International Journal of Electrical, Electronics and Computer Engineering **5**(1): 21-26(2016)

ISSN No. (Online): 2277-2626

A Rule Based Mechanism to Mitigate the Packet Dropping in Mobile Ad hoc Network

Akanksha Khare* and Pushpraj Singh Chauhan**

**Department of Computer Science & Engineering, BIST Bhopal (Madhya Pradesh), INDIA*

***Department of Information Technology, BIST Bhopal (Madhya Pradesh), INDIA*

(Corresponding author: Akanksha Khare)

(Received 10 December, 2015 Accepted 17 February, 2016)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Wireless ad hoc network is extensively used area for research work nowadays because of its dynamic and infrastructure less behavior. But due to such characteristic it is more vulnerable to severe kind of security threats which can theft or break our security system and stop services used for communication. Among various kinds of attacks one of attack is black hole which inject false route and announces itself as it has fresh and shortest route to deliver the packet. The wireless network uses routing protocol to route the packet from source to destination. In this we use rule based approach to detect black hole node by using the retransmitting and time varying mechanism. The proposed method is simulated in NS2.34 network simulation tools and the analysis of the proposed work is done using performance metric like PDR, end to end delay and routing load etc.

Keywords: AODV, Black hole, Dynamic, NS-2.34, security threats, PDR

I. INTRODUCTION

In present year, for the transmission of information computer network is widely used. The network is classified into two category namely wired and wireless network. Wired network has fixed infrastructure due to this it can send the information to the limited users and can handle only small amount of information. The wireless network overcome all these limitations of wired network because it has capability to form dynamic network due to this no. of users can increase or decrease and also able to transmit a larger amount of information.

Mobile ad hoc networks (MANETs) are generally fashioned by an assembly of mobile nodes, which are interconnected using wireless links, which agree to cooperate and forward each other’s packets. One of the basic postulations for the design of routing protocols in MANETs is that all nodes are truthful and cooperative. Which means, if a node alleges it can reach another node by a convince path or distance, the allege is reliance/ true; correspondingly, if a node reports a link split, the link will no longer be used. Although this assumption can fundamentally facilitate the design and accomplishment of routing protocols, it meanwhile commences a vulnerability to numerous category of denial of service (DoS) attacks [1], generally packet dropping attack. To instigate such attack, a malevolent node can stealthily plummet a few or all data or routing packets passing through it.

Due to the short of physical fortification and steady medium access method, packet dropping attack represents a severe menace to the routing function in MANETs. An opponent can effortlessly join the network and compromise a justifiable node after that subsequently start dropping packets that are expected to be conveyed in order to disturb the customary communications. Therefore, all the routes passing through this node not succeeded to ascertain an exact routing path among the source and destination nodes. Although upper layer recognition, such as TCP ACK (Transmission Control Protocol Acknowledgment) can sense end-to-end communication shatter, it is incapable to recognize correctly the nodes which contribute to that. In addition, such system is unavailable in connectionless transport layer protocols like UDP. For that reason, securing the basic operation of the network becomes one of the principal apprehensions in hostile environments in the presence of packets droppers. The confront lies in securing communication for now maintaining connectivity amongst nodes in spite of the attacks launched by the opponents and the recurrently varying topology. It is thus obvious that both phases of the communication, mainly route innovation and data transmission phase, should be protected, calling for widespread security studies.

Whereas a number of surveys [2, 3] dealing with security threats adjacent to routing protocols in MANETs, have provided a few perceptive indications on dissimilar threats and countermeasures, none of them focus on a explicit attack and examine all its characteristics in different routing techniques.

