International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Preventing DSR Protocol against Black Hole Attack for MANET

Rahul Patel, Maitrey Patel

Student, Dept. Of Computer Engineering, Grow More Faculty of Engineering Himatnagar, Gujarat, India
Asst. Professor, Dept. of Computer Engineering, Grow More Faculty of Engineering Himatnagar, Gujarat, India

Abstract- ***Mobile ad hoc network (MANET) is a collection of mobile nodes that communicate with each other without any fixed infrastructure or a central network authority. Dynamic source routing (DSR) is a broadly accepted network routing protocol for mobile ad hoc network (MANET).Black hole is a malicious node that always gives the false route replay(RREP) for any route request(RREQ) without having specified path to the destination node and drops all the received packets. In this paper we proposed Schema is based on Prior Receive-Reply algorithm is used to identify the malicious node in DSR protocol. Schema is divided into two phases, Detection of malicious node before route establishment and Avoid Communication with malicious nodes during data forwarding. The simulation is carried on NS-2 and the simulation results are analyzed on various network performance metrics such as packet send and received, packet dropped, and Average Network throughput, end-to-end delay and packet delivery ratio.***

Keywords: *Mobile ad hoc networks (MANET), Routing Protocols, Black Hole Attack, Security Attack and Simulation.*

1. INTRODUCTION

A mobile Ad hoc network (MANET) [1] is a self – configuring network that does not require any fixed infrastructure, which minimizes their cost as well as deployment time.

Fig .1 MANET Network

MANETs are suitable for use in situations where any wired or wireless infrastructure is inaccessible, overloaded, damaged or destroyed such as emergency or rescue missions, disaster relief efforts and tactical battlefields, military operations, and terrorism response or in the research area like sensor networks.

2. ROUTING PROTOCOL IN MANET [2]

Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network.

Routing protocols for MANETs [2] can be broadly classified into three main categories:-

Proactive routing protocols: Every node in the network has one or more routes to any possible destination in its routing table at any given time.

1). DSDV Protocol.

Reactive routing protocols: Every node in the network obtains a route From Source to destination when it needed for established communication between them for sending data

1). AODV Protocol.
2). DSR Protocol [3]

Hybrid routing protocols: They introduces a hybrid model that combines reactive and proactive routing protocols.

1). ZRP Protocol.

3. OVERVIEW OF DSR PROTOCOL [3]

It is a routing protocol for wireless mesh networks. One of the most popular on-demand routing protocol is dynamic source routing protocol (DSR) in which a node attempts to discover a route to some destination only when it has a packet to send to that destination.
DSR consists of two phase:

A. Route Discovery

Route Discovery is divided into two stages: Route Request (RREQ) and Route Reply (RREP). When the destination node receives the RREQ packet, appends its address and generates a route reply packet (RREP)
When the source node receives RREP, it first stores the route in its Route Cache and then sends data packets through that route.

B. Route Maintenance

In **Route Maintenance** phase, when data is being transmitted and an intermediate node detects that the network topology has changed or the data can't be transmitted to its next hop, it generates a route error. For recover the error previous node send back the route error packet (RERR) to source. After the (RERR) packet received at source node ,source again start route discovery phase to obtain other safe route.

4. TYPES OF ATTACK IN MANET

Security Attack in MANETs [4], [5] is an intricate issue. Attacks in MANET can be categorized into two parts:

- Passive attacks and
- Active attacks

A passive attack does not disturb the routing protocol operation, but only tries to find information by listening to routing traffic, so it is very difficult to detect.

Active attack is altering the data; procure authorization by inserting false packets into the data or modifying packets transition through the network.
Active attack can be further divided into two parts:

- External attacks
- Internal attacks.

External Attack: External attacks are carried out by nodes that do not belong to the network.
Internal Attack: Internal attacks are from nodes that are part of the network.

