Detection of Block hole attack in MANET under AODV Routing Protocol

Dr.L.Nirmala Devi
Department of Electronics and Communication Engineering
University College of Engineering, Osmania University
Hyderabad, India
E-mail: nagiitkgp@yahoo.co.in

***Abstract*— Due to security vulnerabilities of the routing protocols, Mobile ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach the destination node on account of this attack, data loss will occur. Comprehensive attempt has been made to find the effect of malicious nodes on MANETS; hence the Black Hole nodes participate in the network actively and degrade the performance of network. In this paper we proposed a solution for identifying the malicious node in AODV protocol suffering from Black Hole attack**

We compare the scenarios where how a MANET works with and without malicious nodes based on a few performance metrics; such as No of dropped packets, throughput, packet delivery ratio.

Keywords—MANET,AODV,Block hole –attack,selfish node.

I. INTRODUCTION

In ad hoc networks every communication terminal (radio terminal RT) communicates with its partner to perform peer to peer communication. If the required RT is not a neighbor to the initial calling RT (outside the coverage area of the RT), then the other intermediate RTs are used to perform the communication link. This is called multi-hop peer to peer communication. This collaboration between the RTs is very important in the ad hoc networks.

An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network. Routing in Ad Hoc Networks has received a significant attention with a number of different routing protocols, namely proactive, reactive and hybrid. Which protocol is more efficient it depends on the scenario under which these routing protocols are simulated.

Vulnerabilities of operating systems and upper layer applications that belong to user programs such as databases, browsers or client-server applications are not considered as a security issue for ad-hoc networks. General attack types are the threats against the routing layer of the ad-hoc networks; such as physical, MAC and network layer which is the most important function of wireless ad-hoc network for the routing mechanism, orienting the packets after a route discovery process. Other vulnerabilities are application security, network security, database security which is studied in different works which are not explained in detail here.

Attacks to the wireless ad-hoc network in the networking layer usually have two purposes: not forwarding packets or adding and changing some parameters of routing messages; such as sequence number and IP addresses. These are explained in the subsequent sections. Using one of the key mechanisms such as cryptography or authentication, or both in a network, serves as a preventive approach and can be employed against 'attackers'. However, these mechanisms protect the network against attacks that come from 14 outside, malicious 'insiders' which use one of the critical keys can also threaten the security. For instance, in a battle field where ad-hoc networks are used, even if keys are protected by temper proof hardware that are used in the vehicles in the network, it is difficult to say that these vehicles exhibit the same behavior if the enemy captures them.

On the other hand, a node may un deliberately misbehave as if it is damaged. A node with a failed battery which is unable to perform network operations may be perceived as an attack. Another malicious behavior of the nodes is selfishness. Selfish nodes refrain from consuming its resources; such as battery, by not participating in network operations. Therefore; failed and selfish nodes also affect the network performance as they do not correctly process network packets, such as in routing mechanism.We should, therefore ensure that everything is correctly working in the network to support overall security and know how an insider is able to attack the wireless ad-hoc network. Wireless ad-hoc networks should be protected with an intrusion detection system that can understand the possible actions of attackers and can produce a solution against these attacks.

II. DIFFERENT ATTACKS

A. *Passive Eavesdropping*

An attacker can listen to any wireless network to know what is going on in the network. It first listens to control messages to infer the network topology to understand how nodes are located or are communicating with another. Therefore, it can gather intelligent information about the network before attacking. It may also listen to the information that is transmitted using encryption although it should be confidential belonging to upper layer applications.

Eavesdropping is also a threat to location privacy. An unauthorized node can notice a wireless network that exists within a geographical area, just by detecting radio signals. To combat this, traffic engineering techniques have been developed.

B. Selective Existence (Selfish Nodes)

This malicious node which is also known as selfish node and which is not participating in the network operations, use the network for its advantage to enhance performance and save its own resources such as power. To achieve that, selfish node puts forth its existence whenever personal cost is involved. Therefore these selfish node behaviors are known as selective existence attacks. For instance, selfish nodes do not even send any HELLO messages and drop all packets even if they are sent to itself, as long as it does not start the transmission. When a selfish node wants to start a connection with another node, it performs a route discovery and then sends the necessary packets. When the node no longer needs to use the network, it returns to the “silent mode” After a while, neighboring nodes invalidate their own route entries to this node and selfish node becomes invisible on the network.

