ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

# Energy Efficient Applications and Performance Comparison between Routing Protocol for MANET

D.Balaji, J.Sampathkumar

Assistant Professor, Dept. of ECE, Mahendra College of Engineering, Salem, India

Assistant Professor, Dept. of ECE, Mahendra College of Engineering, Salem, India

**ABSTRACT:** A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. The solutions may not always be sufficient, as ad-hoc networks have their own vulnerabilities that cannot be addressed by these solutions. Some malicious nodes pretend to be intermediate nodes of a route to some given destinations, drop any packet that subsequently goes through it, is one of the major types of attack. We introduce a analysis method to detect malicious nodes in MANETs. The mechanism is cooperative were the protocol work cooperatively together so that they can analyze, detect malicious nodes in a reliable manner. We verify our method by running simulations with mobile nodes using Ad-hoc on-demand Distance Vector (AODV) routing, Dynamic Source Routing (DSR), Optimized Link State Routing Protocol (OLSR) and *Destination-Sequenced Distance-Vector* Routing (*DSDV*) on comparison with each other performance. It is observed that the malicious node detection rate is very good; the overhead detection rate is low, packet delivery ratio is little bit high and also the response time is observed when there is a change of mobility speed.

**KEYWORDS:** MANET, Black hole, AODV, DSR, DSDV, OLSR

## I. INTRODUCTION

A Mobile Ad-hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets [1]. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other, however the node 2 can be used to forward packets between node 1and node 2. The node 2 will act as a router and these three nodes together form an ad- hoc network.

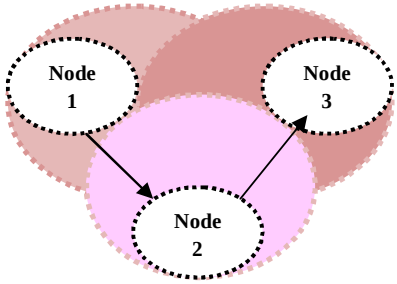



**Fig 2: MANET**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

These networks are faced with the traditional problems inherent to wireless communications such as lower reliability than wired media, limited physical security, time-varying channels, interference, etc [3]. Despite the many design constraints, mobile ad hoc networks offer numerous advantages. A number of proposed solutions attempt to have an up-to-date route to all other nodes at all times. Therefore, reactive routing protocols only set up routes to nodes they communicate with and these routes are kept alive as long as they are needed. Combinations of proactive and reactive protocols, where nearby routes (for example, maximum two hops) are kept up-to-date proactively, while far-away routes are set up reactively, are also possible and fall in the category of hybrid routing protocols. A completely different approach is taken by the location-based routing protocols, where packet forwarding is based on the location of a node's communication partner.

## II. ATTACK ON ROUTING

Two possible threats from malicious nodes are misdirection of traffic, one of the consequences of which may be denial of service, or denial of service as a means to an end itself [2]. These threats can be further subdivided, as in the attack model shown in Figure 2.

Attacks arising from malicious behavior can be divided in to those where packets are originated by the malicious node, and those where a malicious node is an intermediate node and receives control packets for for-warding [5]. When a malicious node is originating packets, it can send control packets using its own source address, an address which belongs to an existing node in the ad hoc network, or an arbitrary address which does not belong to any node. Malicious intermediate nodes can either modify or replay received packets.

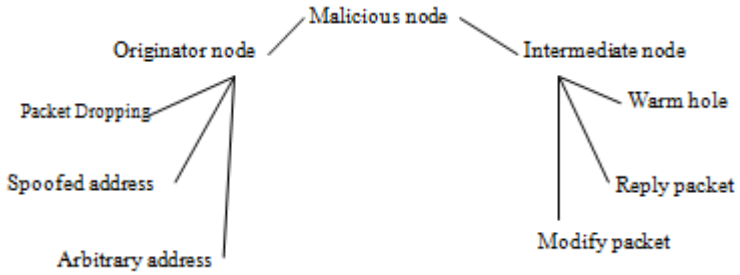



**Fig 2: Malicious attack tree**

This section concentrates on possible attacks on the various mechanisms used to discover and maintain routes in both proactive and reactive protocols [4]. In particular, we investigate if the type of routing protocol used has a bearing on the effort needed to successfully perform such attacks.