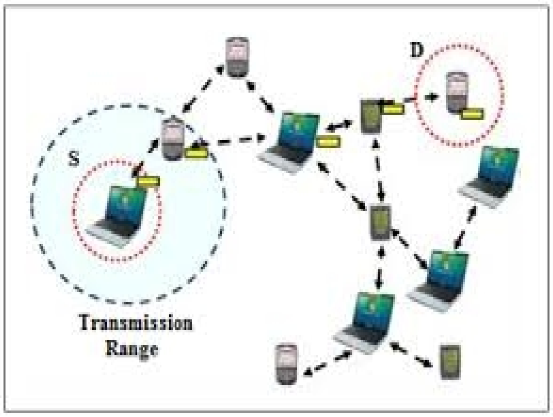

Fig. 1. An overview of wireless ad hoc network.

To complement those efforts, this work studies the packet dropping attack, which is known as one of the most destructive threats in MANETs, and illustrates in depth the different schemes used by adversaries targeting on both reactive and proactive protocols. Furthermore, we conduct an up-to-date survey of the most valuable contributions aiming to avoid the packet droppers. The careful examination and analysis has allowed us to carry out a comparative study of the existing security schemes in terms of specific design rationale and objectives. The ultimate goal is to identify the strengths and weaknesses of each scheme in order to devise a more effective and practical solution which can achieve a better trade-off between security and network performance. The arrangement of the rest part of the paper is done in this way: In section II demonstrate the literature of the preceding work done. After that section III describe with the black hole attack development in AODV. In section IV explain the proposed methodology and algorithm. The section V exemplifies the simulation background and experimental results of the proposed work and last section gives overall conclusion of this paper to thwart the network from malevolent node.

II. LITERATURE REVIEW

The network may compromise from severe kind of threats (black hole) when the data are moving over it which can break or stop the services or resource required for transmission. To avert black hole attack so many techniques have been implemented in which some are explained below:

In [4] proposed a distributed and cooperative method to handle the black hole predicament. The method is distributed so that it can fit with the ad hoc environment of network, and nodes in the protocol work cooperatively collectively so that they can examine, perceive, and abolish probable multiple black hole nodes in a more consistent manner. Simulation outcomes demonstrated that their method accomplished a high black hole detection rate and good quality packet delivery ratio; whereas the overhead is relatively lower as the network traffic enhances.

In [5] proposed an algorithm for exposure of cooperative black hole attack. This commenced the conceptions of maintenance of data routing information table (DRI) and cross checking of a node. It was concluded that the proposed algorithm works healthy in case of detecting the cooperative black hole attack and guarantees a protected as well as a consistent route from source to destination. The work was simulated using throughput, average end-to-end delay, dropped packets and packet delivery division metrics on network simulator NS-2.

In [6] proposed a method in which broadcast synchronization (BS) and relative distance (RD) method of clock synchronization is used to thwart the black hole nodes. In this internal and external clock node compare with the threshold clock if both the clock time is greater than the threshold then it is found that the node is malevolent. This method can effortlessly discover and thwart the block-hole node.

In [7] proposed a method, according to activity of black hole, the method of selecting AODV reactions alters in a way that the source node ignores the response received from black hole node, and sends data packages from a different route. This can be done by allocating conformity level to network node, changing the way of selecting response, updating and distributing fidelity table by the source node. Simulation outcome signifies that, in proposed method, the rate of package delivery has been significantly increased in evaluation with AODV.

In [8] proposed a trouble-free and dexterous approach for providing the security adjoining to the black hole attack in the mobile ad hoc networks based on the AODV routing protocol. In this approach known as ACO, best probable path is used which is based on one of the several parameters such as completely distributed approach. In the specified approach the operations are performed in each node in an exceedingly uncomplicated behavior. The method is based on the asynchronous and self-directed interaction among agents. The algorithm is energetic and error liberal so there is no requiring of defining path resurgence algorithms.

In [9] introduced a novel discovery method based on checking the sequence number in the route reply packets by making exercise of an original message originated by the destination. In this method, when an .intermediary node unicast a RREP packet, the node also unicast a recently defined control message to the destination node to request for the up-to-date SN. Upon receiving, the destination node unicast an answer message to notify the source node of the up-to-date SN. This answer from the destination node enables the source node to authenticate if the intermediate node has sent a faked RREP message by checking if the SN in the RREP message is better than the up-to-date SN.

