Cluster Head and RREQ based Detection and Prevention of Gray hole and Denial of Service Attack in WSN

Reena Rajpoot[1] Krishna K Joshi[2]
[1]Student [2]HOD
[1,2]Department of Computer Science & Engineering
[1,2]MPCT Gwalior, India

Abstract— Wireless sensor network is a type of network which have no communications pattern for communication between nodes, any node can easily join the network and leave the network so attacks are more probable. Gray hole is one of such attacks and it is tough to detect since malicious node switches behavior between normal node and malicious node. For detection and prevention of gray hole attacks our proposed technique is based on Cluster head and RREQ based approach in WSN. In our proposed technique we select a node which has the highest energy as a cluster head and remaining node are marked as work as cluster member. For each node we decide a threshold for sending RREQ if any node generate RREQ more than threshold then we check its RREP threshold value if it's less than one than cluster head will conclude this node as a malicious node and broadcast its node id so that all other nodes also mark it as malicious node and drop the request arrive from this malicious node and for gray hole detection.

Key words: WSN, Denial of Service Attack, Gray Hole Attack, AODV

I. Introduction

Sensor networks are extremely distributed networks of tiny, light-weight wireless nodes, deployed in giant numbers to observe the surroundings or system by the measuring of physical parameters like temperature, pressure, or ratio. Building sensors are created attainable by the recent advances in micro-electromechanical systems (MEMS) technology. The sensor nodes are similar to that of a computer with a processing unit, limited computational power, limited memory, sensors, a communication device and a power source in form of a battery. In a typical application, a WSN is scattered in a region where it is meant to collect data through its sensor nodes. The applications of sensor networks are endless, limited only by the human imagination. WSNs have some special characteristics that distinguish them from other networks such a MANET. The characteristics, are listed as follows, that can lead to the use of WSNs in the real world:

- Sensor nodes possess extremely limited resources, such as battery life, memory space and processing capability.
- Routing protocols and algorithms are preferred to achieve longer sensor life.
- WSNs are self-configuring and self-organizing wireless networks.
- The topology of sensor network changes rapidly and randomly. Sensor nodes are continuously added and deleted from the network.
- WSNs have centralized approach in terms of network control. Data flows from sensor nodes towards a few aggregation points which further forward the data to base stations. Also base stations could broadcast query/control information to sensor nodes. Among the designs of WSNs, security is one of the significant aspects that deserve great attention, considering the tremendous application opportunities. Thus keeping in mind security constraints it presents a brief review of existing techniques for wormhole attack detection in network layer [1].

A. Security Goals for Sensor Networks:

The security goals are broadly categorized as primary and secondary. The primary goals are Standard security goals namely Confidentiality, Integrity, authentication and Availability. The goals belonging to secondary category are Data Freshness, Self Organization, Time Synchronization and Secure Localization.

1) Primary Goals

a) Data Confidentiality:

Confidentiality is the ability to hide messages from a passive attacker so any message communicated via the sensing element network remains confidential. This can be the foremost necessary issue in network security. A sensing element node shouldn't reveal its information to the neighbors.

b) Data Authentication:

Authentication ensuring the message's dependability by distinguishing its origin.

c) Data Integrity:

Data Integrity in sensor networks is required for ensuring the data reliability referring to the ability to verify that the message has not been tempered with, altered or modified. Though the network has confidentiality measures there's still a break that the info integrity has been compromised by alterations.

d) Data Availability:

Availability determines whether or not a node has the power to use the resources and whether or not the network is offered for the messages to speak. However, failure of the bottom station or cluster leader's convenience can eventually threaten the whole device network. Therefore convenience is of primary importance for maintaining associate degree operational network.

2) Secondary Goals

a) Data Freshness:

Even if Data Confidentiality and Data Integrity are assured, there's a requirement to confirm the freshness of every message. Informally, knowledge freshness suggests that the information is recent, and it ensures that no previous messages are replayed. To unravel this downside a nowadays or another time-related counter, is another into the packet to confirm knowledge freshness

b) Self-Organization:

A wireless sensor network is typically an ad-hoc network, which needs each device node be independent and versatile enough to be self-organizing and self-healing in line with completely different things. There's no fastened infrastructure out there for the aim of network management during a device network. This inherent feature brings an excellent challenge to wireless device network security. If organization is lacking during a device network, the harm ensuing from AN attack or maybe the risky surroundings is also devastating.

c) Time Synchronization:

Most sensor network applications believe some variety of time synchronization. Sensors may need to calculate end to end delay of a packet because it travels between two pair wise sensors. A lot of cooperative sensor network could need cluster synchronization for tracking applications.

d) Secure Localization:

Often, the utility of a sensor network can accept its ability to accurately mechanically find every sensor within the network. A sensor network designed to find faults would like correct location data so as to pin purpose the placement of a fault. An aggressor will simply manipulate non-secured location data by news false signal strengths, replaying signals [2].