### *A. WORMHOLE ATTACK*

In a wormhole attack, an attacker receives packets at one point in the network, tunnels them to another point in the network and then replays them into the network from that point. For tunneled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunneled packet arrive sooner than other packets transmitted over a normal multichip route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker[7]. It is also possible for the attacker to forward each bit over the worm hole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network and the attacker could exploit this position in a variety of ways; the attacker can also still perform the attack even if the network communication provides confidentiality and authenticity and even if the attacker does not have any cryptographic keys.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

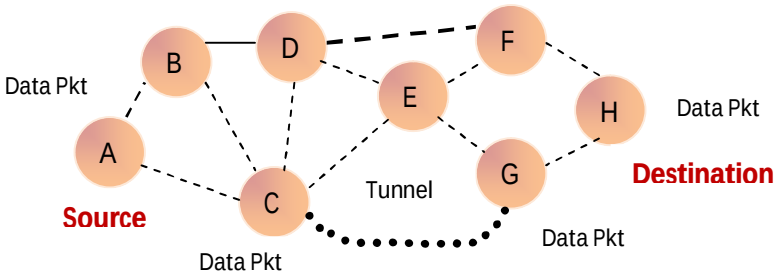



**Fig 3: Wormhole attack**

## III. PROPOSED SOLUTION

To detect the malicious node we have proposed four methods which use a reactive routing protocol known as Ad hoc On-demand Distance Vector (AODV), DSR, Optimized Link State Routing Protocol (OLSR) and Destination-Sequenced Distance-Vector Routing *(*DSDV) routing for analysis of the effect of the black hole attack when the destination sequence number is changed via simulation.

### ILLUSTRATION

When an intermediate node receives a RREP checks if the difference between the Dst_Seq present in the RREP message and the sequence no present in its table is greater than some predefined threshold value, if so then the intermediate node stops forwarding the message and mark the node as „M" or malicious in the status table (ST) and send a notification message (NM) to source node along with the malicious node"s id and neighbor list of the malicious node[9]. Node 6 keeps track of the status of each neighbor node in the ST whether it is a safe node or a malicious one.

**STEPS:**

- *IN receives the RREQ check*
  *If*
  ***RREQ <= Dst_Seq***
  ***Send RREP with the Dst_Seq in SnT***
  *Else*
  ***Broadcast the updated RREQ***
- *IN receives RREP Check*
  *If (Dst_Seq in RREP -Dst_Seq in SnT) >Thr*
  ***ST and make the status as „M***
  *Else*
  ***the status as „S" and forward RREP.***
- *NM, SN broadcast a Further Detection message to all M1HNs*
  *If MN sends a RREP to M1HN*
  ***M1HN send a Test packet to SN via this route***
  *Else*
  ***M1HN send an acknowledgement packet (AP)***
- *SN waits for „wt" time*
  *If a Test Packet is received*
  ***id to FT and set flag as „Y".***
  *Else*
  ***then add the source node id to FT***
- *If all the flags are „N", updates its status table (ST) by adding MN"s id and setting Status as „B".*

*Else*

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

***Set the status as „S".***

### *A. REACTIVE - AD-HOC ON DEMAND DISTANCE VECTOR*

AODV, like all reactive protocols, is that topology information is only transmitted by nodes on-demand. When a node wishes to transmit traffic to a host to which it has no route, it will generate a route request (RREQ) message that will be flooded in a limited way to other nodes[11,6]. AODV avoids the ``counting to infinity'' problem from the classical distance vector algorithm by using sequence numbers for every route. AODV defines three types of control messages for route maintenance:

**RREQ** - A route request message is transmitted by a node requiring a route to a node. Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded.

**RREP** - A route reply message is uni casted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address [8].

**RERR** - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. A possible path for a route replies if A wishes to find a route to J.

