An Energy Preserving Detection Mechanism for Blackhole Attack in Wireless Sensor Networks

Chunnu Lal
CSE Dept. DIT University,
Dehradun, India

Akash Shrivastava
CSE Dept. DIT University,
Dehradun, India

ABSTRACT

Wireless sensor networks (WSNs) are currently used in many application areas such as military applications, control and tracking applications, habitat monitoring applications where they face attacks already experienced by the Internet and wireless ad hoc networks. One such attack is that of Blackhole Denial-of-Service (DoS).In Blackhole attack a node captures all data packets coming to it. WSNs have Sensor Nodes which have limited energy and processing capability. With the resource limitations of WSN devices, they are particularly susceptible to the consumption and destruction of these scarce resources. Denial-of-Service (DoS) attacks have become a major threat to WSNs. It is critical challenge to develop the effective and lightweight security mechanism to detect and prevent various attacks for WSN, especially for the Denial-of-Service (DoS) attack. This paper discusses current state of art in various security mechanisms which detect and prevent the Blackhole Denial-of-Service (DoS) attack in WSNs and proposed an energy-preserving detection mechanism against Blackhole attack.

Keywords

Wireless Sensor Network (WSNs), Denial-of-Service (DoS) Attack, Sensor Node (SN), Base Station (BS)

1. INTRODUCTION

Wireless Sensor Network (WSN) is a network which have a large number of small sensor devices that sensing data to their environment and communicate with each other wirelessly. The purpose of this network is to accomplish a certain task such as environment monitoring. Each node is sending their sensing data to a center node (or sink node).The collected data is used in different domains as surveillance and monitoring habitat.Wireless Sensor Networks (WSNs) are prone to various attacks in which Blackhole a kind of Denial of Service (DoS) attack is very difficult to detect and defend.Denial-of-Service (DoS) attacks where unnecessary packets are sent causing services to appear unavailable and thus these services are denied to the legitimate sensor nodes.In blackhole 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. As a result any information that enters the blackhole region is captured and not able to reach destination causing high end- to- end delay, high energy and low throughput. Previously little amount of work is done for detection and prevention of the Blackhole attack in the WSN making its detection and prevention very crucial as per network performance is concerned.Detecting Denial-of-Service (DoS) attacks and reducing the energy consumption are two important and frequent requirements in WSNs [3,4]. Detecting phenomena such as forest fires or seismic activities implies to keep watch over wide areas. Wireless sensor networks (WSNs) are often used to achieve this watch. In WSNs, we have a large number of sensor nodes which sensing their environment and sending the collected data to the base station (BS)[10].

Because of their limited size, the sensors have very limited resources: memory, computing capability and energy must be spent with care.Other uses of WSNs include activities such as preventing chemical, biological, or nuclear threats inan area, or collecting data on a military field. Insuch sensitive domains, the deployment of a WSNbrings out strong requirements in terms of security.Various works deal with ways of preventing unauthorized access to data or with the necessary precautions to guarantee data authenticity and integrity inside the network. DoS attacks are prevent the source node to deliver its data to the destination. So confidentiality and authentication are of poor use if DoS attacks exist in the network [5, 6, 7].In this work, Optimized Weight Based Clustering algorithm (OWCA) [9]is selected as the clustering algorithm which vulnerable to blackhole DoS attack. Then proposed energy efficient security mechanism is implemented (called OWCAS (Optimized Weight Based Clustering algorithm with Security) and compared with the base OWCA taking various parameters in consideration such as energy, packet delivery ratio and end-to-end delay etc. To achieve these goals NS-2, network simulator [1]is used as a simulation tool to evaluate the performance of both OWCA and OWCAS. This simulation provides valuable insight into system performance under various operating conditions.

2. BLACKHOLE ATTACK IN WSNs

Black hole attacks occur when an intruder captures and reprograms a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station [5]. As a result any information that enters in the blackhole region is captured. Black hole attacks are easy to constitute and they are capable of undermining network effectiveness by partitioning the network, such that important event information do not reach the base stations. The network performance parameters i.e. throughput and end- to- end delay, energy are affected in the presence of blackhole nodes; throughput becomes very less and end- to- end delay increases [2].