II. Working of AODV Routing Protocol

When source wants to communicate with destination source broadcast a Route Request packet to all its neighbours this packet consists of sequence number generated by source node if any of neighbour s not having direct path to destination then they will again retransmit this Rout Request packet to its neighbours, So there is possibility of loop formation &retransmission of same packet to same node. To avoid this, intermediate node checks the sequence number of packets. if the packet is not duplicate then only it add its own identifier in sequence number & then forward the packet the destination node when receives the Rout Request packet then it sends back rout reply packet with higher sequence number along the reverse route which is followed by Rout Request packet. When source receives Rout Reply packet at that time source can send data to destination. Next important thing is maintenance of route. If a node detects any failure then it sends Route Error message to source [3] Fig.1 will explain the working of AODV with example

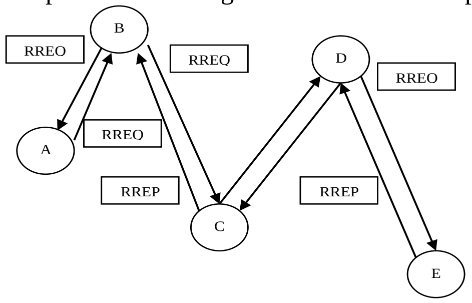

Fig. 1: Working of AODV

There are 5 nodes present in WSN A, B, C, D, E. as shown in Fig.1. Circle shows the limited communication range of each node. Node B wants to communicate with node E then B will broadcast RREQ to all its neighbours i.e. A & C. Now node A does not have direct path to destination, so it rebroadcast RREQ to its neighbour. It is received by B itself & discards it. On the other hand node C is there if it has greater sequence number than RREQ then it discards RREQ and replies with RREP having higher sequence number if not then it update sequence number in routing table and re-forward RREQ packet to node D. Now node D has path to node E so it send back RREP packet with greater sequence number and the path B->C->D->E is selected for communication. Now suppose there is a node which forwards wrong routing information in network then route discovery Process is difficult as shown in following example. In figure S node is source and E is destination. Node S broadcast the RREQ packet to node A and B .they don't have path to destination so B retransmit RREQ to Node D. Node A retransmit RREQ to node C. Now node D has the path to destination so it sent back RREP packet with higher sequence number indicating that i have path to destination. On the other hand node C is a malicious node which sends wrong routing information it does not have path to destination then also it replies to node A with fabricated higher sequence number indicating that I have path to destination but actually this is wrong information. Now source node observe that RREP coming from node C is having greater sequence number than RREP coming from Node D so it will select path which goes through node C. During data transfer this malicious node can drop some or all data or can alter data which causes problem in network operation this is nothing but security attacks.

There can be two kinds of attacks

- Passive attack
- Active attack

A. *Passive Attack:*

This type of attack does not disturb the network operation. In this the aim of attacker is only obtain the information being transmitted without making any changes in that message so it will violate the message confidentiality detection of these type of attacks is difficult. Powerful encryption mechanism can avoid these types of attacks

B. *Active Attacks:*

This type of attack badly affect on network operation. In this attacker node creates attack by making changes in data packet or by dropping data packets or by adding some wrong data in packet. Gray Hole and Black Hole attacks are active attack. [4]

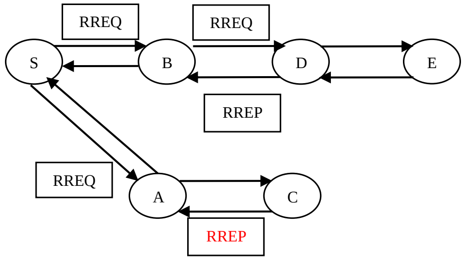

Fig. 2: Working of AODV in presence of malicious node

III. Denial of Service Attack

This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks [5]

DoS attack takes place at different layers of WSN. Thus, by DoS attacks the network connectivity is critically affected as consequences challenging the network functionalities, namely delivery of data and control packet. Additionally consuming the system resources, such as battery power and bandwidth and additionally isolates legitimate users from accessing data or services within the network because of the malicious behavior of the node DoS attacks is also initiates all layers.

