Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET

Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre
Department of Computer Science and Engineering, SGB Amravati University,
JDIET, Yavatmal, India

Email:- amolabhosle@gmail.com

Department of Computer Science and Engineering, SGB Amravati University,
JDIET, Yavatmal, India

Email:- thosar_tushar@yahoo.com

Department of Computer Science and Engineering, SGB Amravati University,
JDIET, Yavatmal, India

Email:- snehal.mehatre@gmail.com

ABSTRACT

Mobile ad hoc network (MANET) is a self-configuring network that is formed automatically via wireless links by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. The mobile nodes allow communication among the nodes outside the wireless transmission range by hop to hop and the forward packets to each other. Due to dynamic infrastructure-less nature and lack of centralized monitoring points, the ad hoc networks are vulnerable to attacks. The network performance and reliability is break by attacks on ad hoc network routing protocols. AODV is a important on-demand reactive routing protocol for mobile ad hoc networks. There is no any security provision against a "Black Hole" and "Wormhole" attacks in existing AODV protocol. Black hole nodes are those malicious nodes that conform to forward packet to destination. But they do not forward packet intentionally to the destination node. The black hole nodes degrade the performance of network eventually by participating in the network actively. The propose watchdog mechanism detect the black hole nodes in a MANET. This method first detects a black hole attack in the network and then provide a new route to this node. In this, the performance of original AODV and modified AODV in the presence of multiple black hole nodes is find out on the basis of throughput and packet delivery ratio. In a wormhole attack, intruders tunnel the data from one end of the network to the other, leading distant network nodes to trust they are neighbors' and making them communicate through the wormhole link.

KEYWORDS

AODV, Black Hole, MANET, RREP, RREQ

1. INTRODUCTION

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the assistance of any stand-alone infrastructure or centralized administration [3]. Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks. Each node in

DOI : 10.5121/ijcsea.2012.2105

mobile ad hoc networks is fit out with a wireless transmitter and receiver, which permits it to communicate with other nodes in its radio communication range. Nodes usually share the similar physical media; they transmit and get signals at the same frequency band, and follow the same hopping sequence or spreading code. If the destination node is not within the transmission range of the source node, the source node takes help of the intermediate nodes to communicate with the destination node by relaying the messages hop by hop. Fig. illustrated the Mobile ad-hoc network. In order for a node to transmit a packet to a node that is out of its radio range, the cooperation of other nodes in the network is required; this is called as multi-hop communication. Therefore, each node must act as both a host and router at the same time.

Mobile wireless networks are generally open to attack to information and physical security threats than fixed wired networks. Securing wireless ad hoc networks is particularly difficult for many reasons including vulnerability of channels and nodes, absence of infrastructure, dynamically changing topology and etc. The wireless channel is available to both legitimate network users and malicious attackers. The abstract of centralized management makes the classical security solutions depends on certification authorities and on-line servers not applicable. A malicious attacker can quickly become a router and break network operations by intentionally not following the protocol specifications.

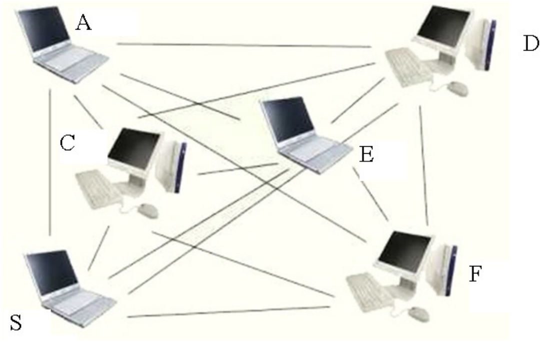


Fig: Mobile Ad-Hoc Network

The nodes can move randomly and freely in any direction and organize themselves arbitrarily. They can unite or leave the network at any time. The network topology changes frequently, rapidly and unpredictably which significantly changes the status of trust among nodes and adds the complexity to routing among the mobile nodes. The self-centeredness of nodes in ad hoc networks may tend to deny providing services for the advantage of other nodes in order to save their own resources acquaint new security that are not addressed in the infrastructure-based networks.