Actually, dropping packets may be divided into two categories according to the aims of the attacking node. Attacker may want to drop the packets of only the other nodes that it will attack later. To do that it must look at the packet to see whether it comes from this node. If attacker looks at the content of all packets aggregating from the network, it spends CP0055c resource and naturally battery life. This is not desirable behavior for selfish nodes because it spends battery life. Therefore attackers are not interested in the content of the packets if its aim is not to consume its own resources. First category of dropping packets cannot be evaluated as a selfish node behavior. Selective existence is kind of a passive attack, nodes just do not participate in the network operations and they do not change the content of packets.

C. Gray Hole Attack (Routing Misbehavior):

Gray hole attacks is an active attack type, which lead to dropping of messages. Attacking node first agrees to forward packets and then fails to do so. Initially the node behaves correctly and replays true RREP messages to nodes that initiate RREQ message. This way, it takes over the sending packets. Afterwards, the node just drops the packets to launch a (DoS) denial of service attack.

If neighboring nodes that try to send packets over attacking nodes lose the connection to destination then they may want to discover a route again, broadcasting RREQ messages. Attacking node establishes a route, sending RREP messages. This process goes on until malicious node succeeds its aim (e.g. network resource consumption, battery consumption). This attack is known as routing misbehavior.

Dropping packets is also one of the behaviors of failed or overloading nodes. One should not evaluate every dropping packet action as a selective existence, gray or black hole attack. Actually most routing protocols have no mechanism to detect whether data packets have been forwarded, DSR being the only exception.

D. Black Hole Attack:

The Black Hole Attacks compared to Gray Hole Attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole akin to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the center of the wireless network.

If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

Gray hole attacks against one or two nodes in the network to isolate them, where as black hole attack affects the whole network. Moreover, the malicious node that attempts gray hole attacks cannot be perceived easily since it does not send false messages. Behavior of failed or overloaded nodes may seem like selfish nodes attacks or gray hole attacks due to dropping of messages. But, since failed nodes cannot fabricate a new control message, they cannot form a black hole attack although they will drop the message later.

E. Impersonation:

Due to lack of authentication in ad-hoc networks, only MAC or IP addresses uniquely identify hosts. These addresses are not adequate to authenticate the sender node. Therefore non-repudiation is not provided for ad-hoc network protocols. MAC and IP spoofing are the simplest methods to pretend as another node or hide in the network.

Malicious nodes achieve impersonation only by changing the source IP address in the control message. Another reason for impersonation is to persuade nodes to change their routing tables pretending to be a friendly node, such as attacks against routing table.

One of the interesting impersonations is Man-in-the-middle attack . Malicious node performs this attack by combining spoofing and dropping attacks. Physically, it must be placed as the only node within the range for destination, in the middle of the route or victim node must be prevented from receiving any other route information to the destination. Malicious node may also change the routing tables of the victim node to redirect its packets, using attacks against the routing table. At this point, malicious node waits for an RREQ message to the destination node from source node. When source node sends an RREQ message, malicious node drops the RREQ and replays a spoofed RREP message to source node as if it is coming from the destination node.

At the same time, malicious node sends a RREQ message to the destination node and 18 drops the RREP message from the destination node. By doing this; malicious node manages to establish a route both to the source and the destination node and attacker controls the communication between the source and destination. If the communication is encrypted or entails an authentication as to MAC or IP address, malicious node can easily get the up layer communication.

F. Modification Attack:

Control massages are used to establish the shortest and true path between two nodes. But malicious nodes want to route packets to the direction that they want, modifying content of the control messages (e.g. RREQ, RREP and RERR). Modification means that the message does not carry out its normal functions.

Route information such as hop count, sequence number, life time etc. are carried along with control messages. This information has a big role in establishing a true route. Modifying these fields in the control messages, malicious node can perform its own attacks. Impersonation is not one of these kinds of attacks; impersonation is only performed by modifying source address to pretend as another node in the network. But changing route information in control messages is performed to mislead the victim or intermediate node and this modification is generally against the replay messages.