Different types of Network Layer attacks are described below [5]:
1).Denial of Service attack: This attack aims to attack the availability of a node. If this attack is successful then services of network will not be available.
2).Man- in- the- middle attack: An attacker place between the sender and receiver and sniffs any information and data which are sent between two nodes.
3.) Impersonation or Spoofing: In this attack a malicious node can act as a genuine node and monitor the network traffic.
4).Routing Attacks: In this attack two type of attack. One is attack on routing protocol and another is attack on packet forwarding or delivery mechanism.
5).Gray-hole attack: This attack has two phases. In the first phase the node advertise itself as having a valid and shortest path to destination and second phase, nodes drops all packets with a certain probability which send by source.
6).Black hole Attack: A malicious node sends false routing information and claiming that it has a shortest path from Source to destination. The malicious node does this by assigning a highest sequence number to the reply packet. And during data forward phase malicious node drops all data packets that normally forwarding those packets from source to destination.

5. BLACK HOLE ATTACK [6], [7]

During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path between source and destination A black hole is a kind of attack that can be easily working against routing in mobile ad hoc networks, where a malicious node intercept the packets by advertising itself as having the shortest path to the node.
Black hole attack is active attack which discuss in previous topic. A black hole is a node that always responds with a RREP message to every RREQ by assigning a highest sequence number, even though it does not really have a shortest route to the destination node.
In the following illustrated Fig. 2, imagine a malicious node M where S is Source Node and D is Destination node. When node S broadcasts a RREQ packet, then nodes 1, 3 and M receive it. Node M, being a malicious node, so it immediately sends back a RREP packet to source node S for claiming a route to the destination. Node S receives the RREP from malicious node M earlier then RREP from 1 and 3.

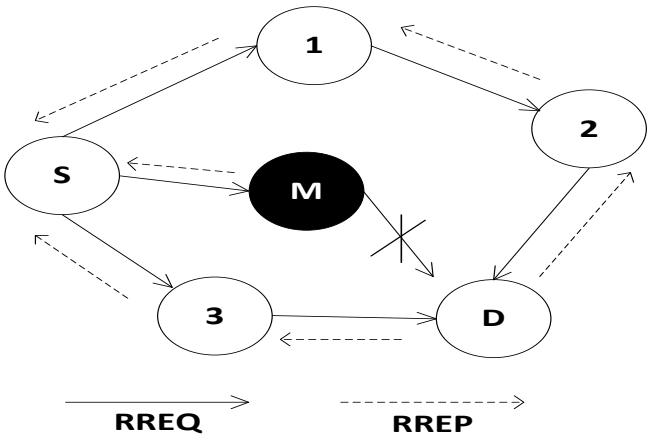

Fig. 2 Example of Black hole Attack

Node S assumes that the path through M is the shortest route for sending data to destination and sends data packet to the destination through it. When the node S sends data to M, the malicious node M drops all data packets that normally forwarding those packets from source S to destination D.

A. Types of Black Hole Attacks

A Black Hole attack is a type of denial of service attack. Divided into following two types.

1).Single Black Hole Attack

In single black hole attack only one malicious node attack on the route.

2).Co-operative Black Hole Attack

In the Co-operative Black Hole attack the malicious nodes have an effect in a group.

6. LITERATURE REVIEW

In [8] Lee et al. proposed the two different message like route confirmation request (CREQ) and route confirmation reply (CREP) to detect the black hole attack. The midway node in addition to transferring RREPs to the source node furthermore sends CREQs to its next-hop node towards the destination node. If a route is present, it sends the CREP to the source. After receiving the CREP, the source node compares the route which presented in RRE. If both are same then source route is correct.

In [9], Shurman et al. proposed the source node to wait until the arrival of a RREP packet from above two nodes. On list of multiple RREPs, the source node checks about a common hop. If at least one hop is common, the source node considers that the route is safe.

In [10], Association based Routing which is to be applied over the DSR protocol in order to enhance the security. The purpose of this scheme is to detect malicious node by defined some association criteria between two node.

In [11],Pirzada and McDonald present a method to improve the DSR protocol. They propose the method of deploying trust gateways to reinforce the DSR protocol. In this schema, the number of malicious nodes in the network is identified and with the use of the trust base gateway, for avoid in the exchange of data packets.