2. ROUTING PROTOCOL

The primary goal of routing protocols in ad-hoc network is to establish minimum path (min hops) between source and destination with minimum overhead and minimum bandwidth use so that packets are transmitted in a timely manner. A MANET protocol should function adequately over a large range of networking context from small ad-hoc group to larger mobile multihop networks[13]. As Fig shows, the categorization of these routing protocols.

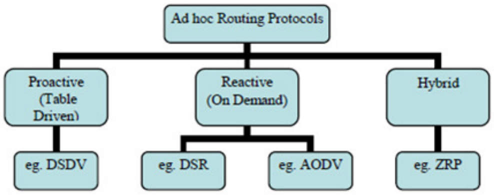


Fig: Hierarchy of Routing Protocol

Routing protocols can be categorized into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type of protocol are Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on-demand protocols, in opposite, do not regularly update the routing information. It is circulated to the nodes only when necessary. Example of this type of protocol is Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type of protocol is Zone Routing Protocol (ZRP).

2.1 Proactive Routing Protocol (Table Driven)

In a network utilizing a proactive routing protocol, every node keeps one or more tables representing the complete topology of the network. These tables are updated constantly in order to keep up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be alternate between the nodes on a regular basis, leading to comparatively high overhead on the network. On the other hand, routes will be available on request. Many proactive protocols arise from conventional link state routing, along with the Optimized Link State Routing protocol (OLSR)[13].

2.2 Reactive Routing Protocol (On-Demand Driven)

Reactive routing protocols[6] are on-demand protocols. These protocols do not try to keep correct routing information on all nodes at all times. Routing information is collected only when it is required, and route determination based on sending route queries throughout the network. The primary benefit of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be consumed. While reactive protocols do not have the fixed overhead needed by keeping continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network because of query flooding. Because of these weaknesses, reactive routing is less applicable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes[13].

2.3 Hybrid Routing Protocol

Wireless hybrid routing is depends on the idea of organizing nodes in groups and then allowing nodes different functionalities inside and outside a group [6]. Both routing table size and update packet size are decreased by involving in them only part of the network (instead of the whole); thus, control overhead is decreased. The most popular way of building hierarchy is to group nodes geographically close to each other into definite clusters. Each cluster has a leading node (cluster head) to communicate to other nodes on behalf of the cluster. The other way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be acquired through this flexibility. Since mobile nodes have only a single unidirectional radio for wireless communications, this type of hierarchical organization will be mentioned to as logical hierarchy to distinguish it from the physically hierarchical network structure[13].

2.4 Security Criteria for Mobile Ad-Hoc Network

While the security requirements for ad hoc networks are the same the ones for fixed networks, namely availability, integrity, confidentiality, authentication, and non-repudiation.

2.4.1 Availability:

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [9]. This security standard is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes do some of the network services unavailable, such as the routing protocol or the key management service [9][14].

2.4.2 Integrity:

Integrity guarantees the individuality of the messages when they are delivered. Integrity can be adjusted mainly in two ways [9].

- Malicious altering
- Accidental altering

A message can be deleted, replayed or revised by an adversary with malicious goal, which is admire as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is classified as accidental altering.

2.4.3 Confidentiality

Confidentiality means that certain information is only use by those who have been authorized to access it. In other words, in order to keep the confidentiality of some confidential information, we require keeping them secret from all entities that do not have the privilege to access them.

2.4.4 Authenticity

Authenticity is basically assurance that participants in communication are genuine and not impersonators [9]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations[14].

2.4.5 Non Repudiation

Non Repudiation guarantees that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

3. AODV ROUTING PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) [4] is a reactive routing protocol which creates a path to destination when required. Routes are not built until certain nodes send route discovery message as an intention to communicate or transmit data with each other. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deals with data transmission. This scenario decreases the memory overhead, minimize the use of network resources, and run well in high mobility situation. In AODV, the communication involves main three procedures [4], i.e. path discovery, establishment and maintenance of the routing paths. AODV uses 3 types of control messages to run the algorithm, i.e. Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. The format of RREQ and RREP packet are shown in Table I and Table II.