2.1 Blackhole Attacking Scenarios Considered For Proposed Detection Mechanism

Clusters without blackhole attack show normal flow of packets. Fig.1 have 5 sensor nodes (i.e. SN1, SN2, ----- SN5), cluster head node (CH1) and a Base Station (BS). The sensor nodes sense any physical phenomenon from their environment, convert this into information and send this sensed and processed information to Cluster Head node (CH1). Sensor nodes SN1, SN2, SN3, SN4 and SN5 are reporting to Cluster Head CH1. The Cluster Head CH1 further sends data collected from sensor nodes to Base Station (BS). Fig below shows the clusterhead communication scenario if a node (SN2 in Fig. 2) acts as a blackhole attacker. All sensor nodes in a cluster sense any physical phenomenon from their environment, convert this into information and send this sensed and processed information to Cluster Head node. But if a node became as a blackhole node it sense the data from environment but does not send any data to the cluster head. Fig. 3 below shows the clusterhead communication scenario if cluster head behaves as a blackhole attacker and does not send any data packets to the base station after getting data packets from all nodes in the cluster.

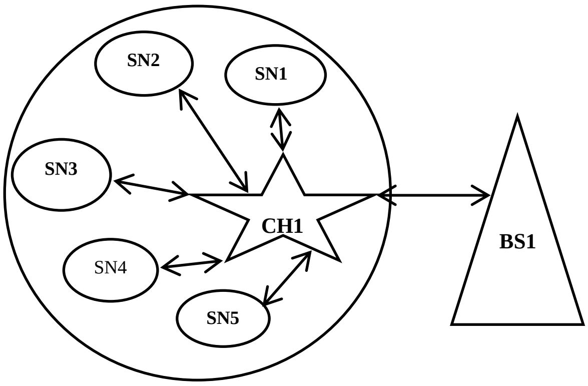

Fig.1: Cluster without blackhole attack

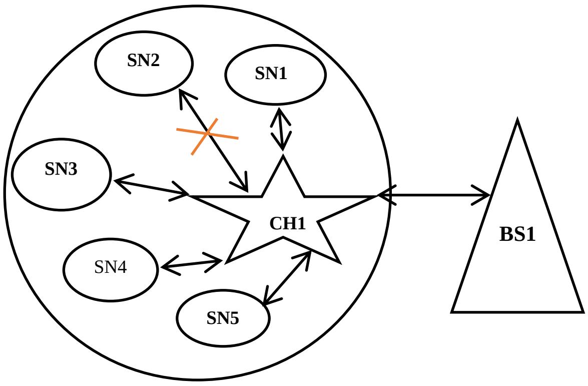

Fig.2: Cluster with blackhole attack (if a node in a cluster acts as a blackhole attacker)

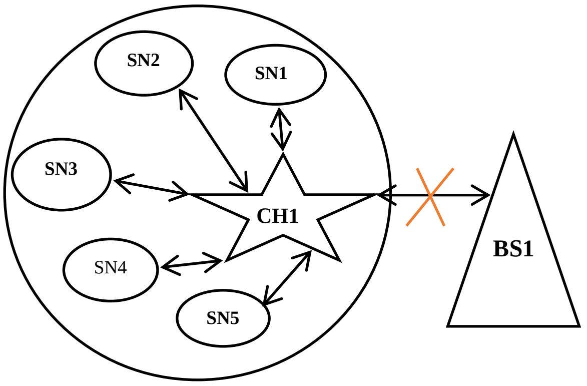

Fig.3: Cluster with blackhole attack (if cluster head acts as a blackhole attacker)

3. REVIEW THE EXISTING DETECTION AND PREVENTION MECHANISMS FOR BLACKHOLE ATTACK IN WSNS

In [4],the authordiscussed the vulnerability of the network to blackhole attack. The use of intelligent agents called Honeypots is done to detect these attacks. The Honeypots generate dummy Route Request (RREQ) packets to lure and trap blackhole attackers.