In [12], each RREP packet is required by intermediate node to send the information about next hop. After receiving this RREP packet, source node sends a Further Request(FREQ) to next hop to verify that it has path is safe or not. If Intermediate node reply by the Further Reply (FREP) packet with route to destination then source node consider path is safe otherwise consider that intermediate node is malicious node.

In [13], the authors analyzed the black hole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. In this paper authors propose a statistical anomaly detection schema to detect the black hole attack, by compare the destination sequence numbers of the received RREPs.

In [14], Intrusion Detection Systems (IDS) are one of the main techniques utilized to prevent attacks against security threats. Intrusion detection is a process of detecting black hole attack by predefines subsequent actions.

In [15] In this paper, proposed scheme for Detecting Black Hole Attacks in MANETs by “Detecting Black hole Attacks on DSR-based (DBA-DSR) Mobile Ad Hoc Networks". is introduced. The BDA-DSR protocol detects and avoids the black hole problem before the actual routing mechanism is started by using fake RREQ packets to catch the malicious nodes.

7. PROPOSED WORK

The solution, which is proposed to prevent the black hole attacks in the MANET. In this method checking whether there is large difference between the sequence number of source nodes or intermediate node who has sent back RREP. Here the new attribute destination sequence number (DSN) is a 32 bit integer associated with every route. This sequence number is used for find the route as fresher route between source and destination. If the destination sequence number is larger than others route DSN, then considered that this DSN from the malicious node. If there exists much more differences between source and destination sequence number, then the Intermediate node or destination node is malicious node. Then select the Node having highest value of destination sequence number among the RR Table entries and consider as black hole node. See in Fig.3 the Flow Diagram for Detect Black Hole

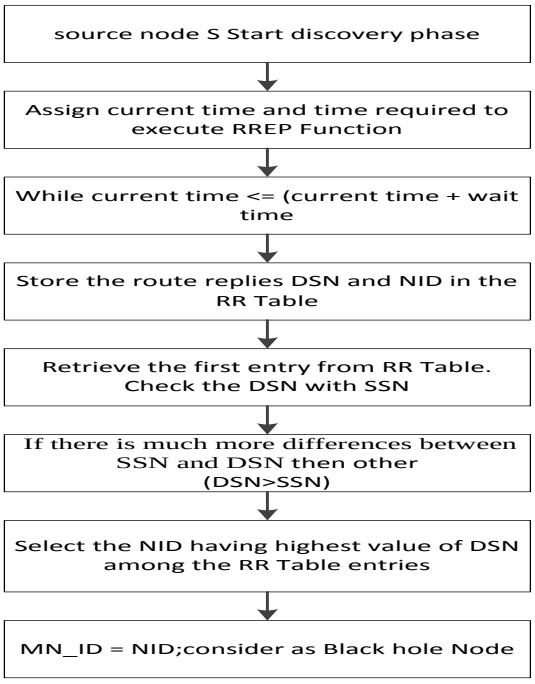

Fig.3 Flow Diagram of Detecting Black hole

Algorithm :(*Prior Receive-Reply*)

Method Parameters: Destination Sequence Number (DSN), Node ID (NID), Malicious Node ID (MN_ID)

Step 1: Initialization Process: Start discovery phase with the source node S. Assign current time and time required to execute the Prior-Receive Reply (RREP function).

Step 2: Store Process: Store all the Route Replies DSN and NID entry in the RR (Request Reply) Table. Repeat the store process until the time exceeds.

```
While ((current time ≤ (current time + wait time))
{
 Store the route replies DSN and NID in the RR-Table.
}
```

Step 3: Detect and Remove Malicious Node: Retrieve the first entry from RR (Request Reply) Table. Compare the DSN with SSN, if DSN is greater than SSN, and then delete the first selected entry from the RR Table.

```
If (DSN > SSN)
{
   MN_ID = NID;    Delete entry from table

}
```

Step 4: Node Selection Process: Sort the contents of RR Table entries according to the DSN. Select the NID having highest value of DSN among the RR Table entries. Consider as malicious node and send MN_ID to all network nodes during default Receive Reply method of DSR Protocol. Continue step 3 and step 4 until we have to find the destination node.

Step 5: Continue Default Process: Call Receive Reply method of default DSR Protocol.

