Black hole Attack Aware Secured Efficient Dynamic Source Routing Protocol for MANET's

Mari venkatesh.C[1] (PG Scholar),
Chandy College of Engineering, Tuticorin, Tamilnadu.
mari_venkatesh007@yahoo.co.in.

Ashok Kumar M[2] (AP/dept of ECE)
Chandy College of Engineering, Tuticorin, Tamilnadu.
ashgct@gmail.com

***Abstract*-A mobile Ad-hoc network is one of the self behavior networks that form the temporary network structure with the help of many mobile nodes without the existence of the central access point. The MANET used in many application such as disaster areas and military communication etc. In this MANET's dynamic node movement makes the changes in the network topology rapidly. According to the dynamic movement MANET faces the many challenging task in the field of protocol security such as black hole attack and other DOS related attacks. In this paper presented the Secured Efficient Dynamic Source Routing(EDSR) protocol for avoid Black hole attack .This work mainly based on to prevent the black hole attack by using the prevention method. The used prevention method is Intrusion Detection System with Anti Black hole Mechanism in EDSR. This preventsmethod designed by compare the suspicious value with the predefined threshold. The suspicious value exceeds the predefined value of threshold means that IDS node establishes the block message to its neighboring nodes and prevent from the attack. In this work also evaluate the performance of the network with prevention and without prevention. Hence proved the secure EDSR produce the best outcome compared with unsecured EDSR.**

Key words: ABM, Black hole attack, EDSR, IDS, Malicious node. MANET.

I. INTRODUTION

A mobile ad hoc network means that the set of mobile nodes that share the data information with other nodes without the existence of essential network device such as essential access router. In Mobile Ad hoc Networks (MANET) the network communication performed with the help of intermediate nodes. In MANET major issue is finding the shortest path to reach the destination. This problem solved by using the MANET routing protocols. The MANET routing protocols are classifies into two types :(i) Proactive routing protocol, (ii) Reactive routing protocol. This network used in so many purposes such as disaster revival, mobile services, etc.

Proactive protocol maintains the routing table for each and every node and every node searches the routes with the help of the intermediate nodes. In particular routing based on the nearest node routing table. It also called as table driven routing protocols.The reactive routing protocol initiate the route determine progression when the two nodes planned to transmit the data between them. So only it called as on demand routing protocols. Some on demand routing protocols are AODV and DSR.

A. DSR (Dynamic Source Routing protocol)

DSR is one of the reactive routing based protocols which are able to manage a mobile ad-hoc network without the use of episodic table-up gradation process, such as DSDV protocols. DSR was deliberately designed for use in multi-hop wireless ad hoc networks. According to the structure of Ad-hoc network need to reducing the bandwidth during the dynamic topology changes. In this technique to locate a route is only after the demand receiving from the source. DSR has two phases [11];

- Path finding
- Path main tance

Path finding process:

In DSR the source node is used to find out the full path from the source to the destination node and update the information of the in-between route nodes in the routing table. This path finding process done with the help of route request and route reply process from source to destination.

Path maintenance:

In DSR every node confirms its existence and also knows the next hop information. In this process each node forwards the information only once. Suppose a packet not reach the desire node, then that packet is retransmitted after the long times until an authentication is received from the next hop. The retransmission gets failure response means that a route error message is sent to the source node that can remove route from source route cache. So the source node needs to determine another route to achieve the target with the help of route cache of the source node. The route not presents in the route cache means that it broadcast the route error message [11].

B. Security

The behavior of mobility for mobile ad hoc networks needs additional mechanism for providing security. The network topology is highly dynamic as nodes regularly connect or leave the network. According to its dynamic nature, mobile nodes need security when it moves from one place to another. Hence, a powerful security solution is required to achieve protection and high network performance. More secure routing protocols have been recently presented by researchers. An attack problem is one of the famous security issues. A black hole attack is most popular attack in the network communication. In the process of black hole attack a malicious node occupy the routing protocol and establish another route to reach the

destination node. But the malicious node drops the hello packets and not forward packets to next hop of neighbors. Then the result of the network performance is decrease and it establish the other attacks such as flooding attack and warm hole attack due to the malicious node. The security explanation encompasses all three components of prevention, detection, and reaction. So the security problems are solved by selecting the appropriate methods of prevention, detection and reaction [1] [9].