In [5], the author proposed to combat the Black hole attack by using negotiation with neighbors who claim to have a route to destination. The simulation results show that the proposed protocol provides better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

In [8], the authorproposed an efficient technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission is proposed.

4. PROPOSED DETECTION MECHANISM AGAINST BLACKHOLE ATTACK

Due to blackhole attack packets doesn’t reach the destination within time producing long delay in the network and decrement in throughput. Here this paper work proposed a blackhole attack detection mechanism which detects the blackhole attacker node.

Step1: In the proposed mechanism, first consider a sensor field consisting of set of randomly deployed sensors in a rectangular field and a base station (BS). The BS is fixed and located far from the sensors.

Step2: ACluster contains nodes which are in the communication range of each other. A node among sensor nodes acts as an attacker. Attacker node has capability that it sense data from environment but does not send it to the cluster head or base station. This attacker node may become a cluster head any time.

Step3: A cluster head (CH) is elected by the sensor nodes. Election of a cluster head (CH) is done by using OWCA (Optimized Weight Based Clustering) algorithm [9].

Step4: Now all sensor nodes are divided into different clusters. Each cluster has a CH and some nodes which are communication range from CH. When cluster is formed, cluster head is elected and it becomes the responsibility of the cluster head to detect the intruder node in that cluster. All the sensor nodes are in the control of cluster head. CH maintains a table via assigning IDs and Sequence number (Seqno) to all nodes present in their cluster as shown in Table 1. When clusters are formed, cluster heads are elected and it becomes the responsibility of the Base Station to detect if any cluster head becomes an attacker. All the cluster heads are in the control of base station. Base Station maintains a table via assigning IDs and sequence number of all Cluster Heads present in their network as shown in Table 2.

Table 1. ID and Seqno assignment to nodes in a cluster

Node	**ID**	**Seqno**
SN1	IDSN1	2
SN2	IDSN2	2
-	-	-
SNn	IDSNn	2

Table 2. ID and Seqno assignment to Cluster Heads

Cluster Head	**ID**	**Seqno**
CH1	IDCH1	3
CH2	IDCH2	3
-	-	-
CHn	IDCHn	3

Step5: Authentication process between cluster heads and base station: In authentication process, Base Station (BS) in the network sends the Authentication Packet (AP) to each of the cluster head in the network. This authentication packet contains three fields; The ID of the cluster head node, Seqno and an authentication bit that is set to make it possible to recognize the authenticity of a CH node. Authentication bit has two values 0 and 1.

IDCHn	Seqno	Auth bit

Fig. 4 Authentication packet fields

Fig. 4 shows the structure of authentication packet. All cluster heads respond to the authentication packet being sent by the Base Station (BS) with Reply Packet (RP).

IDCHn	Seqno	ACK bit

Fig. 5 Reply Packet Fields

Fig.5 shows structure of the Reply Packet (RP) which contains three fields; ID of the cluster head, Seqno and ACK bit field having a particular bit which obtained by incrementing one to the Auth bit. ACK bit is used for authentication purpose to prove that the reply is coming from the authenticated node. ACK bit has two values 0 and 1.

Authentication process between cluster head and cluster nodes: In authentication process, Cluster Head (CH) in the network sends the Authentication Packet (AP) to each sensor node in the cluster. This authentication message contains three fields; The ID of the node, Seqno and an authentication bit that is set to make it possible to recognize the authenticity of a node. Authentication bit has two values 0 and 1.

IDSNn	Seqno	Auth bit

Fig.6: Authentication packet fields

Fig. 6 shows the structure of authentication packet. All sensor nodes respond to the authentication packet being sent by the cluster head with Reply Packet (RP).

IDSNn	Seqno	ACK bit

Fig.7: Reply Packet Fields

Fig.7 shows structure of the Reply Packet (RP) which contains three fields; The ID of sensor node who is sending that packet, Seqno and ACK field having a particular bit is set which obtained by incrementing one to the Auth bit. ACK bit is used for authentication purpose to prove that the reply is coming from the authenticated node.

Step 6: Detection mechanism if a blackhole attacker node present in a cluster: Fig.1 depicts the normal flow of traffic in the WSN. Sensor nodes (SN1, SN2, -----, SN5) sense physical phenomenon, converts this into information and pass that information to the cluster head in the form of Data Packets (DPs).