This method has additional network overhead and time delay since node in the network produces novel packets.

III. SECUTIY ATTACK

Confidentiality, Authorization, Integrity, Availability are the basic requirements for a secured network. Transmission of data packets in MANET takes place in an open medium which makes it vulnerable to security attacks. MANET is more vulnerable than a wired network. There are two basic types of security attacks detected in MANET as [10]:

-Internal Attacks and
-External Attacks.

Internal Attacks. Internal Attacks are carried out by the most promising and trusted nodes that are the part of the network. The trusted node acts as the genuine node and attains an unauthorized access. It also participates in other network activities. Such malicious nodes generate wrong routing information for other nodes in the network.

External Attacks. External Attacks are carried out by the malicious nodes outside the network. Such attacks cause congestion in the network generating false routing information. These attacks prevent the network from normal communication. Passive attacks and Active attacks are further classification of such attacks.

Passive Attacks. Passive attacks neither harm nor alter the data transmitted across the network. The malicious node listens to the network and senses the medium through an unauthorized access. Powerful encryption algorithms are the only solution to keep the data safe from being corrupted. Such attacks can be prevented.

Active Attacks. Active attacks may harm or alter the data being transmitted across the network. It may even prevent the flow of message from one node to another. The attack involves actions of the intruders with the aim to attack the data traffic. The malicious nodes through an unauthorized access sense the network and change or modify the routing information, the packet sequence number etc and thus resulting into congestion in the network. These attacks are seen in several layers of the protocol stack. Some of them are Black Hole Attack, Worm Hole Attack, DoS Attack and Gray hole Attack. Here we discuss about the Black hole Attack in AODV and TORA Protocol.

IV. BLACK HOLE ATTACK IN AODV

An ad-hoc routing protocol [11] is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile adhoc network. Being one of the category of ad-hoc routing protocols, on-demand protocols such as AODV (Ad-hoc On demand Distance Vector) and DSR (Dynamic Source Routing) establish routes between nodes only when they are required to route data packets. AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network. In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery. Every neighboring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough route, it unicasts an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise.

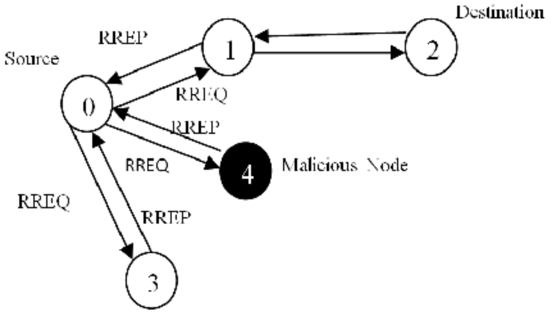

Fig. 2. Illustration of Black hole attack.

The same process continues until an RREP message from the destination node or an intermediate node that has fresh route to the destination node is received by the source node. Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes. This deliberate dropping of packets by a malicious node is what we call a black hole attack [12]. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in Fig. 1 above, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1, 3 and 4.

However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2. An RREP message from a malicious node [6] is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them.

V. PROPOSED WORK

In this section of the paper, we are explaining our proposed methodology to defend the network from black hole attack which announces false information to the source node that it has shortest route to the destination.

In the proposed scheme here use rule based retransmitting approach is also used and varying timing of re-transmission to keep away from superfluous and exaggerating packets transmission. There are multiple approaches are applied to secure the current entire network, whereas node based on multi option, such as if PDR performance is continuous decreases and packets transmission between next two hops takes much time as previous two hops than the current packets will be dropped and that will be called blocked request, and following updating will be done in entire network, discovery of new path, path sequence number and shared key for securing the network.

