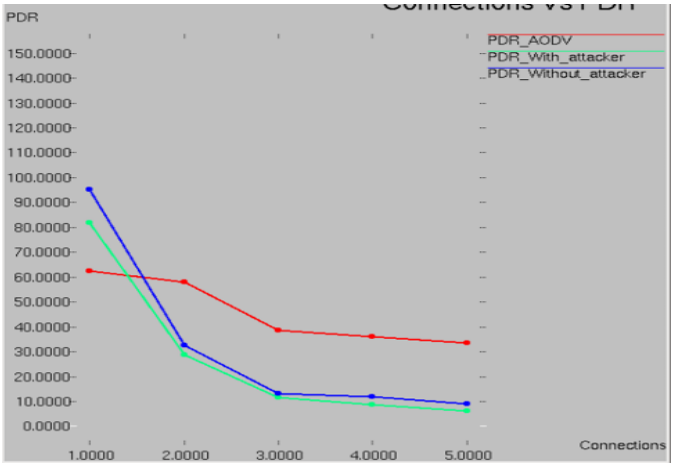

Fig. 7 *Connection vs packet delivery ratio*

Figure 7 shows the improvement in the packet delivery ratio due to incorporation of this protocol. PDR_AODV is the packet delivery ratio of nodes in AODV protocol, where packet delivery ratio decreases. As compared to AODV routing protocol Packet delivery ratio of nodes before attack and after attack difference is 4 to 5 percent.From figure 8, it can be observed that delay without attacker decreases. Delay in AODV is nearly very less. This algorithm decreases the delay even if the nodes are under attack.