G. Attack Against The Routing Tables:

Every node has its own routing table to find other nodes easily in the network. At the same time, this routing table draws the network topology for each node for a period (max. 3 seconds, duration of ACTIVE_ROUTE_TIMEOUT constant value of AODV protocol). If malicious node attacks against this table, attacked nodes do not find any route to other nodes whom it wants to connect. This attack is always performed by fabricating a new control message. Therefore it is also named fabricating attack.

There are many attacks against routing tables. Each one is done by fabricating false control messages. For example; to attempt a black hole attack, malicious node first invades into the routing table of the victim, sending false RREP message. Malicious node also spreads false RERR messages to the network so that valid working links are marked as broken. Another attack type against the routing table is to attempt to create lots of route entries for non-existent nodes, using RREQ messages. As a result, routing table of the attacked node is full and does not have enough entry to create a new one. This attack type is known as routing table overflow.

Attacks against the routing tables also affect the network integrity, changing the network topology established in the routing tables. Incorrect control messages are disseminated quickly in the network due to route discovery process and influence the network integrity in a wide area. Therefore attacks against the routing table are known as Network Integrity Attacks.

H. Sleep Deprivation Torture Attack (Battery Exhaustion):

Many techniques are used to maximize the battery life and mobile nodes prefer to stay at the sleep mode, when they are not used. Sleep Deprivation Torture is one of the serious types of Denial of Service Attacks, which affects only nodes, especially handheld devices that have limited resources. In a period time, attacker can propagate some control messages through the network, in which other nodes are interested. Other nodes pass to the operation mode from the sleep mode and start processing these unnecessary packets until their batteries completely run out.

III. THE AODV PROTOCOL:

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol provides quick and efficient route establishment between nodes desiring communication and AODV was designed specifically for ad hoc wireless networks. It provides communication between mobile nodes with minimal control overhead and minimal route acquisition latency.

The AODV routing protocol is capable of both unicast and multicast routing. It is an on-demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination, to be included in any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and simplicity in program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

The main advantage of this protocol is that routes are established on demand and destination sequence numbers are used to find the latest route to the destination. The connection setup delay is lower.

One of the disadvantages of this protocol is that intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries. Also multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead. Another disadvantage of AODV is that the periodic beaconing leads to unnecessary bandwidth consumption.

A. AODV Operation:

In AODV, the network is silent until a connection is needed. When the network node needs a connection, it broadcasts a request for it. Other AODV nodes forward this message, and record the node that they heard it from, creating an explosion of temporary routes back to the requesting node. When a node receives this route request message and if it already has a route to the desired node, it sends a message backwards through a temporary route to the requesting node. The requesting node then begins using the route that has the least number of hops through other nodes. Unused entries in the routing tables are recycled after a time. When a link fails, a routing error is passed back to a transmitting node, and the process repeats.

B. Sending ROUTE REQUEST (RREQ):

A node disseminates a RREQ when it determines that it needs a route to a destination and does not have one available. This can happen if the destination is previously unknown to the node or if a previously valid route to the destination expires or is marked as invalid. The Destination Sequence Number field in the RREQ message is the last known destination sequence number for this destination and is copied from the Destination Sequence Number field in the routing table. If no sequence number is known, the unknown sequence number flag MUST be set. The Originator Sequence Number in the RREQ message is the node's own sequence number, which is incremented prior to insertion in a RREQ. The RREQ ID field is incremented by one from the last RREQ ID used by the current node. Each node maintains only one RREQ ID. The Hop Count field is set to zero.Before broadcasting the RREQ, the originating node buffers the RREQ ID and the Originator IP address (its own address) of the RREQ for PATH_DISCOVERY_TIME. In this way, when the node receives the packet again from its neighbors, it will not reprocess and re-forward the packet.