Furthermore in proposed approach shared key plays a important role to secure a network. Here, key is changes after some unauthorized activity to provide more powerful security to the path and network .Additionally in proposed approach set IDS node that observe the neighbors node furthermore if IDS gets any discarded inactivity in close convenient range, so persist watch the meticulous node and if aggressor node receive packets excluding not forward, consequently that node set as attacker and it gets to be blocked, an additional mania if several node continues throwing the routing packet to the particular node, then it will also treated as attacker node, then it will be also blocked in to entire network. Later than the successfully blocking it changes the entire route moreover starts sending data to the destination node. Although the transmission of packets they also monitor the performance of PDR, if it gets decreases at any time moment then it should be go to the observation period until not identified the reason of that.

The purpose of security algorithm is asymmetric post distribution cryptography initially the keys are generated and shared by in network nodes only and to generate the key nodes append their different level number. For sharing the keys among nodes either distributed as well as centralized methodology is used and the level is equal to half the no. of bits in the given address. So, the nodes at the same level share their keys by this distributed way. However, a centralized technique is used for nodes at different levels. Such keys are assigned centrally by the base station.

Proposed Algorithm

```
Set mobile node = BlcNd          //Total Mobile Nodes
Set Sender node = S                  //S □ BlcNd
Set Receiver Node = R                // R □ BlcNd
Set Routing Protocol =AODV
Set radio range = Rd_rng;            //initialize radio range
Set packet sequence no = pkt_sno;

AODV-RREQ_B (S, R, Rd_rng)
{

        IF (Rd_rng>550 && S != true)
                Destination is unreachable
}
Route_Discovery()
{
rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination
if (dist==active)
{
send ack to source node with rtable1;
Data_packet_send(s_no, nexthop, type)
}
Else
{
Destination node is unreachable;
Sh_key(Rd_rng, pkt_sno); //additional secure to the network + change packet sequence no
}
And update routing table
rtable->insert(rtable->rt_nexthop); // nexthop to RREQ source
rtable1->insert(rtable1->rt_nexthop); // nexthop to RREQ destination
}
Else
packet drop
End if
}
RREQ_Limit(S, R, BlcNode)
{
        Bi € BlcNode         // Blackhole
        PDRu,v               // packet delivery ratio of path X to Y
        Bi generate Msg
        Bi Broadcast (Msg, ii)
        IF (Ii receives Msg)
        {
```

```
 Calculate Tn = Msg-ti  - Msg-t1     //   where   I   end message in time t
Cnt(Msg)                             // count sent msgs
$\partial$ = Msg/Tn                  // per packet time
IF (limit-time <= ($\partial$*10))
{
RREQ_Blocked()  // Node is blocked

}
Else IF (incoming == active && outgoing ==active)
 {
  RREQ accepted by neighbor node;
 PDR = ∑ no of packet receive / ∑no of packet sent
  IF (PDR is continues decreases) THEN
         {
             RREQ_Blocked ()  //Can't accept packets from neighbor;
             Starts discovery of new path;
ELSE
             continue communication;
}
}

Sh_Key (Rd_rng, pkt_sno)
 LOOP (R ≤ Rd_rng)
              listen to the neighbor
             IF (Hello-packet(nodeID, Rd_rng) = Received) THEN
                         IF (level==same) THEN
                                     Key = nodeID+ number-of-bits (nodeID)/2
                         ELSE
                                     Key = node ID + secondary-Key
                         Key-set = Key-set □ Key
                         Reply(node ID, MAC, Key)
                         END IF
                         pkt_sno = pkt_sno + $2^{pkt\_sno+i}$;
             END IF
END LOOP
END Sh_Key;
```

VI. EXPERIMENTAL RESULTS

In this paper first we implemented AODV routing protocol for MANET under varying CBR (Various Parameters) and Scenes (Various Parameters) by varying the different parameters. After this we implemented malicious nodes in the network and then evaluated AODV routing protocol under the same conditions on which we evaluated AODV routing protocol for MANET. All the parameters have varied on the averages of five runs over different randomly generated mobility patterns.