There are some benefits of proposed solution are:
(1)The malicious node is detected at the initial stage itself and immediately removed. (2) The malicious node has the highest Destination Sequence number (DSN) and it is the first RREP to arrive. The comparison of DSN and SSN is made only to the first entry in the table without checking other entries in the RR table. (3) No modification is made in other default operations of DSR Protocol

After detect black hole in network there are two possibilities for remove it from network are,

Case I: If Intermediate node is Black Hole node.
In above cases, neighbor node removes routing table entries having malicious node for all future communication as well

Case II: If Destination node is Black Hole node.
Each intermediate node will drop the control message and avoid the communication with malicious node.
See in Fig.4 the Flow Diagram for remove Black Hole from the network.

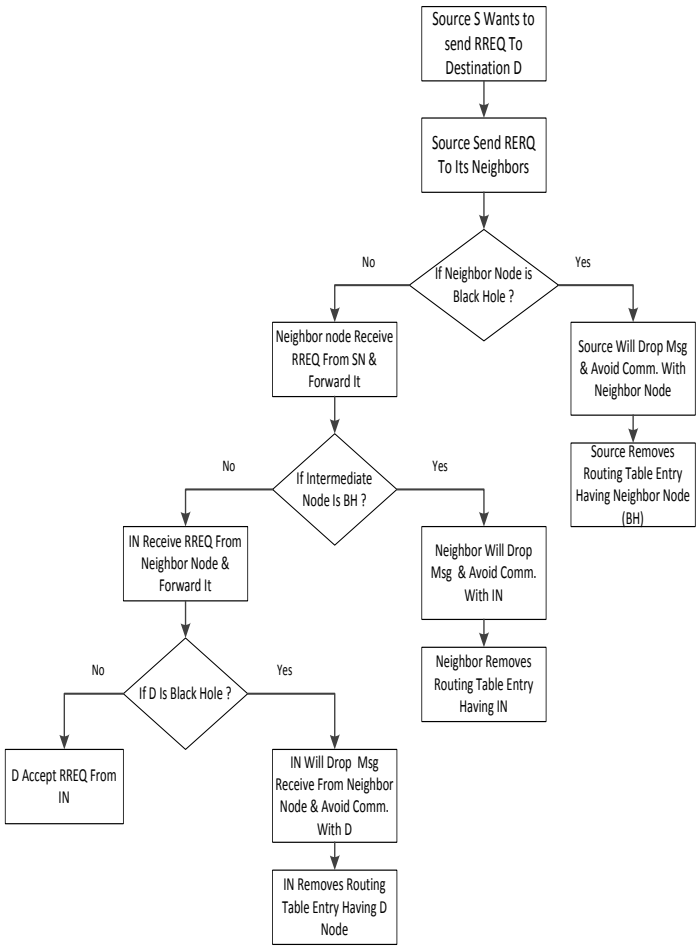

Fig.4 Flow Diagram of Removing Black hole

8. SIMULATION RESULT

In this section, we describe our simulation environment and simulation results. The simulation is being implemented in the ns2 simulator. NS2 is an open-source network simulator research in computer communication networks. The simulation parameters are described in following Table 1.

Table.1 Simulation Parameters

Parameter	Value
Simulator	NS-2.35
Routing Protocol	DSR
Traffic type	UDP-CBR
MAC Type	802.11 MAC Layer
Coverage area	1500m * 300m
No. of Nodes	25,50
No. of Black Hole Nodes	6
Packet Size	512 Bytes
Simulation Time	300 sec

8.1 Sent Packet

It represents the number of packets that sent by the source node.

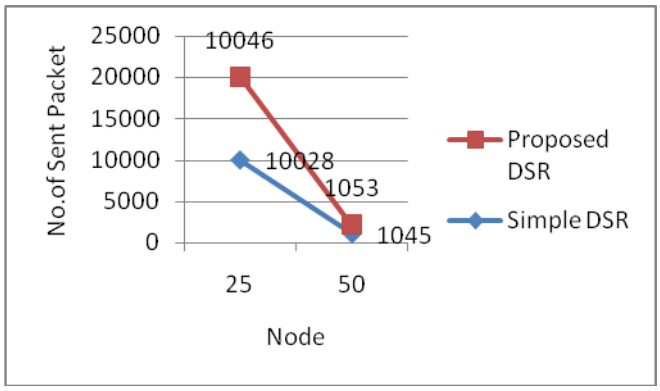

Fig.5 Sent Packets

8.2 Received Packet

It Represent the number of the received packets by the destination node.