II. RELATED WORK

Mohammad A. Mikki et al [6] presented the concept about Energy Efficient Location Aided Routing protocol. In this work developed based on the Location Aided Routing protocol. In this concept the coverage area divided into six equal parts and placing one reference base station at the center of the coverage area. The reference base station used to store the information about the mobile nodes and the data communication through the reference base station only. For that reason only it produce the good network performance.

The comparison of the routing protocols based on the network parameters. The compared protocols are EDSR, DSDV, AODV and DSR protocols. In this model EDSR routing process construct based on the DSR protocol. In this comparison appraise the performance such packet loss, delivery ratio, delay, through put and control over head. From that evaluation the DSR based EDSR produce the best performance.

Harmandeep Singh et al [2] reviews the special effects due to the black hole attack and appraise the performance of the routing protocol. Rahul Sharma et al [7] presents the work against the black hole attack in AODV network by done some modification in AODV routing process. SwatiJain et al [8] review about the black hole attack and various prevention techniques. Vipan Chand Sharmaetal [10] propose the black hole detection method by modifying the AODV protocol. In this method we add the two things, a new routing table RR-Table (Request Reply), a timer WT (Waiting Time) to the data structures in the AODV Protocol. Mayuri Gajera et al [4] presented one the method to prevent the data from black hole attack by using Identity-based Key Management (IKM). Ketan Chavda et al [3] review the detection and prevention method of the black hole attack such neighborhood based method, DPRAODV (Detection Prevention Reaction AODV) scheme. Swati Jain et al[9] evaluate the performance when black hole attack and flooding attack present in the MANETs. Ming-Yang Su et al[5] proposed the prevention method of black hole method using IDS(Intrusion detection system) with ABM(Anti Black hole Mechanism) in AODV routing protocol. Fan-Hsun Tseng et al [1] survey against the various method of preventing the black hole method such neighborhood based method, Time based threshold detection scheme, Next hop information scheme and IDS based system on ABM.

III. PROPOSED WORK

A. Overview of current work

The main aim of the current work to secure the DSR based Efficient Dynamic Source Routing protocol. In this protocol secure from the attack during the communication between the two nodes. Mainly focused to prevent the protocol from the black hole attack and flooding attack with the help of malicious node detection. In that work a method to preventing the DSR based EDSR from attack. Thus the method is

- IDS (Intrusion Detection System) on ABM(Anti Black hole Mechanism).

B. Design Method

In fig (2) the design method consist of environment settings, node creation, node clustering, ids node setting , attack creation, attack detection by using ABM, and sending black message to its neighboring and performance evaluation

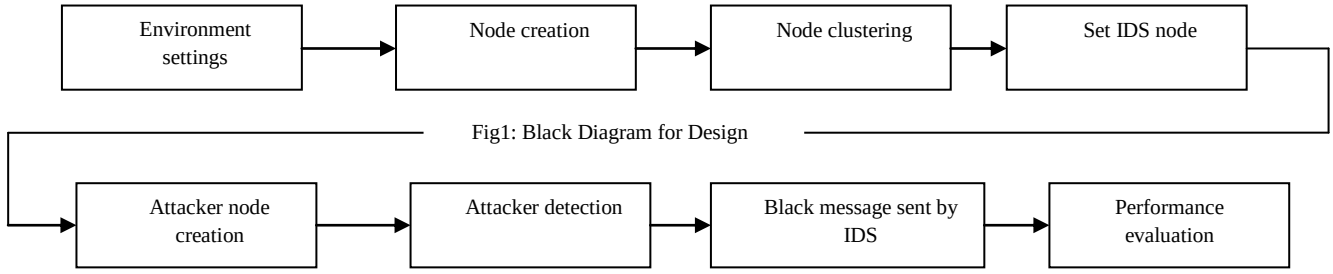

Fig1: Black Diagram for Design

C. Environment Settings

In this work developed in wireless environment. The wireless environment settings consists of channel type , propagation model, network interface , Mac version, type of queue, length of queue and type of antennas. These settings are important for designing the network.

D. Node creation

Node creation consists the number of nodes, nodes location with x and y co ordinates, node size, packet size, mobility value in x and y co ordinates, node setting time and node color and description such source node, destination node and base node.

E. Node clustering

Node clustering means that nodes are clustered based on the similarity of distance and x and y values. Before that need to know the information about the neighboring node by means of sending the hello packets or route request and route reply packets. Distance calculation using the equation (1)

$$D=\text{Sqrt}\left((x_2-x_1)^2+(y_2-y_1)^2\right)\ldots\ldots (1)$$

D-Distance between two nodes.