IDSNn	Seqno	Data

Fig.8: Data Packet (DP)

Data Packet (DP) contains three fields; one is the ID, Seqno of node who is sending this packet. Blackhole attacker node will not send any data packet to cluster head. Cluster head will not get any data from node which is a blackhole attacker (SN2 in Fig.2). Cluster head waits for a fixed period of time (wait-ch). If the node (SN2) in the cluster doesn't send any packet even after this time period, it means an attacker exist in the cluster. The detection of blackhole node by cluster head as ID of IDSN1 is detected because it is sending the Reply Packet (RP) but not the Data Packets (DPs). CH remove attacker node from their routing table and call the procedure of clustering. Now by re-clustering another node covered the area left unattended due to attacker node.

If a cluster head become blackhole attacker: Fig.3 depicts that the cluster head (CH1) collected data from all nodes in the cluster but doesn't send any data packets to the base station. Base station waits for a fixed period of time (wait-bs). If cluster head doesn't send any of these packets even after this time period, it means the Cluster Head (CH1) is a blackhole attacker. Base station send a stop packet to the source nodes in a cluster, after getting stop packet from base station, source nodes stop sending data packets to the cluster head and remove the cluster head from their routing table. In Fig.3 cluster head CH1 becomes the blackhole node as it consumes all the Data Packets (DPs) coming from the Sensor nodes without forwarding them to the base station. The detection of Blackhole node by base station as ID of IDCH1 is detected because it is sending the Reply Packet (RP) but not the Data Packets (DPs). BS remove attacker node from their routing table and call the procedure of clustering. Now by re-clustering a new cluster head is selected.

5. ENERGY COMPUTATION ALGORITHM FOR PROPOSED MECHANISM

Both cluster head (CH) and Base Station (BS) used some energy in attack detection. The energy equations of cluster head and base station can be modified as given below.

Step 1: Initialize all the first order radio model parameters i.e. Electronics energy (E_{elec}), Amplifier energy (E_{amp}), Aggregation energy (E_{DA}).

Step 2: Calculate the energy consumed by CH node in receiving data signals from its members, transmitting data to BS, attack detection (E_{CHD}).

$$E_{CH} = (E_{elec} * k * CH_{degree} + E_{DA} * k) + (E_{elec} * k + E_{amp} * d_{tonextCH}^2 * k) + E_{CHD}$$

Where, k= number of bits transmitted, CH_{degree} = degree of cluster head, $d_{tonextCH}$ =distance between two cluster heads.

Step 3: Energy used by all CH node is

$$E_{TOT\_CH} = E_{CH(1)} + E_{CH(2)} + E_{CH(3)} + \ldots\ldots\ldots\ldots + E_{CH(NC)}$$

NC represents number of clusters.

Step 4: Calculate the energy consumed by non-CH node to transmit data signals to the CH.

$$E_{non\_CH} = (E_{elec} * k) + (E_{amp} * R_{Tx}^2 * k)$$

Where, R_{Tx} =range of data transmission

Step 5: Energy used in all non-CH node is

$$E_{TOT\_nonCH} = (N-NC) * E_{non\_CH}$$

Where, N represents number of nodes.

Step 6: Calculate the energy consumed by BS in receiving data signals from CHs, transmitting data, attack detection (E_{BSD}).

$$E_{BS} = (E_{elec} * k + E_{amp} * R_{Tx}^2 * k + E_{DA} * k) + E_{BSD}$$

Step 6: Total energy consumption is sum of energy used in all CH node and energy used in all non-CH node.

$$E_{TOT} = E_{TOT\_CH} + E_{TOT\_nonCH} + E_{BS}$$

6. SIMULATION RESULTS

6.1 Simulation Parameters

Table3. Simulation parameters used

Parameters	**Value**
Number of nodes(N)	10-100 in steps of 10
Network size(X*Y)	1500 × 1000
Transmission range(r)	250m
Electronics energy(E_{elec})	50nJ/bit
Amplifier energy(E_{amp})	100pJ/bit/m^2
Aggregation energy(E_{DA})	50nJ/bit
Simulation Time	5 s
Traffic Type	CBR(Constant Bit Rate)
Packet Size	128 bit
Number of attackers	1
Propagation Model	Two-Ray-Ground
Mobility	50m
wait-bs	.1ms
wait-ch	.1ms
Energy of a node	100 Joule

6.2 Performance Metrics[5]

To evaluate performance of OWCA and OWCAS under blackhole attack, we have used the following performance metrics.