In transport layer a malicious node,

1) A malicious node transmits a huge volume of SYN (Synchronization) packet destined to the target node. These SYN packets may be from spoofed source addresses of out of reach nodes. If the attacker is spoofing source addresses from nodes that are out of reach, the target node can arrange to complete the session by transmitting back SYN ACK (Acknowledgement) packets which is able to never be acknowledged or reset.

In network layer a malicious node,

1) Broadcasts huge volume of packets to the victim to avert victim or the entire network by setting up or continuing transmission and consuming victim's bandwidth and battery power.
2) Take Parts in a route but simply dropping certain data packets.
3) Sends fallacious route updates.
4) Replicas of a transmitted packet and later transmits out the replicas continually and persistently to the victim's buffers draining the power supply or consuming bandwidth.
5) Denying the availability of the current path or purposely transmits data packets to the incorrect destination.

In Physical and Media Access Control (MAC) layer a malicious node,

1) Can successfully cut off wireless connectivity between nodes by sending continuous radio signals such that other legitimate users are denied from accessing a particular frequency channel by keeping that channel busy.
2) Transmitting jamming radio signal so that collision with legitimate signals takes place.

IV. Gray hole attack

Gray Hole attack is an active type of attack where attacking node first agrees to forward packets then fails to try to so, that ends up in dropping of messages. Gray Hole attack is one in all the attacks in network layer that comes beneath the class of active attacks in WSN. In gray hole attack have a tendency to can't predict the chance of losing knowledge. In gray Hole Attack a malicious node refuses to forward particular packets and just drops them. The packets originating from one source address or a spread of source addresses by selection drops by attacker and forwards the remaining packets. Gray Hole nodes in WSNs are terribly dominant. Each node maintains a routing table that stores following hop node information. When a source node desires to route a packet to the target node, it uses a selected route if such a route is out there in its routing table. Otherwise, nodes begin a route discovery method by broadcasting Route Request (RREQ) message to its neighbours. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node. A Route Reply (RREP) message is distributed back to the source node once the RREQ reaches either the destination node itself or the other node that encompasses a current route to destination [6].

V. Literature Survey

Dharini et al (2015) in [7] proposed a detection scheme for detecting flooding attack and gray hole attack. The proposed detection mechanism consumes less energy and also there is not much change in the throughput, packet delivery ratio and delay when compared to ideal hierarchical wireless sensor network scenario. Thus the proposed detection mechanism is light weight in nature, hence proving its efficiency. A light weight energy prediction algorithm is implemented to observe the abnormality of the nodes' behavior. Prediction accuracy obtained is quite high thereby the detection accuracy is also achieved. The proposed detection scheme will increase the detection ratio thereby achieving energy saving. By effectively detecting and isolating the intruders from the network, the network's lifetime is also enhanced.

P.V.Sawant et al (2015) [8], introduced a detection framework for DoS attack utilizing elements namely normalization and triangle area map procedures under Multivariate Correlation Analysis (MCA) which are helpful for precise movement depiction. Traffic Characterization is finished by separating geometric connection between's system movement aspects. DoS attack detection framework that is capable of identifying both known and unknown DoS attack since it actualizes the guideline of anomaly based discovery for attack redesign. Viability of the framework is expanded on account of its capacity to take in the new examples of authentic system traffic. Triangle-area based system is utilized to accelerate the procedure. Discovery of SQL infusion is additionally presented in the framework for security motivation.

Avenash Kumar et al [9], this technique consist of three major steps foe efficient measure for detecting as well as preventing the attack. The first step is to store the reply packet second step is checking the hop distances of the node that is found to be suspected and the last step is to reject the reply packet. For recognizing the suspected node, the respected neighbour of previous node and the node that is suspected verifies the two hop distance node capability to reach the destination.

Hizbullah Khattak et al [10], presented a solution for avoiding the occurrence of black and gray hole attacks. For this they eliminate the first encountered path and select the second minimal route for communication. Whenever source node receives the reply messages from various nodes that are connected with destination, it simply discards the first reply message arriving from any intermediate node that is connected with destination for the avoidance of the attacks.