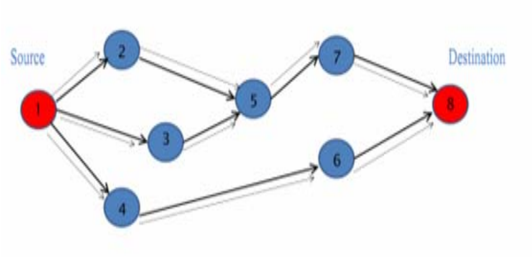


Fig 10: Propagation of route request

C. Forwarding RREQ:

When a node receives a RREQ, it first creates or updates a route to the previous hop without a valid sequence number then checks to determine whether it has received a RREQ with the same Originator IP Address and RREQ ID within at least the last PATH_DISCOVERY_TIME. If such a RREQ has been received, the node silently discards the newly received RREQ. If it needs to forward, it first increments the hop count value in the RREQ by one to account for the new hop through the intermediate node.

D. Generating ROUTE REPLY (RREP):

A node generates a RREP if either:

i. *It is itself the destination, or it has an active route to the destination, the destination sequence number in the node's existing route table entry for the destination is valid and greater than or equal to the*

E. *Destination Sequence Number of the RREQ.*

When generating a RREP message, a node copies the Destination IP Address and the Originator Sequence Number from the RREQ message into the corresponding fields in the RREP message. Once created, the RREP is unicast to the next hop towards the originator of the RREQ, as indicated by the route table entry for that originator. As the RREP is forwarded back towards the node which originated the RREQ message, the Hop Count field is incremented by one at each hop. Thus, when the RREP reaches the originator, the Hop Count represents the distance, in hops, of the destination from the originator.

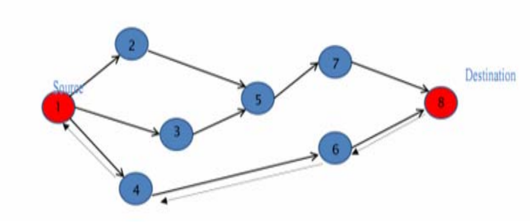


Fig 11: Propagation of Route reply packet

F. Route Reply Generation by the Destination:

If the generating node is the destination itself, it must increment its own sequence number by one if the sequence number in the RREQ packet is equal to that incremented value. Otherwise, the destination does not change its sequence number before generating the RREP message. The destination node places its (perhaps newly incremented) sequence number into the Destination Sequence Number field of the RREP, and enters the value zero in the Hop Count field of the RREP.

G. Route Reply Generation by an Intermediate Node:

If the node generating the RREP is not the destination node, but is an intermediate hop along the path from the originator to the destination, it copies its known sequence number for the destination into the Destination Sequence Number field in the RREP message. The intermediate node places its distance in hops from the destination (indicated by the hop count in the routing table) Count field in the RREP. The Lifetime field of the RREP is calculated by subtracting the current time from the expiration time in its route table entry.

H. Receiving and Forwarding Route Replies:

When a node receives a RREP message, it searches (using longest prefix matching) for a route to the previous hop. If needed, a route is created for the previous hop, but without a valid sequence number. Next, the node increments the hop count value in the RREP by one to account for the new hop through the intermediate node. The node consults its route table entry for the originating node to determine the next hop for the RREP packet, and then forwards the RREP towards the originator using the information in that route table entry. If a node forwards a RREP over a link that is likely to have errors or be unidirectional, the node should set the 'A' flag to require that the recipient of the RREP acknowledge receipt of the RREP by sending a RREP-ACK message back.

IV. BLACK HOLE ATTACK:

In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behavior in the scenario of the figures of the previous section.

In this scenario shown in Figure 11, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets.

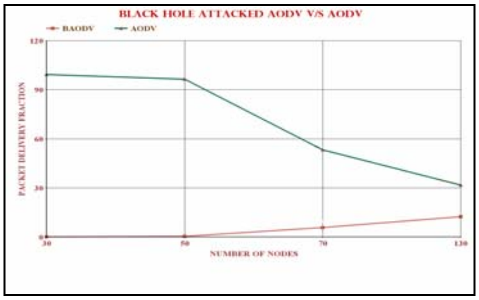
In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets. In our scenarios we use UDP data packets.