Packet Delivery Ratio: Packet delivery ratio is a very important factor to measure the performance of routing protocol in any network. The major parameters are packet size, no of nodes, transmission range and the structure of the network. The packet delivery ratio can be obtained from the total number of data packets arrived at destinations divided by the total data packets sent from sources. In other words Packet delivery ratio is the ratio of number of packets received at the destination to the number of packets sent from the source. The performance is better when packet delivery ratio is high.

Mathematically it can be shown as-

Packet Delivery Ratio = Σ(Total packets received by all destination node) / Σ(Total packets send by all source node)

Average End-to-End Delay: Average End-to-end delay is the time taken by a packet to route through the network from a source to its destination. The average end-to-end delay can be obtained computing the mean of end-to-end delay of all successfully delivered messages. Therefore, end–to-end delay partially depends on the packet delivery ratio. As the distance between source and destination increases, the probability of packet drop increases. The average end-to-end delay includes all possible delays in the network i.e. buffering route discovery latency, retransmission delays at the MAC, and propagation and transmission delay.

Mathematically it can be shown as :

$D = {}^{n}\Sigma_{i=1} (Tri - Tsi) / n$

Where

D = Average End- to-End Delay

i = packet identifier

Tri = Reception time

Tsi = Send time

n = Number of packets successfully delivered

Average Throughput: It is the average of the total throughput. It refers to the amount of data successfully transferred from a sender to a receiver in a given time. Due to Blackhole attack packets doesn't reach the destination within time producing long delay in the network and decrement in throughput. OWCA does not having any security mechanism, due to this when a blackhole attacker node exist in the network, it consumes all the packets coming to it and does not reply for any request packet.

Mathematically it can be shown as:

Average Throughput = (recvdSize /(stopTime-startTime))

Where

recvdSize = Store received packet's size

stopTime = Simulation stop time

startTime = Simulation start time

6.3 Evaluation and Results:

Fig.11 describes the graphical view of throughput values of OWCA (Optimized Weight Based Clustering) and OWCAS (Optimized Weight Based Clustering with Security). From the above graph it can be analyzed that the throughput over number of nodes is much better in case of OWCAS as compared to OWCA.

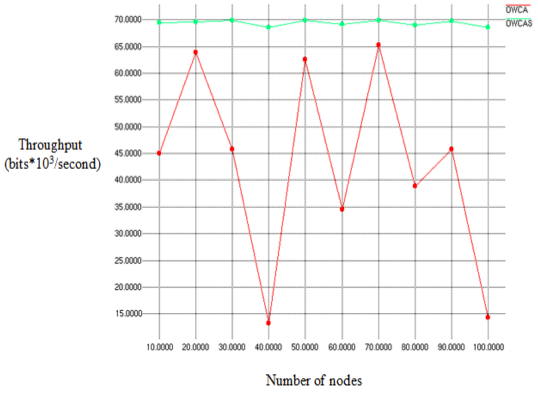

Fig.11: Throughput Comparison of OWCA and OWCAS

The reason for that in OWCA with routing does not have any security mechanism thus attacker node drops the packets in the network and decrease the throughput of the network. Hence, as the number of nodes increases the packet drop increases which subsequently results in decrement in the throughput. In OWCAS, when attacker node is removed from the network, the packets are successfully sent to the destination. Due to this, packets are successfully received at destination and throughput of the network increased. Fig.12 shows End-to-end delay values of OWCA and OWCAS with varying number of nodes in seconds.Due to Blackhole attack packets doesn't reach the destination within time producing long delay in the network. In OWCAS, when attacker node is removed from the network, then the packets are successfully sent to the destination nodes and End-to-End delay of the network decreased. Hence, as the number of nodes increases the packet drop increases which subsequently results in increase in the End-to-end delay.