DeepaliA Lokare et al [11] slight changes are introduced in the AODV protocol and a novel algorithm Credit Based AODV (CBAODV), where a value known as credit value is assigned to every node for its neighbouring nodes. The value is incremented whenever a request packet (RREQ) is received and decrement on receiving the reply packet. Nodes detect the presence of gray hole whenever they encounters a negative value by one of its neighbours and discards all the present routes that are established by the suspicious nodes for its table.

VI. PROBLEM STATEMENT

Existing work based on only energy consumption and cluster head selection scheme, each time when we change cluster head and transfer routing table in this procedure memory consumption high and increase memory overhead which is drawback of wireless sensor network in on the basis on energy consumption we cannot declare any node as a malicious.

VII. PROPOSED WORK

Wireless sensor network is a collection of sensor nodes which is organize into a synchronize manner. Each node has ability of processing skills and contains different type of memory. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Sensor network are popular and used in different area like medical monitoring, environment monitoring this type of network use in battle field, habitat monitoring, automation, agriculture, and security. There is different type of sensor network which is use in different area sensor network like biometric sensors, optical sensors, gas sensors, physical sensors, environmental sensors. Design or implementation of sensor network is most popular for research now days, energy of node is one of the hot area of research in sensor network because sensor nodes have small life time, because nodes have very small amount of battery power if they work like ad-hoc network it reduce more energy and in our network area number of dead nodes increase or performance of network decrease existing work depends on node energy and cluster head selection method if cluster head become intruder node then there is no method to identify node malicious behavior. For detecting and preventing malicious behavior of node we propose a technique Cluster head and RREQ based malicious behavior detecting and preventing approach in WSN. In our propose work we select a node which have highest energy as a cluster head and remaining node work as a cluster member, for each node we decide a threshold for sending RREQ if any node generate RREQ more than threshold than we check its RREP threshold value if it’s less than one than cluster head broad cast the node id of this node so that all node drop the request arrive from this malicious node, and for gray hole detection if node does not send RREP frequently then for checking its malicious behavior we send RREQ which is generate by flooder node if any node reply positively so same as we do with this malicious node and drop the route which is generate by this malicious node.

A. Proposed Algorithm

```
–   Step1: initialize network();
–   Step2: create clusters c1,c2...,cn .
–   Step3: If(node energy> energy of all nodes )
    {
            Select the Node as cluster head
    }
  else{
            Mark the Node as cluster member
  }
–   Step5: Cluster head measure RREQ and RREP for
    messages coming from each node
–   Step4:  If(RREQ > threshold  && RREP < = 1)
    {
            Mark the sender node as malicious node;
            drop the route generate by this node.
     }
     else {
            Mark the sender node as normal node
    }
–   Step5: If (sender node does not send RREP
    frequently) Send RREQ generated by flooder node
–   Step6: check ACK count.
–   Step7: If (ACK count > threshold count)
            Mark the sender node as malicious node;
            drop the route generate by this node.
    }
    else{
            Mark the node as normal node
    }
–   Step8: Broadcast the node Id of malicious node
```

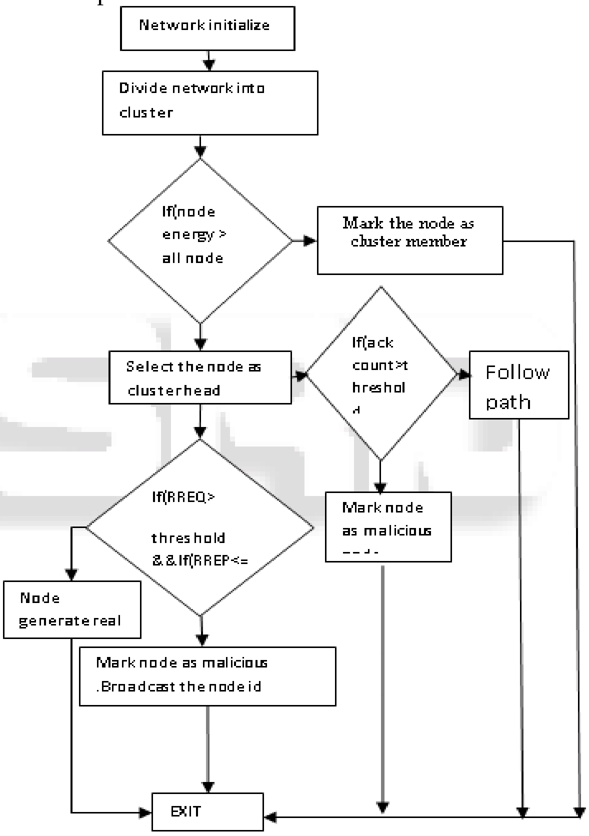
Network initialize
Divide network into cluster
If(node energy > all node
Mark the node as cluster member
Select the node as clusterhead
If(ack count>t hreshol d
Follow path
If(RREQ> threshold &&If(RREP<=
Mark node as malicious
Node generate real
Mark node as malicious .Broadcast the node id
EXIT

Fig. 3: Flow chart of Proposed Model

VIII. SIMULATION AND RESULTS

The simulation is carried out on Network Simulator-2 (ns-2).