I. RREQ field

Source_ address	Source_ sequence	Broadcast_ Id	Destination_ address	Destination_ sequence	Hop_ Count

I. RREP field

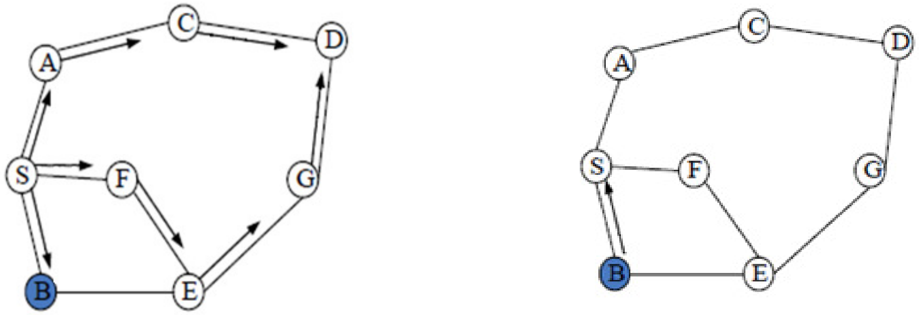
Source_ address	Destination_ Address	Destination_ sequence	Hop_ count	Lifetime

When the source node wants to establish the communication with the destination node, it will issue the route discovery procedure. The source node broadcasts route request packets (RREQ) to all its accessible neighbors'. The intermediate node that receive request (RREQ) will check the request. If the intermediate node is the destination, it will reply with a route reply message (RREP). If it is not the destination node, the request from the source will be forwarded to other neighbor nodes. Before forwarding the packet, each node will store the broadcast identifier and the previous node number from which the request came. Timer will be used by the intermediate nodes to delete the entry when no reply is received for the request. If there is a reply, intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from. The broadcast identifier and the source ID are used to detect whether the node has received the route request message previously. It prevents redundant request receive in same nodes. The source node might get more than one reply, in which case it will determine later which message will be selected based on the hop counts. When a link breaks down, for example due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable due to the loss of the link. It then creates a route error (RERR) message which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Once the source receives the RERR, it reinitiates route discovery if it still requires the route.

4. BLACK-HOLE ATTACK

The black hole attack[5] is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to announce itself as having a accurate route to a destination node, even though the route is counterfeit, with the intention of intercepting packets. In an ad-hoc network that uses the AODV protocol, a black hole node pretends to have a fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the black hole node instatly responds with an RREP message that contains the highest sequence number and this message is received as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source considers that the destination is behind the black hole and rejects the other RREP packets coming from other nodes. The source then starts to transmit out its data packets to the black hole believing that these packets will reach the destination. Vulnerabilities of ad-hoc networks against black hole attacks have solution based on modification of the AODV protocol. The solution has to examine the route through the next hop in the accepted path. This solution means that next hop information shall be added to the standard AODV header. Similar approach is followed in[7] where the nodes are asked to transmit their neighborhood sets once the route is set up. In [8] two solutions are suggested for detecting the black hole attack in ad-hoc networks. First solution involves transmitting a ping packet to the destination to check the set up route. If the acknowledgement does not come from the destination, presence of a black hole is analyze. The other approach proposed is depends on maintaining track of sequence numbers as black holes usually temper with these transmitting packets with unusually high sequence numbers[1].

We assume node B to be a malicious node. Using routing protocol, B claims that it has the routing to the destination node whenever it receives RREQ packets, and sends the response to source node at once. The destination node may also give a reply. If the reply from a normal destination node reaches the source node of the RREQ first, everything works well; but the reply from B could reach the source node first, if B is nearer to the source node. Moreover, B does not need to check its RT when sending a false message; its response is more likely to reach the source node firstly. This makes the source node thinks that the routing discovery process is completed, ignores all other reply messages, and begins to send data packets. The forged routing has been created. As a result, all the packets through B are simply consumed or lost. B could be said to form a black hole in the network, and we call this the black hole Attack.



(a) Propagation of RREQ message (b) Propagation of RREP message

Fig: Black Hole Attack

5. PROPOSED WORK

To analyze the effects of black holes, we simulated the wireless ad-hoc network with and without a black hole node present in the network. To be able to do that, we innovate a new protocol, which we called "Modified AODV". This new protocol, modified AODV is inherited from the existing AODV routing protocol. In Watchdog mechanism, each node keeps two extra tables, one is known as pending packet table and another one is knows as node rating table. There are four fields in pending packet table, Packet ID, Next Hop, Expiry Time and Packet Destination[1].