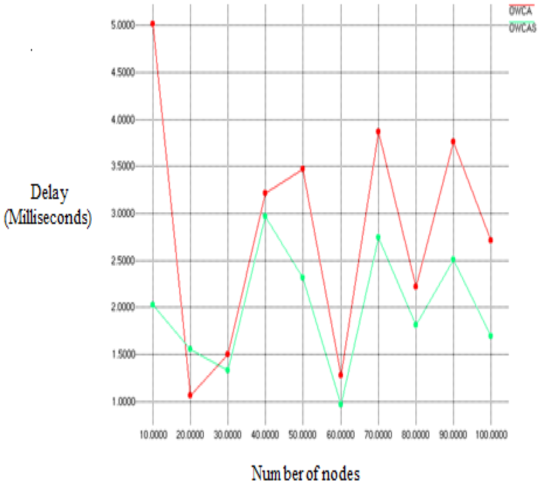

Fig.12: Delay comparison of OWCA and OWCAS

Fig. 13 shows Consumed energy values of OWCA and OWCAS with varying number of nodes. From the graph it can be analyzed that the Energy consumed over number of nodes is much less in case of OWCAS as compared to OWCA.Due to Blackhole attack packets are dropped by the blackhole node and cannot reach to the destination. Due to packet dropped by attacker, retransmission of the dropped packets will be done by source nodes and energy will be wasted.

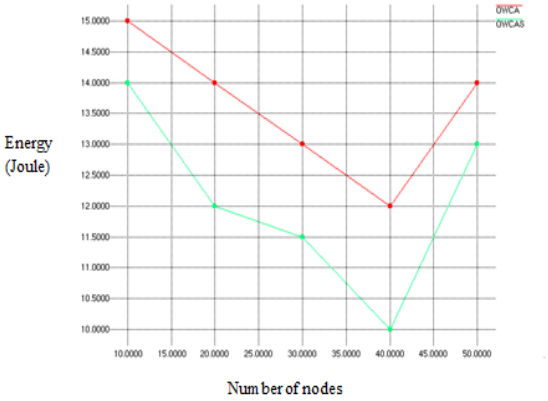

Fig.13: Comparison of energy consumed in OWCA and OWCAS

Fig.14 shows the comparison graph of Packet delivery Ratio over number of nodes between OWCA and OWCAS. From the graph it can be analyzed that the packet delivery ratio over number of nodes is much better in case of OWCAS as compared to OWCA. This is because OWCA does not have any detection mechanism for blackhole attack. Hence as the number of nodes increases the packet drop increases which subsequently results in decrease in the packet delivery ratio. In OWCAS proposed detection mechanism is applied for detection of blackhole attacker resulting blackhole attacker does not participate in re-clustering. When the attacker removed from the network, packets are successfully delivered to destination and packet delivery ratio which is the ratio of successfully received packets and sent packets are increased. Hence, packet delivery ratio is much better in OWCAS as compared to OWCA.