X_1, X2- Node 1 and Node 2 values of x respectively.Y_1, Y2- Node 1 and Node 2 values of y respectively.
After calculating the distance between the nodes then the cluster formed based on the similarity of the region and distance.

F.IDS (Intrusion Detection System)

An IDS (Intrusion Detection System) monitors the system activities for malicious actions or rule violation and produces reports to a management station. The intrusion detection technique first developed in the wired network and has become very important security solution for the wired network and mobile adhoc networks [5].

G. Intrusion Detection System in EDSR

In fig (2) shown the arrangement of the intrusion detection system in EDSR. In EDSR the coverage area can be divided into six equal parts. The IDS node was preset in the every part of the clustering area. Every IDS node progress the abnormal detection process with the help of nearest node information. The neighboring IDS nodes can share their investigation results with other IDS nodes in between the coverage range. The cooperation between IDS nodes generally occur when a certain IDS node detects abnormal information but that information not enough to prove the abnormal condition. In this situation, the IDS node has requirement of abnormal node detection in the communication range and also performs searches to their security logs in order to track the possible traces of the intruder.

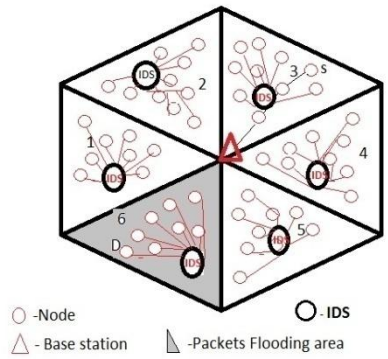

Fig 2: IDS arrangement in EDSR

H. Detection and Correction method

In this work define the malicious node detection and security method by modifying EDSR protocol and using the IDS with ABM (Anti Black hole Mechanism).

I. Anti-Black hole Mechanism (ABM)

In [5] this concept mainly used in IDS for estimate the suspicious value from misbehaver node communication. The misbehave node send the amount of false reply and false request to the source based on that request or reply whether it exceeds the predefined value or not. If it exceeds the predefined value, it generates the prevention method.

Procedures of ABM

It consists of three main procedures (i) Procedure of ABM for Route Request. (ii) Procedure of ABM for Route Reply. (iii) Procedure for Block message.

Procedure of ABM for Route Request (RREQ)

This procedure executed when the IDS node sniffs a RREQ transmitted by node N.
It based on following parameter
Route Request table (RQT), Entry of Request table.
Step 1: search the entry of RQT with RREQ
If ((source, destination, source sequence)) = ((sourceRREQ_ip, Destination RREQ_ip, source sequence RREQ_ip)).
Step 2: if the entry exists in ROTE.
That node must store in the broadcasting node filed in the table.
Step 3: Check the hop counts if (hop count of RREQ > hop count of ROTE).
Hop count of RREQ is maximum and ROTE expiration time increased by 3.
Step 4: Otherwise create the RQTE and store the RREQ in the new entry and increase the Expiration time by 15 ms.

Procedure of ABM for Route Reply (RREP)

This procedure executed when the IDS node sniffs a RREP transmitted by node N.
It based on following parameter
Route Request table (RQT), Entry of Request table(RQTE),Route Reply(RP), Entry of Reply table (RPT), Suspicious Node (SN), Entry of Suspicious Node Table (SNTE).
Step 1: check if the node is not a destination node.
Step 2: search the entry of RQT with RREP.
If ((source, destination)) = ((sourceRREP_ip, Destination RREP_ip,))
Case 1: if the entry not exists in ROTE.
Then drop the RREP
Case 2: if the entry exists in ROTE and the node present in the broadcasting field. Then drop the RREP
Procedure of Block message
Case 3: if the entry exists in ROTE and the node not present in the broadcasting field.
Search SNT for entry with node ID=N;
If the entry exist in SNTE
Check whether the node is active or inactive
If active means drop the RREP.
Otherwise increase the value of suspicious
If (suspicious value >= predefined value)
Then the status will be active and broadcast the block message. Otherwise create new SNTE table and store the node and status.