V. PERFORMANCE METRICS:

A. Packet Delivery Fraction:

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

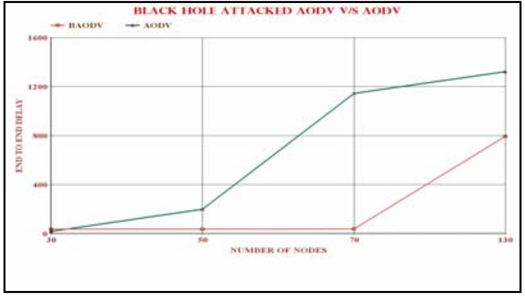
∑ Number of packet receive / ∑ Number of packet send



B.Average e-e delay (ms):

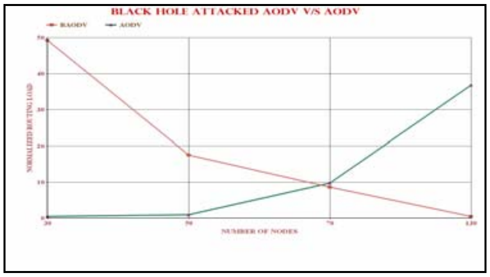
The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections



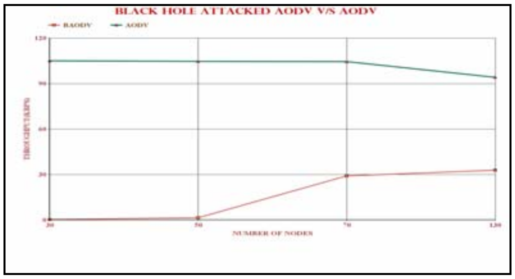
C. Normalized Routing Load:

The sum of the routing control messages such as RREQ, RREP, RRER, and HELLO called normalized routing load etc, counted by k bit/s.



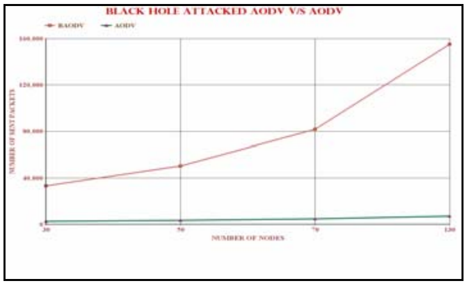
D. Average Throughput [kbps]:

Throughput is the amount of data moved successfully from one place to another in a given time period.



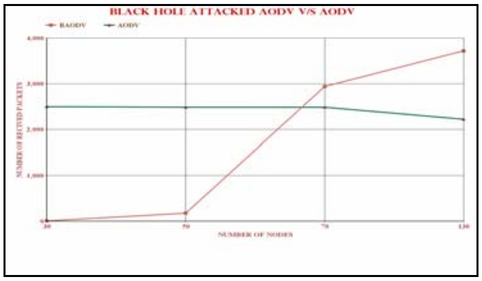
E. Number of sent packets:

The total number of sent packets from all the source node(s) in the simulation is called as the Number of sent Packets.



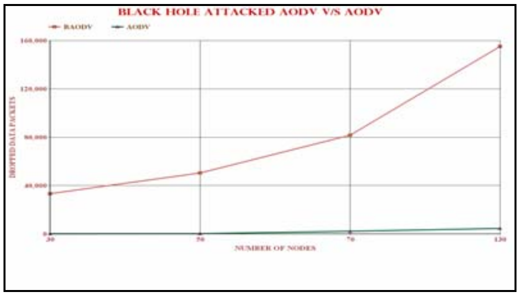
F. Number of received packets:

The total number of received packets from all the destination node(s) in the simulation is called as the Number of Received Packets



G. Number of dropped data (packets):

The total number of packets dropped from all the nodes during the simulation is called number of dropped packets.

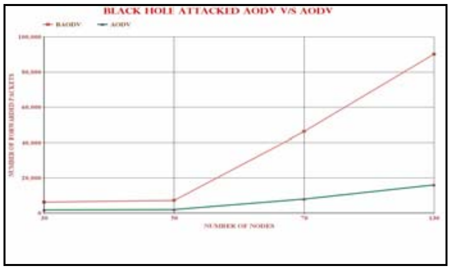


H. Number of dropped data (KBPS):

The number of dropped packets gives the measure of the packets which are discarded due to congestion and duplication at the nodes.