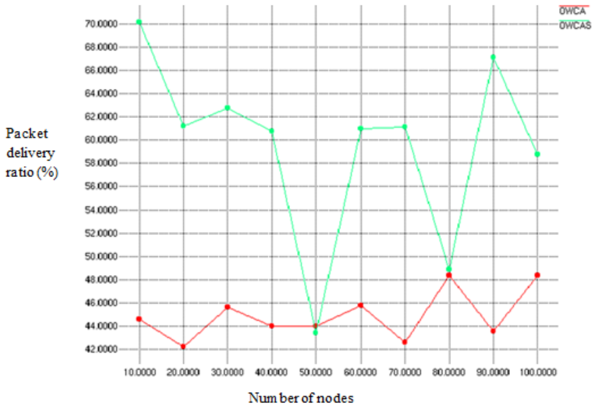

Fig.14: Packet delivery ratio comparison of OWCA and OWCAS

7. CONCLUSION

Energy of nodes in Wireless Sensor Networks (WSNs) is very limited. To reduce the energy consumption in the network, first this work used an OWCA (Optimized Weight-based Clustering Algorithm) to partition the network into different clusters. Each cluster has a Cluster Head (CH) along with sensor nodes which exist in the communication range to CH. Clustering is a method in which sensor nodes do not need to send their data directly to the Base Station (BS) because if all nodes send their data directly to BS, lot of energy of these nodes will get waste in transmission. Nodes in a cluster send data to their CH. CH collects data packets from all nodes in their cluster and send these data packets to the BS. Now if a blackhole attacker node exists in the network, this node senses the data from environment but does not send this data to the CH. The area covered by attacker node will be left unattended. If this attacker node becomes CH during simulation time, then all nodes send their data to CH. Now CH is an attacker, it takes data packets from all nodes in their cluster and does not send these collected packets to BS. Due to blackhole node, other nodes energy get wasted in packet transmission. Throughput of the network decreased because packets will not reach to the BS. End-to-end delay of the packets increased because packets will not reach at destination on time. Packet delivery ratio of the network decreased because a large number of packets will not receive successfully on the destination. So it is very important to provide a detection mechanism for blackhole Denial of Service (DoS) attack. This research work proposes an energy preserving detection mechanism against blackhole Denial of Service (DoS) attack. Proposed detection mechanism detects the node ID of attacker. Now this node will not participate again in the clustering algorithm. By removing attacker node from the network, the proposed mechanism saves node energy, increase throughput, decrease End-to-End delay of packets and increase packet delivery ratio of the network.In the presence of blackhole attacker parameters of network such as End-to-end delay, Packet delivery ratio, energy and throughput are affected. This work has observed that in the presence of blackhole attack the performance of network degraded very rapidly in clustering based WSNs. The proposed detection mechanism is capable to detect and prevent the Blackhole attacker occurring in the WSN.In future this work can be extended with varying number of attackers. OWCA clustering algorithm is utilized for partition the network into different clusters. In future another clustering method can be used for the analysis purpose.

8. REFERENCES

[1] Fall, K. and Varadhan, K. 1997. Editors ns Notes and Documentation. The VINT Project, UC Berkeley, LBL, USC/ISI, and Xerox PARC.

[2] Afrand, Agah and Sajal, K. 2007.Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach. International Journal of Network Security, 5(2):145–153.

[3] Arazil, O., Qi, H. and Rose, D. 2007.A Public Key Cryptographic Method for Denial of Service Mitigation in Wireless Sensor Networks.IEEE Sensor, Mesh and Ad Hoc Communications and Networks, pp. 51-59.

[4] Prathapani, A., Santhananr, L. and Agrawal, D. P. 2009. Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks.IEEE 6th International Conference on Mobile Adhocand Sensor System (MASS), pp. 753-758.

[5] Medadian, M., Mebadi, A. and Shahri, E. 2009. Combat with Black Hole Attack in AODV Routing Protocol.IEEE MalaysiaInternational Conference on Communications, pp. 530-535.

[6] Anastasi, G., Conti, M., Di Francesco, M. and Passarella, A. 2009. Energy conservation in wireless sensor networks: a survey. Ad Hoc Networks, ScienceDirect, 7: 537–668.

[7] Ben-Othman, J. and Yahya, B. 2010. Energy efficient and QoS based routing protocol for wireless sensor networks. Journal of Parallel and Distributed Computing, ScienceDirect, 70(8):849–857.

[8] Misra, S., Bhattarai, K., and Xue, G. 2011. BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. IEEE International Conference on Communications (ICC), pp. 1-5.

[9] Babu., N. V., Boregowda, S. B., Puttamadappa, Shivaraj. and Davanakatti, S. 2012. An optimized weight based clustering algorithm in heterogeneous wireless sensor networks. Sundarapandian et al. (Eds): ICAITA, SAI, SEAS, CDKP, CMCA, CS & IT 08, pp. 185–195.

[10] Ballarini, P., Mokdad, L. and Monnet, Q. 2013. Modeling tools for detecting DoS attacks in WSNs. Security and Communication Networks Wiley Online Library, 6(4):420–436.