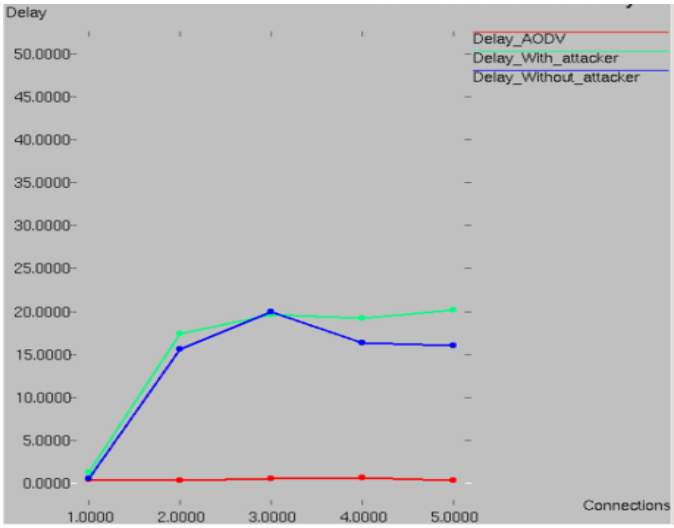

Fig. 8 Connections versus delay

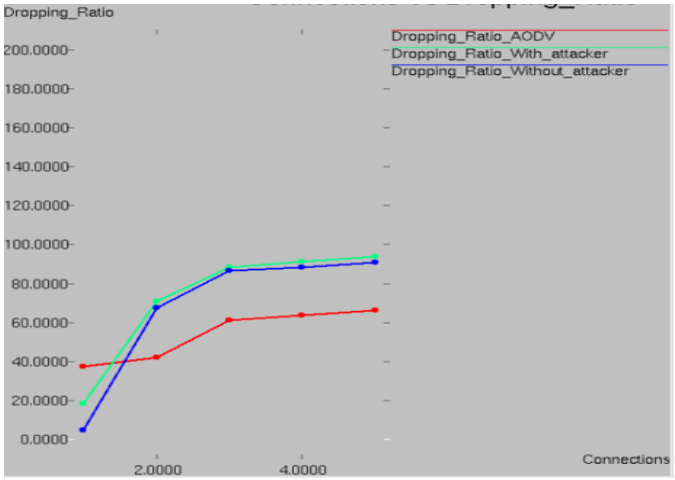

Fig. 9 Connections versus dropping ratio

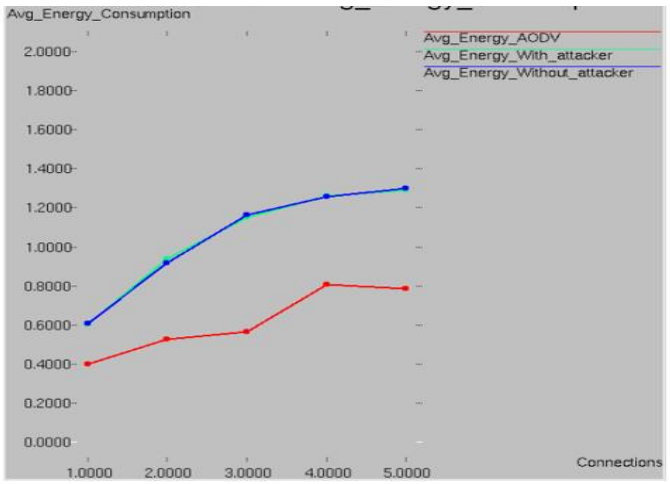

Fig. 10 *Connections versus average energy consumption*

Figure 9 shows that percentage of dropping ratio of nodes with attack and without attacker is less than 4-5 %. Figure 10 shows that average energy consumed by the node is nearly same by the node when under attack condition and even in normal condition. Energy consumed in AODV protocol is very less.

7 Conclusion

In this paper, technique for detection and removal of blackhole attacker has been presented. Due to this technique, there is increase in packet delivery ratio and delay is also decreased. Proposed mechanism discovers new route to destination by avoiding the attacker nodes. Dropping ratio under attack is around 4 percent less than in comparison to AODV protocol. Number of packet loss is also decreased. Result showed that packet delivery ratio under normal flow is 43.2935 and under proposed scheme with attack was 39.4057. End-to-end delay under normal flow is 10.5026 msec and under proposed scheme with attack is 9.4160. Throughput under normal flow is 13.8578 bps and under proposed scheme with attack is 12.6133 bps. Total energy consumption under normal flow is 79.5844 mJ and under proposed scheme with attack is 79.8618 mJ. Thus, the proposed algorithm is capable to detect and prevent the black hole attack in the wireless sensor network. Future ScopeStill there is a scope to improve the network parameter values under blackhole attack by using

other schemes to detect and prevent balckhole attack in wireless sensor network. In future present study will be extended for different topologies and varying number of attacks.

REFERENCES

[1] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[2] H. Deng, W. Li, and D. P. Agrawal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.

[3] S. Banerjee "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[4] S. Bhargava and D. P. Agarwal, "Security Enhancements in AODV protocol for Wireless Ad Hoc Network," IEEE Vehicular T echnology Conference, VTS 54TH ,2001,vol. 4,pp.2143-2147.

[5] M. A. Shurman, S. M. Yoo, and S. Park, "Blackhole Attack in mobile Ad Hoc Networks" in Proceedings of ACM of 42nd annual South-East Regional Conference, pp. 96-97,2004.

[6] P. Agrawal, R. K. Ghosh, and S. K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

[7] S. Indrasinghe, R. Pereira, and J. Haggerty, "Conflict Free Address Allocation Mechanism for Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)

[8] M. Mohsin and R. Prakash, "IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson.

[9] Y. A. Huang and W. Lee, "A Cooperative Intrusion Detection System for Ad Hoc Networks," Proceedings of 1st ACM Workshop on Ad Hoc and Senor Networks, pp. 135-147,2003.

[10] V. K. and A. Paul, "Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks", International Journal of Computer Applications (0975 - 8887) Volume 1, No. 22, 2010.

[11] M. Wazid, A. Katal, R. S. Sachan, R. H. Goudar and D. P. Singh, "Detection and Prevention Mechanism for Blackhole Attack in Wireless Sensor Network", International conference on Communication and Signal Processing, April 3-5, 2013.

[12] M. Tiwari, K. V. Arya, R. Choudhari, and K. S. Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", IEEE 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT) 2009.