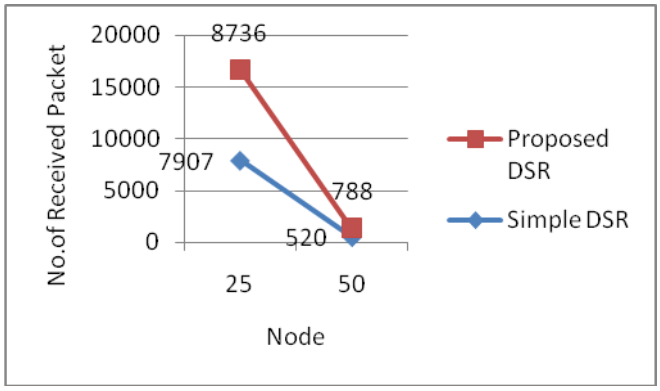

Fig.6 Received Packets

8.3 Dropped Packet

It represents the number of packets that sent by the source node and fail to reach to the destination node.

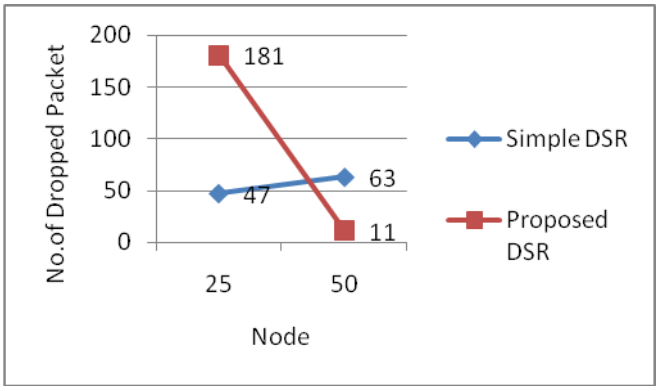

Fig.7 Dropped Packets

8.4 Packet Delivery Ratio (%)

Defined as number of packets received at the destination to the total number of packets that sent by the source.

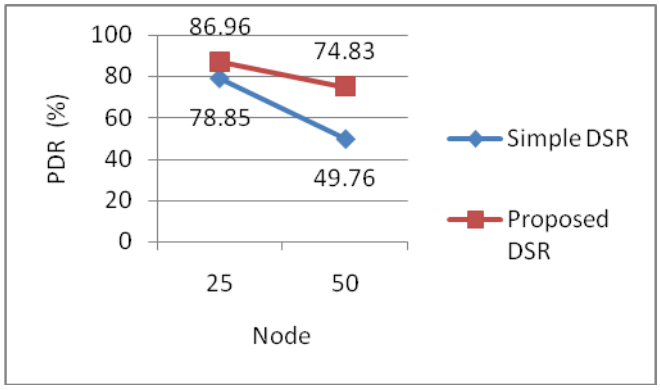

Fig.8 Packet Delivery Ratio

8.5 Average End-to-End Delay (sec)

It represents the time required to move the packet from the source node to the destination node.

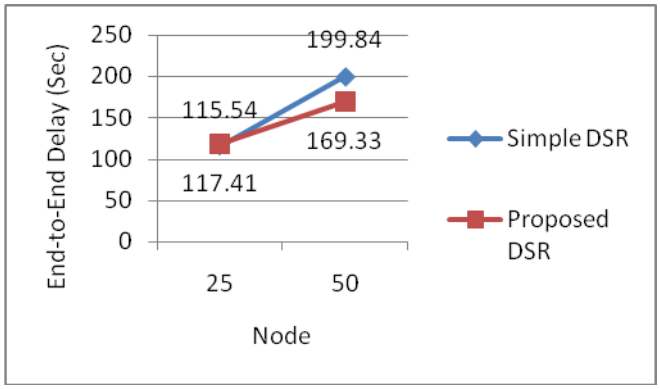

Fig.9 End-to-End Delay

8.6 Average Throughput (kbps)

The throughput is the number of bytes transmitted or received per second.