I. Pending packet table

Packet ID	Next Hop	Expiry Time	Packet Destination

- Packet ID: ID of packet sent.
- Next Hop: Address of next hop node
- Expiry Time: Time-to-live of packet
- Packet Destination: Address of destination node.

There are also four fields in node rating table, Node Address, Packet drops, Packet forwards and Misbehave. This table updated corresponding to pending packet table.

I. Node rating table

Node Address	Packet Drops	Packet Forwards	Misbehave

- Node Address: Address of next hop node.
- Packet Drops: Counter for counting the dropped packet.
- Packet Forwards: Counter for counting the forwarded packet.
- Misbehave: It has two values 0 and 1, 0 for well behaving node, 1 for misbehaving node

Watchdog Mechanism: - In pending packet table, each node maintains track of the packets, it sent. It contains a unique packet ID, the address of the next hop to which the packet was forwarded, address of the destination node, and an expiry time after which a still-existing packet in the buffer is considered not forwarder by the next hop.

In node rating table, each node maintains rating of nodes, which are next to it (means nodes are within its communication range). This table includes the node address, a counter of dropped packets noticed at this node and a counter of successfully forwarded packets by this node[1].

The fourth field of the above node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1(means it is interprited as a misbehaving node), otherwise it is deliberated as a legitimate node. An expired packet in the pending packet table causes the packet drops counter to increase for the next hop correlated with the pending packet table entry.

Each node listens to packets that are inside its communication range, and only to packets associated to its domain. Then, it checks each packet and prevent forged packet. If it notices a data packet in its pending packet table, then it deletes this data packet from pending packet table after authenticating the packet. If it notices a data packet that exits in its pending packet table with source address different from the forwarding node address, then it increases the packet forwarding value in node rating table[1].

For determining whether a node is misbehaving or act as a legitimate one, rest on the selection of threshold value. For example if we assume a threshold value of 0.5. This means that as long as a misbehaving node is transmitting twice packets as it drops it will not be distinguish. If we assume a lower value of threshold then it will increase the percentages of false positives. After finding a misbehaving node, a node will attempt to do local repair [2] for all routes passing through this misbehaving node. If local repair process fails, then it will not transmit any RERR packet upstream in the network. This process attempts to prevent a misbehaving node from dropping packets, and also prevent blackmailing of legitimate nodes. To avoid constructing routes, which traverse misbehaving nodes, nodes drop all RREP messages arriving from nodes currently marked as misbehaving. To stop misbehaving node to act actively in a network, the all packet starting from this node has been dropped as a form of punishment[1].

Introduced mechanism proposed an algorithm is as follows:

```
1. Data packet forwarded or sent.
2. Copy and keep the data packet in pending packet table until it is expired or forwarded
3. If (data packet forwarded)
{
    Increment the corresponding forwarded packet in the node-rating table and remove the
    data packet from pending packet table
}
4. If (data packet expires in the pending packet table)
{
    Increment the corresponding dropped packet in the node-rating table and removes the
    data packet from pending packet table.
    If (dropped packet > threshold (th1)) then
    {
      If ((dropped packet / forwarded packet) > threshold (th1))
        {
            Node is misbehaving.
            Promiscuous node locally tells all the node of its wireless range that particular
            node is misbehaving node.
            Discard RREP message coming from the misbehaving node
        }
    }
}
```

6. WORMHOLE ATTACKS

In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called “wormhole link”. They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network. Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets.

Wormhole attack [10] commonly associates two remote malicious nodes shown as X and Y in Figure-4. X and Y both are attached via a wormhole link and they target to attack the source node S. During path finding process, S broadcasts RREQ to a destination node D. Thus, A and C, neighbors of S, accept RREQ and transmit RREQ to their neighbors. Now the malicious node X that receives RREQ forwarded by A. It records and tunnels the RREQ via the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ to its neighbor B. Finally, B forwards it to destination D. Thus, RREQ is forwarded via S-A-X-Y-B-D. On the other hand, other RREQ packet is also forwarded through the path S-C-D-E-F-G-D. However, as X and Y are connected via a high speed bus, RREQ from S-A-X-Y-B-D reaches fist to D. Therefore, destination D ignores the RREQ that reaches later and chooses D-B-A-S to unicast an RREP packet to the source node S. As a result, S chooses S-A-B-D route to send data that