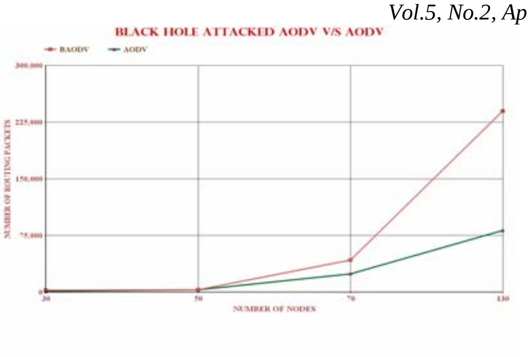
I. Number of forwarded packets:

The total number of forwards packets from all the nodes (except that packet source and destination) in the simulation is called as the Number of forwarded Packets.



J. Routing packets:

The total number of routing packets from all the nodes in the simulation is called as the Number of Routing Packets.



VII. CONCLUSION

performance of AODV, Black hole AODV routing protocols for ad-hoc networks using ns-2 simulations. AODV, Black hole AODV use the reactive On-demand routing strategy. In this paper developed a new routing protocol with malicious nodes. In case of non cooperating nodes i.e. AODV, black hole AODV .AODV performs better than black hole AODV as black hole AODV contains malicious nodes the no of dropped packets will be high its performance is low.

REFERENCES

[1] http://en.wikipedia.org/wiki/Personal_area_network, 25 July 2005.

[2] T. Franklin, “Wireless Local Area Networks”, Technical Report http://www.jisc.ac.uk /uploaded_documents/WirelessLANTechRep.pdf. 25 July 2005.

[3] J. Reynold, “Going Wi-Fi”, Chapter 6, The Wi-Fi Standards Spelled out, Pg. 77.

[4] http://certifications.wi-fi.org/wbcs_certified_products.php 25 July 2005.

[5] P. Misra,. “Routing Protocols for Ad Hoc Mobile Wireless Networks”, http://www.cse.wustl.edu/~jain/cis788-99/adhoc_routing/index.html, 14 May 2006.

[6] P. Yau and C. J. Mitchell, “Security Vulnerabilities in Adhoc Network”.

[7] G. Vigna, S. Gwalani and K. Srinivasan, “An Intrusion Detection Tool for AODV-Based Ad hoc Wireless Networks”, Proc. of the 20th Annual Computer Security Applications Conference (ACSAC’04).

[8] P. Ning and K. Sun, “How to Misuse AODV: A Case Study of Insider Attacks Against Mobile Ad-Hoc Routing Protocols”, Proc.of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY., June 2003.

[9] S. Marti, T. J. Giuli, K. Lai and M. Baker, “Mitigating Routing Misbehavior in Ad Hoc Networks”, Proc. 6th Annual Int’l. Conf. Mobile Comp. and Net., Boston, MA. pp. 255-265. August 2000. 51

[10] D. Johnson, D. Maltz and J. Broch, “DSR the Dynamic Source Routing Protocol for Multihop 2001.

[11] H. Deng Wireless Ad Hoc Networks”. Ad Hoc networking, Chapter 5, page 139-172. Addison-Wesley, W. Li and D. P. Agrawal, “Routing Security inWireless Ad Hoc Networks”. University of Cincinnati, IEEE Communication Magazine, October 2002.

[12] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks”, Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science, 1999. University of Cambridge Computer Laboratory.

[13] C.Perkins, “(RFC) Request for Comments– 3561”,Category: Experimental, Network, Working Group, July 2003.

[14] K Fall and K. Varadhan, The NS Manual, November 18, 2005, http://www.isi.edu/nsnam/ns/doc/ns_doc.pdf.25July2005.

AUTHORS PROFILE

Dr. Nirmala Devi .L received B.E and M.E degrees from Osmaia university 1997,2005, and Ph.D degree in Electronics and Communication Engineering 2014 in the area " Optical Netwotks" from Osmania University Hyderabad, India.

She joined in Department of Electronics and Communication Engineering Osmania University, Hyderabad, India in the year 2007.

She has published many research papers in national and international conferences and journal, her area of interest is Wireless communication networks, Wireless sensor network and Optical networks.