Table 1: Simulation environment.

Simulator used	NS-2.34
Topology area	1000 X 1000
No. of Mobile Nodes	50
Simulation Time	250
Speed	45 m/sec
Packets	CBR
Black hole	1, 2, 3
Protocol	AODV, Black hole AODV, IDS-AODV

Result Analysis

In order to simulate the scenarios described above, the implementation was done in NS-2.34 Network Simulator. The scenario for the simulation of the proposed work is set accordingly: zero black hole node, one black hole node, two black hole node and three black hole node. The scenario of all these are shown below:

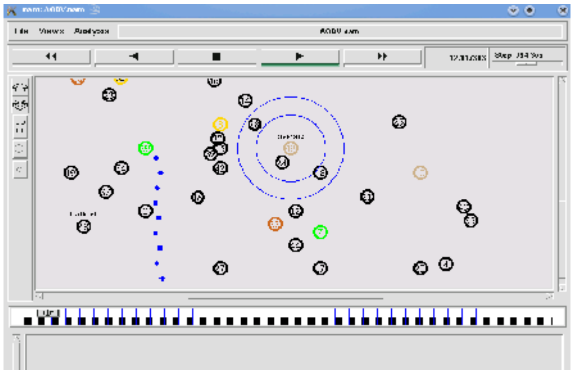

Fig. 3. Simulation scenario with black hole nodes.

Now the analysis of the proposed methodology is done using performance measuring parameters such as end to end delay (E2E), routing load (RL) and packet delivery ratio (PDR).

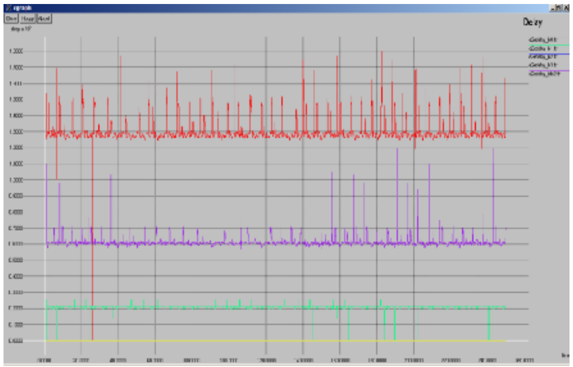

Fig. 4. End to End delay with simulation time.

Fig. 4 shows the end to end delay of the network is less when the network doesn't have any black hole node and as black nodes increases the delay occurs during the transmission of the packets from source to destination.

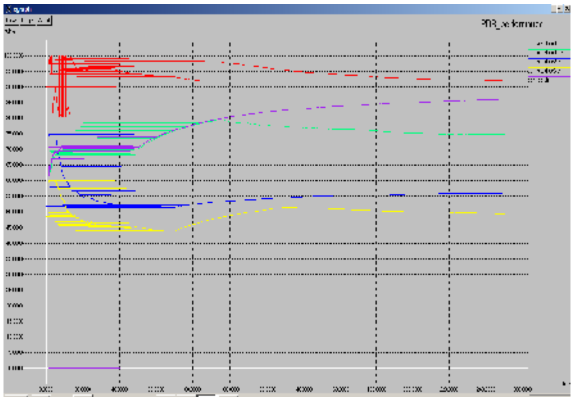

Fig. 5. PDR performance with simulation time.

The above Fig. 5 shows the packet delivery ratio of all these nodes. When network does not consist any black hole node, the packet delivery of the system increase very rapidly and if it contain malicious node then the packet transmission rate degraded very fastly.

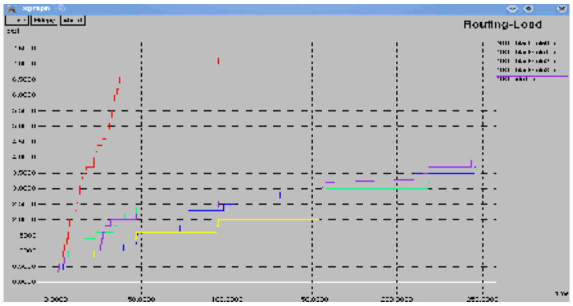

Fig. 6. Routing Load with simulation time.