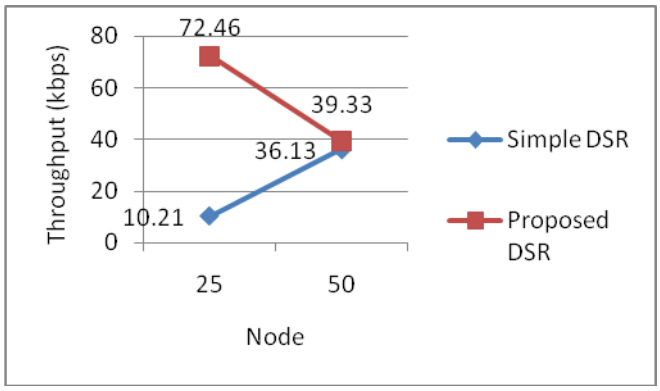

Fig.10 Average Throughput

9. CONCLUSION

In this paper we have gone through the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for it in the DSR protocol. This technique is very simple and efficient approach for defending the DSR protocol against Black Hole attacks. The Proposed method can be used to find the secured routing path by detect and preventing the black hole nodes in the MANET by indentifying the malicious node with their sequence number.

In above simulation result we can see that there are some parameter result are improved then simple DSR protocol results by using our approach for preventing black hole attack.

Finally we can conclude that our proposed algorithm has achieved good improvement in PDR with admissible end-to-end delay.

REFERENCES

[1] S. Corson ,J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations" ,IETF RFC 2501, Jan. 1999.

[2] Elizabeth M. Royer, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks ", IEEE Personal Communications, pp. 46-55, April 1999

[3] J. Broach, D. Johnson, and D. Maltz. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks", IETF Internet draft, Oct. 1999, work in progress.

[4] P. Goyal, S. Batra, A. Singh. "A literature review of security attack in mobile ad-hoc networks",

International Journal of Computer Applications IJCA, 9(12):24–28, 2010.

[5] Tayal S, Gupta V, "A Survey of Attacks on MANET Routing Protocols",International Journal of Innovative Research in Science, Engineering and Technology, 2(6), 2280-2285

[6] Latha Tamilselvan , Dr. V Sankaranarayanan , "Prevention of Black hole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications , 0-7695-2842-2/07 $25.00 © 2007(IEEE)

[7] Dangore M. Y, & Sambar S. S ,"A Survey on Detection of Black hole Attack Using AODV Protocol in MANET", International Journal on Recent and Innovation Trends in Computing and Communication, 55-61.

[8] S.Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, Yoshiaki Nemoto,"Detecting Black Hole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol. 5, No. 3, 2007 .

[9] Nisha P John, Ashly Thomas, "Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review", International Journal of Innovative Research and Development 1, 232-245.

[10] N.Bhalaji, Dr.A.Shanmugam,"Association Between Nodes To Combat Black Hole Attack In DSR Based Manet",978-1-4244-3474-9/09/$25.00 ©2009 IEEE.

[11] Asad Amir Pirzada, Chris McDonald, "Deploying Trust Gateways to Reinforce Dynamic Source Routing", 2005 3rd IEEE International Conference on Industrial Informatics, (INDIN '05),Aug. 10-12, 2005

[12] Akshat Jain, Shekher singh Sengar, Vikas Goel "Colluding Black Holes Detection in MANET" (IJERT), Vol. 2 Issue 1, January- 2013 ISSN: 2278-0181

[13] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto; "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", (IJNS), Vol.5, No.3, Nov. 2007

[14] YibeltalFantahunAlem,Zhao Cheng Xuan,"Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 978-1-4244-5824-0/$26.00 c 2010 IEEE

[15] Isaac Woungang," Detecting Black hole Attacks on DSR-based Mobile Ad Hoc Networks", 978-1-4673-1550-0/12©2012 IEEE