IV. SIMULATION SETUP PROCEDURE

The simulation work done with the help of Network Simulator. In this simulator used to animate the network operation. The operation can be performed by defining the node configuration and the simulating setup. The node configuration parameter follows

- *Parameter configuration:* Channel set as the wireless channel, propagation model set as the two ray ground model, network interface set as the wireless physical medium, Mac type set as the Mac version 802.11, queue interface set as CMUPriqueue, antenna type set as Omni directional for gathering the full area unique coverage, queue length set as 50 for each node to store the data, set number of node as 50, routing protocol as Dynamic Source Routing protocol and set the overall simulation area as (1600, 1200).
- *Nodes position settings:* After setting the node configuration need to set the node position within the range of simulation area. Then the simulation area can be divided into six equal parts based on the X and Y values. For the node movement needs to set the random movement function for each and every node that movement done in both x and y direction up to 100m distance and this node movement operation execute every 5 ms. Difference between two nodes set as 250 m. The reference base station placed at the center of the area.
- *Connection settings:* The reference base station used to store the information about the whole node and the communication done through the reference base station. If the node needs to communicate with other node that needs the traffic model, so the traffic model is established using the User datagram Protocol attach to the source nodes. Then define the size of the packet as 512KB, interval set as .06ms and constant bite rate error as 100 KB per Sec and null agent attach to the destination node and establish the connection between the source node and destination node or sink node.
- *IDS creation:* At that time of IDS node creation need to check the IDS node whether it's present in the source node list and the destination node list or not. Suppose it present in the source or destination list means it consider as the normal node if it's not present means act as the IDS node. After placing the IDS node that node calculating the nearest node information by using neighbor distance calculation using eq (1).Then the calculated details should be stored in the IDS neighbor table.
- *Attacker node creation:* After that the two attacker node is created and it places particular interval time of simulation. The attacker node interrupts the source node and it sent the immediate route reply with an abnormal sequence number and hop count or the node sending the false message to the source. At first time it's not considered as abnormal node, but the source node not sending the reply. The IDS node monitors the misbehave node with the help of the suspicious node table. Then the IDS node initializes the ABM (Anti Black hole Mechanism) process.
- *ABM Process: In* that process it calculates the amount of false reply from the black hole node and based on that false reply the suspicious value should be increased. The suspicious value set as 2 if the node sending the false reply 2 and more than two times means that node consider as the Black hole node. After detecting the black hole node the IDS node sent the black message to its neighbor node and blocking the black hole node operation.

At that time of this process need to evaluate the performance of the network during the black hole node present and after the prevention method. The performance depends on the packet loss, delivery ratio, energy consumption, delay and throughput of the network. These all evaluated from the graphical analysis.

V. RESULT AND DISCUSSION

A. *Node arrangement with attacker node*

In fig (3) describes the attacker occurrence in the network. The attacker occurs during the communication between the nodes. The attacker represented by unique color and some unique function. It also labeled as an attacker.

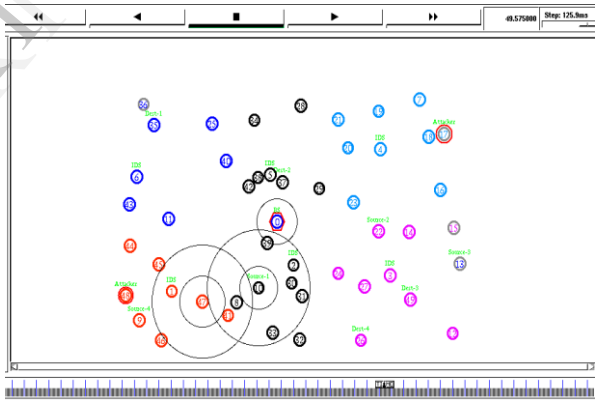

Fig 3: Node with attacker

B. *Packet loss*

In table (8) denotes the packet loss between EDSR with prevention and without prevention from the attack. The packet loss is calculated between the simulation duration of10 to 70 seconds. The packet loss of the EDSR with prevention method is very less compared to the without prevention at particular time periods.