The above Fig. 6 shows the routing load occurs on the network due to these nodes. When network does not consist any black hole node, the routing load of the system decrease very rapidly with respect to simulation time and if any malicious node present in the network then it enhances the traffic due to the load on the network increase.

VII. CONCLUSION

During the transmission of the packets over network different kinds of security threats make attack in which one of the serious network threats is black hole attack. In this paper, we propose a rule based approach to mitigate the packet drop due to presence of malicious threat. We use retransmitting and varying timing of retransmission which keep superfluous packet and overdoing packets transmission which works on the basis of possibilities and for regularly monitoring the network IDS is set which monitors their neighboring node activity if any malevolent node or superfluous activity is performed by the node then it will discard them. This approach is very efficient in detecting the malicious node. It enhances the rate of packet transmission and also decreases the routing load of network.

REFERENCE

[1]. X. Wu and D. K. Y. Yau, Mitigating denial-of-service attacks in MANET by incentive-based packet filtering: A game-theoretic approach, *In Proc. 3rd International Conference on Security and Privacy in Communications Networks, Nice, France, September 2007.*

[2]. T. R. Andel and A. Yasinsac, "Surveying Security Analysis Techniques in MANET Routing Protocols", *IEEE Communication. Surveys & Tutorials*, **9**(4): 70-84, Fourth Quarter 2007.

[3]. P. Argyroudis and D. O'Mahony, "Secure Routing for Mobile Ad Hoc Networks", *IEEE Communication. Surveys & Tutorials*, **7**(3): 2-21, Third Quarter 2005.

[4]. Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, LNAI 4819, pp. 538–549, In proceeding of Springer-Verlag.

[5]. Ms. Gayatri Wahane and Prof. Ashok Kanthe, "Technique for Detection of Cooperative Black Hole Attack in MANET". *IOSR Journal of Computer Science (IOSR-JCE),* e-ISSN: 2278-0661, PP.59-67, 2014.

[6]. Harsh Pratap Singh, Rashmi Singh, "A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc network using AODV protocol", *International Conference on Electronics and Communication Systems (ICECS) 2014* , Page(s):1 - 8 Print ISBN:978-1-4799-2321-2.

[7]. Iman Zangeneh, Sedigheh Navaezadeh, Abolfazl Jafari, "Presenting a New Method for Detection and Prevention of Single Black Holes Attack in AODV Protocol in Wireless Ad Hoc Network" *International Journal of Computer Applications Technology and Research,* Volume **2**– Issue 6, 686 - 689, 2013, ISSN: 2319–8656.

[8]. Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi, "Detection and Prevention of Blackhole Attack in MANET Using ACO", *IJCSNS International Journal of Computer Science and Network Security*, VOL.**12** No.5, May 2012 21.

[9]. XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET", Autonomous Decentralized Systems, 2009. ISADS '09. *International Symposium on,* vol., no., pp.1-6, 23-25 March 2009.

[10]. Dipika Jain, Ms. Sunita Sangwan, "The Effects of Black hole attack on AODV and TORA protocols: A Review", *International Journal of Engineering Trends and Technology (IJETT)* – Volume **20** Number 1 – Feb 2015.

[11]. Nisha P John, "A New Approach for the Detection of Black hole Nodes in AODV Based Mobile Ad-Hoc Networks", *International Journal of Engineering Research & Technology* (IJERT) Vol. **2** Issue 1, January- 2013 ISSN: 2278-018.

[12]. G. Sandhu and M. Dasgupta, "Impact of blackhole attack in MANET" *International Journal of Recent Trends in Engineering and Technology*, **3**(2), 2010.