The number of node used is 50 nodes. The xy-dimension is of size 2000X2000. The initial energy is 0.5joules. The start of simulation is 0.1miliseconds and the end of simulation is 100.0miliseconds.

Parameters	Values
XY Dimension	2000X2000
Number of nodes	50
Initial energy	0.5joules
Start simulation	0.1miliseconds
End simulation	100.0 milliseconds

Table 1: List of Simulation Parameters

A. *Throughput:*

Per second transfer of data on bandwidth is known as throughput. The Fig.3 represents a throughput graph between base approach and proposed approach. The throughput of the proposed approach is good than the base approach.

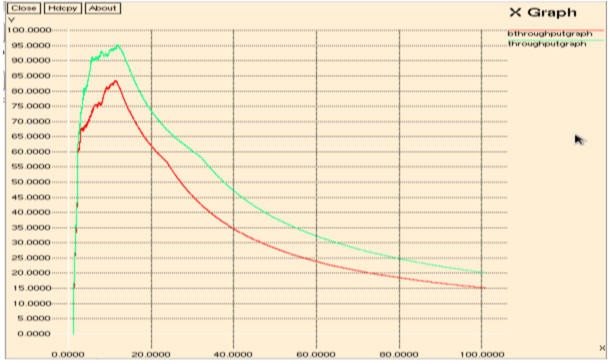

Fig. 4: Throughput graph between Base and Proposed

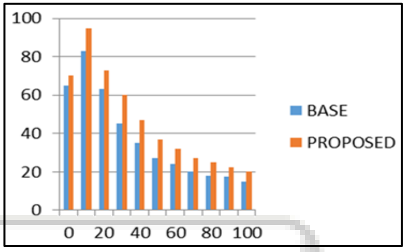

Fig. 5: represents a throughtput Bar Chart between base approach and proposed approch.x-Axis represent a time and y-Axis represent a throughput.

X-Axis—Represent Time
Y-Axis— Represent Throughput

B. *Packet Delivey Ratio:*

Defined as the ratio of packets delivered from source to destination. The Fig.4 represents a PDR graph between base approach and proposed approach. The packet delivery ratio of the proposed approach is good than the base approach.

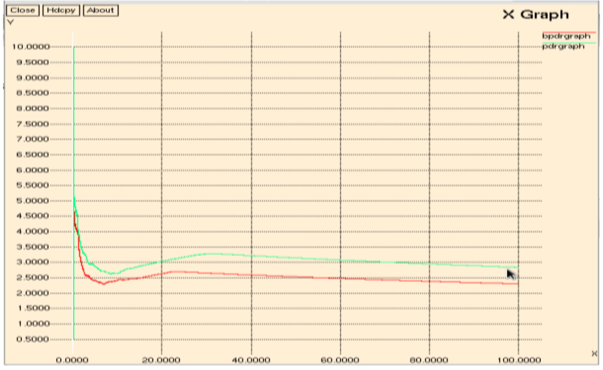

Fig. 6: PDR graph between Base and Proposed

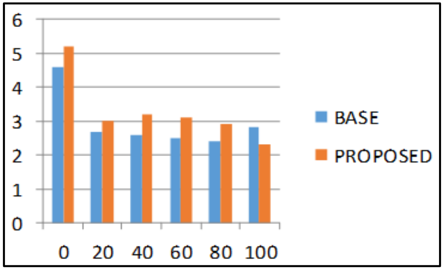

Fig. 7: represents a packet delivery ratio Bar chart between base approach and proposed approch.x-Axis represent a time and y-Axis represent a pdr

X-Axis—Represent Time
Y-Axis— Represent PDR

C. *Routing Overhead:*

The routing overhead is defined as data of data and flooding of data in the network transmitted by application, which utilizes a bit of accessible transfer rate of communication protocols. The Fig.6 represents a routing overhead graph between base approach and proposed approach. The overhead of the proposed approach is more than the base approach. Since the overhead should be minimum but as the routing increases in the proposed work the overhead also increases.