Table 1: Table for Packet loss

Time	EDSR	ATTACK
10	7	0
20	0	0
30	0	37
40	0	0
50	2	0
60	2	0
70	0	41

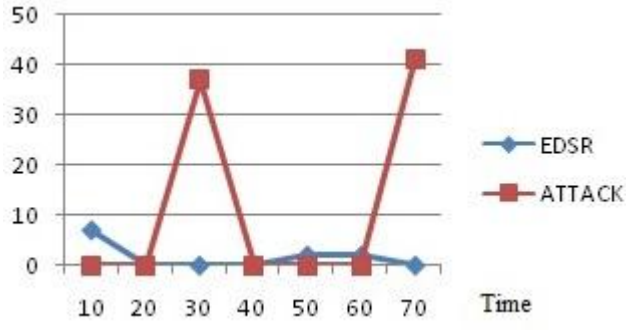

Fig 4: Packet loss

During the simulation two attackers are introduced in between to the other nodes at the respective time interval 30 Sec and 70 Sec. In that particular time period, the attackers restrict the data forwarding by sending the false reply to the source. According to that reason the fig (4) shows the increased level of packet loss up to 41 packets in without prevention method. In the prevention method, the packet loss significantly reduced by using IDS.

C. Delivery ratio

The table (2) shows the variation of the packet delivery ratio between the secure method and unsecure method of EDSR. The packet delivery ratio level of the unsecure method decreased into 20% while intruder presents. In these methods produced 90% to 100% packet delivery ratio, while without interference of intruder nodes.

Table 2: Table for Packet delivery ratio

Time	EDSR	ATTACK
10	.9	1
20	1	1
30	1	.2
40	1	1
50	.9	1
60	1	1
70	1	.2

*Above values interns of percentage.

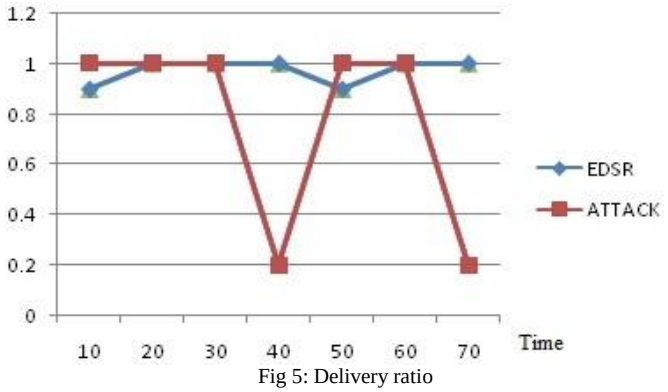

Fig 5: Delivery ratio

In fig (5) also denotes the graphical representation of the packet delivery variations between secure and unsecure methods.

D. *Energy consumption*

In fig (6) and Table (3) describes the energy consumption of the network at that time of using EDSR protocol. This energy consumption is calculated by two manners (i) with security prevention. (ii) Without security prevention.

Table 3: Table for Energy consumption

Time	Attack	EDSR
10	97.9144	99.4053
20	95.6679	98.5635
30	93.5374	96.5245
40	88.8838	93.5903
50	86.185	91.5368
60	83.5149	89.2769
70	80.282	87.413

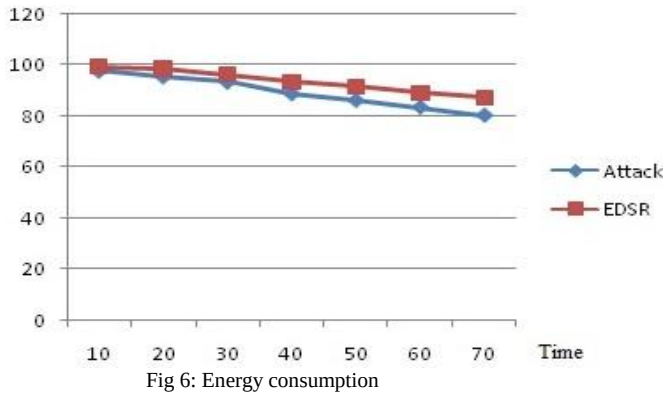

Fig 6: Energy consumption

In with security prevention, energy consumed up to 87% during the simulation time of 70 sec. At the same simulation time interval, without security prevention, energy consumed up to 80%. The energy consumption difference between these two methods is nearly 7%.

D. *Throughput*

Throughput defined as the amount of packet per unit dispatched from one to other nodes and it scaled as bit per second. In the table (4) describes the difference between the throughput of with security and without a security method for every particular time interval.