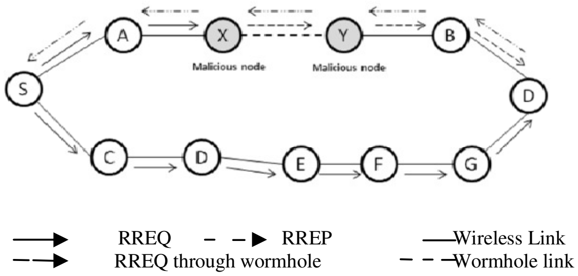


Fig: Wormhole Attack

indeed passes through X and Y malicious nodes that are very well placed compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks.

7. COUNTERMEASURES AGAINST WORMHOLE ATTACKS

For detection and prevention of wormhole attacks, “Packet Leash” mechanism is suggested in which all nodes in the MANET can obtain authenticated symmetric key of every other node. The receiver can authenticate information like time and location from the received packet.

“Time of Flight” is a technique used for prevention of wormhole attacks. It calculates the round-trip journey time of a message; the acknowledgement estimate the distance between the nodes based on this time, and conclude whether the calculated distance is within the maximum possible communication range. If there is a wormhole attacker involved, packets end up travelling further, and thus cannot be returned within the short time.

8. CONCLUSION

MANET requires a reliable, efficient, and scalable and most importantly a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. Mobile Ad Hoc network is likely to be attacked by the black hole attack and wormhole attack. To solve this problem, here present a watchdog mechanism and time of flight to detect and overcome black hole attack and wormhole attack and improve the data security in mobile ad-hoc network.

REFERENCES

[1] Kanika Lakhani, Himani Bathla, and Rajesh Yadav, “A Simulation Model to Secure the Routing Protocol AODV against the Black-Hole Attack in MANET”, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010

[2] C. E. Perkins, S. R. Das, and E. Royer, “Ad-hoc Demand Distance Vector (AODV)”, http:/www.ietf.org/internet-draft/draft-ietf-manet- aodv-05.txt, Mobile Ad Hoc Networking Group, IETF

[3] David B.Johnson and Dravid A. Maltz, “Dynamic Source routing in ad hoc wireless networks”, *Technical report, Carneigie Mellon University*, 1996

[4] Harris Simaremare and Riri Fitri Sari, “Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks”, International Journal of Computer Science and Network Security, VOL-11, June 2011, Page Number-6.

[5] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Networks”, University of Cincinnati, *IEEE Communication magazine*, October 2002.

[6] Imrich Chlamtac, Marco Conti, Jennifer J. - N. Liu “ Mobile ad hoc networking: imperatives and challenges ”, School of Engineering, University of Texas at Dallas, Dallas, TX, USA, 2003.

[7] Lidong Zhou, Zygmunt J. Hass, “Securing Ad Hoc Networks*”, IEEE Special Issue on Network Security*, Vol-13, Nov-Dec 1999, Page Number - 24-30L.

[8] P. Ning and K. Sum, “How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol”, Tech Rep, TR- 2003-07, CS Department, NC University, April 2003

[9] Wenjia Li and Anupam Joshi, “Security Issues in Mobile Ad Hoc Networks”, Department of Computer Science and Electrical Engineering, University of Maryland.

[10] Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, “A Review of Current Routing Attacks in Mobile Ad Hoc Networks”, International Journal of Computer Science and Security, Volume-2 Issue-3, pp. 18-29

[11] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, “MANET Routing Protocols and Wormhole Attack against AODV” , IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010

[12] Dongbin Wang, Mingzeng Hu and Hui Zhi, “A survey of secure routing in ad hoc networks”, Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, PRC

[13] K. Lakshmi, S.Manju Priya, A.Jeevarathinam, K.Rama and K. Thilagam, “Modified AODV Protocol against Black hole Attacks in MANET”, International Journal of Engineering and Technology Vol.2 (6), 2010

[14] Dr. M.S.Aswal, Paramjeet Rawat and Tarun Kumar “Threats and Vulnerabilities in Wireless Mesh Networks”, International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009