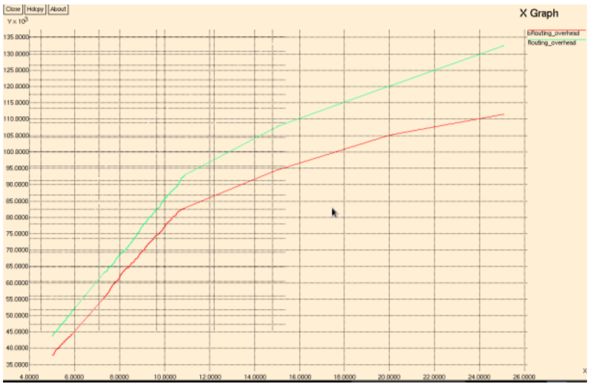

Fig. 8: Routing Overhead between Base and Proposed

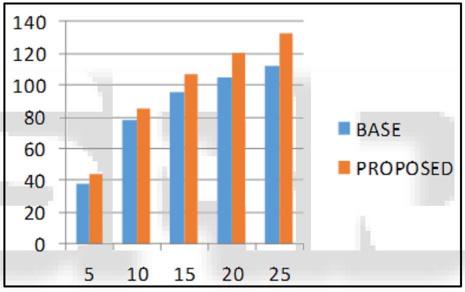

Fig. 9: Represents a Routing overhead Bar chart between base approach and proposed approch.x-Axis represent a time and y-Axis Overhead*10000

X-Axis—Represent Time
Y-Axis—Overhead *10^3

IX. Conclusion

Design or implementation of sensor network is most popular for research now days, energy of node is one of the hot area of research in sensor network because sensor nodes have small life time, because nodes have very small amount of battery power if they work like ad-hoc network it reduce more energy and in our network area number of dead nodes increase or performance of network decrease existing work depends on node energy and cluster head selection method if cluster head become intruder node then there is no method to identify node malicious behaviour. For detecting and preventing malicious behaviour of node we propose a technique Cluster head and RREQ based malicious behaviour detecting and preventing approach in WSN. In future, apply this approach on different routing protocols and will enhance the routing overhead.

References

[1] Vaishali Pahune, Sharda Khode;” Security Issues, Attacks and Challenges In Wireless Sensor Network”.

International Journal Of Engineering Sciences & Research Technology, 2015

[2] Vikash Kumar, Anshu Jain and P N Barwal; “Wireless Sensor Networks: Security Issues, Challenges and Solutions”. International Journal of Information & Computation Technology., 2014

[3] Elizabeth M. Royer, Charles E. Perkins “An Implementation Study of the AODV Routing Protocol”, Wireless Communications and Networking Confernce, 2000. WCNC., 2000 IEEE (Volume:3)

[4] Mahendra Kumar, Ajy Bhushan, Amit Kumar, “A Study of wireless Ad -Hoc Network attack and Routing Protocol attack” Volume 2, Issue 4 , April 2012

[5] M. Gunasekaran, K. Premalatha; “A Survey on DoS Attacks and Countermeasures in Mobile Ad Hoc Networks”. International Journal of Advanced Research in Computer Science, 2010

[6] J. Sen, M. G. Chandra, Harihara S.G., H. Reddy, P. Balamuralidhar “A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks” ICICS 2007

[7] N. Dharini, Ranjith Balakrishnan And A. Pravin Renold;” Distributed Detection Of Flooding And Gray Hole Attacks In Wireless Sensor Network”. International Conference On Smart Technologies And Management For Computing, Communication, Controls, Energy And Materials (ICSTM),2015

[8] P.V.Sawant, M.P.Sable, P.V.Kore, S.R.Bhosale; “A System For Denialofservice Attack Detectionbased On Multivariate Correlation Analysis”. Multidisciplinary Journal of Research in Engineering and Technology,2015

[9] Avenash Kumar, Meenu Chawla;”Destination based group gray hole attack detection in WSN through AODV”. Internationl Journal of Computer Science,2012

[10] Hizbullah Khatt ak, Nizamuddin, Fahad Khurshid, Noor ul Amin “Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash.” IEEE, 2013

[11] DeepaliA.Lokare,A.M Kanthe,Dina Simunic, “Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in WSN”, International Journal Of Computer Applications, 2014