Time	ATTACK	EDSR
10	0.056	0.055
20	0.0694	2.4
30	1.34	8.10
40	2.60	9.3
50	1.86	9.63
60	1.74	8.24
70	1.197	5.7

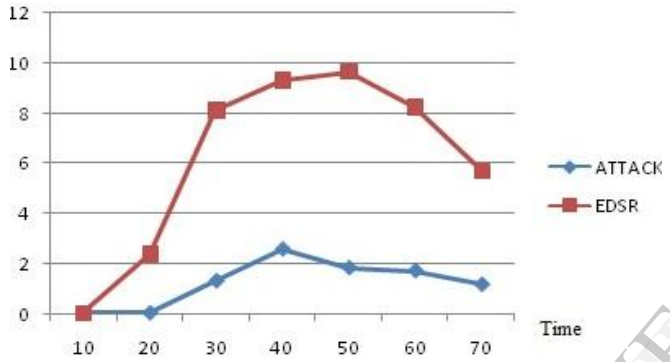

Fig 7: Throughput

From that table (4) and fig (7) throughput is very less in without security method compared to secure method. In the secure method can reach 96% throughput level, but the unsecure method can reach only 26% throughput level. In that particular time the attacker is interrupted with that specific node communication. The attacker node restricts the packet forwarding and also drops the packets. The above mentioned reason creates the decreased throughput level of the unsecure method of EDSR.

VI. CONCLUSION

In this attempt to design the Secure based Efficient Dynamic Source Routing protocol for preventing from the Black hole node. These secure detections and prevention of the node communication done by the IDS with ABM technique. All IDS perform the ABM technique for estimating the suspicious value of the abnormal node based on that suspicious value the node can be defined as the normal and abnormal or malicious node. After the detection of the malicious node the IDS node processes the block message service to its neighbor to avoid the attack. Based on these processes the performance of the network parameter such packet loss, delay, delivery ratio, energy consumption and throughput was evaluated with prevention and without prevention using the NS-2 simulation.

REFFERENCES

[1] Fan-Hsun Tseng, Li-Der Chou, Han-Chieh Chao, "A-Survey of black hole attacks in wireless mobile ad hoc networks", *Springers Transaction on Human-centricComputing and Information Sciences*, Vol 1, no 4, Nov 2011.

[2] Harmandeep Singh, Manpreeet Singh, "Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MA-NETs" *International Journal of Advanced Trends in Computer Science and Engineering*, , Vol 2, No.3, pp43 -46. May – June 2013.

[3] Ketan S. Chavda, Ashish V.Nimavat, "Comparative Analysis of Detection and Prevention Techniques of Black Hole Attack in AODV Routing Protocol of Manet", *International Journal of Futuristic Science Engineering and Technology*, Vol 1, No1,pp 11-14,Jan 2013.

[4] Mayuri Gajera, Sowmya K. S, "Prevention of Black Hole Attack in Secure Routing Protocol", *International Journal of Science and Research* , Vol 2 No 6,pp 221-224, June 2013.

[5] Ming-Yang Su, "Prevention of selective black hole attack on mobile ad hoc networks through intrusion detection systems*",Elsevier Transaction on computer communication* , Vol 34 ,pp 107-117,2011.

[6] Mohammad A. Mikki, "Energy Efficient Location Aided Routing Protocol for Wireless MANET'S", *International Journal of Computer Science and Information Security*, Vol. 4, No. 1 & 2, 2009.

[7] Rahul Sharma, Naveen Dahiya, Divya Upadhyay, "An Analysis for Black Hole Attack inAODV Protocol and It Solution", *International Journal of Computer Science and Mobile Computing* ,Vol.2 No. 4, pp. 391-395, April- 2013.

[8] Swati Jain, Naveen Hemrajani, "Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview" *International Journal of Science and Research*, Vol 2 No5,pp 70-73,May 2013.

[9] Swati Jain, Dr Naveen Hemrajani, Dr. Sumit Srivastava, "Simulation and Analysis of Performance Parameters For Black Hole and Flooding Attack in MANET Using AODV Protocol", *International Journal Of Scientific & Technology Research* Vol 2, No 7,pp 66-69, July 2013.

[10] Vipan Chand Sharma, Atul Gupta, Vivek Dimr**i, "**Detection of Black Hole Attack in MANET under AODV Routing Protocol", *International Journal of Advanced Research in Computer Science and Software Engineering, Vol* 3, No 6, pp.438-443,June – 2013.

[11] K. Sivakumar, Dr. T. Ravichandran, "Efficient Data Aggregation for Mobile Sampling in Wireless Sensor Networks", *IJEST, Vol. 4 No.07, pp-3531-3536, July 2012.*