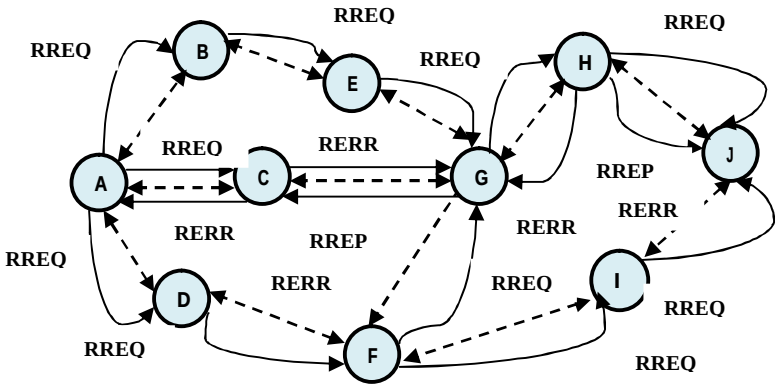



**Fig 4: Malicious attack tree**

### *B. REACTIVE - DYNAMIC SOURCE ROUTING*

A source routing protocol must solve two challenges, which DSR terms Route Discovery and Route Maintenance. Route Discovery is the mechanism whereby a node S wishing to send a packet to a destination D obtains a source route to D [13, 10]. When Route Maintenance indicates a source route is broken, S can attempt to use any other route it happens to know to D, or can invoke Route Discovery again to find a new route.

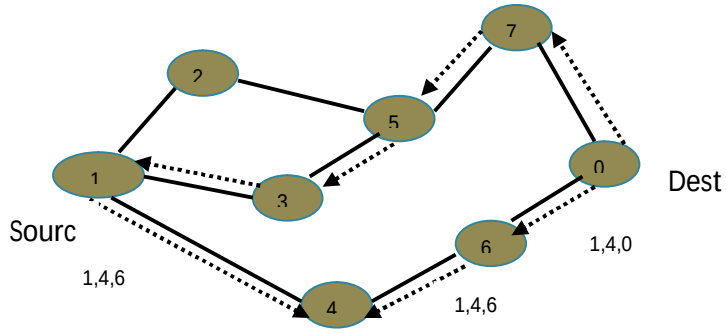



**Fig 5: Route Discovery**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

The basic mechanism of forwarding Route Requests forwards the Request if the node (1) is not the target of the Request and (2) is not already listed. Also, the Time-to-Live field in the IP header of the packet carrying the Route Request may be used to limit the scope over which the Request will propagate, using the normal behavior of Time-to-Live defined by IP.

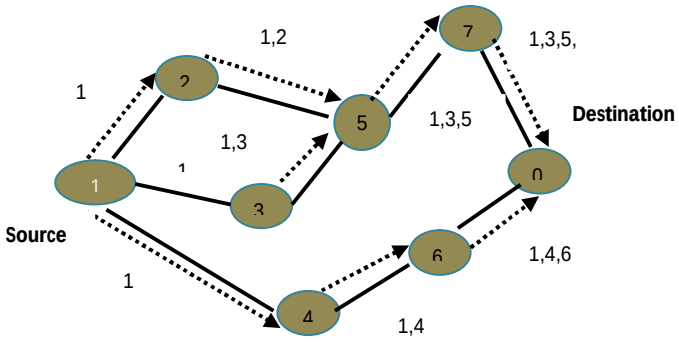



**Fig 6: Route Request**

All source routes learned by a node are kept in a Route Cache, which is used to further reduce the cost of Route Discovery. Further, when a node B receives a Route Request from S for another node D, B searches its own Route Cache for a route to D. If B finds such a route, it does not propagate the Route Request, but instead returns a Route Reply to node S based on the concatenation of the recorded source route from S to B in the Route Request and the cached route from B to D.

***C. OPTIMIZED LINK STATE ROUTING (OLSR)***

It is a table-driven pro-active protocol. As the name suggests, it uses the link-state scheme in an optimized manner to diffuse topology information. In a classic link-state algorithm, link-state information is flooded throughout the network. OLSR uses this approach as well, but since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. The route calculation itself is also driven by the tables.OLSR defines three basic types of control messages.

**HELLO** - HELLO messages are transmitted to all neighbors. These messages are used for neighbor sensing and MPR calculation.

**TC** - Topology Control messages are the link state signaling done by OLSR. This messaging is optimized in several ways using MPRs.

**MID** - Multiple Interface Declaration messages are transmitted by nodes running OLSR on more than one interface. These messages list all IP addresses used by a node.

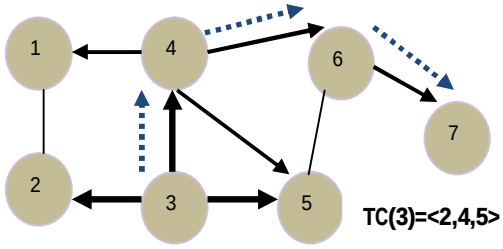



**Fig 7:OLSR Routing**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

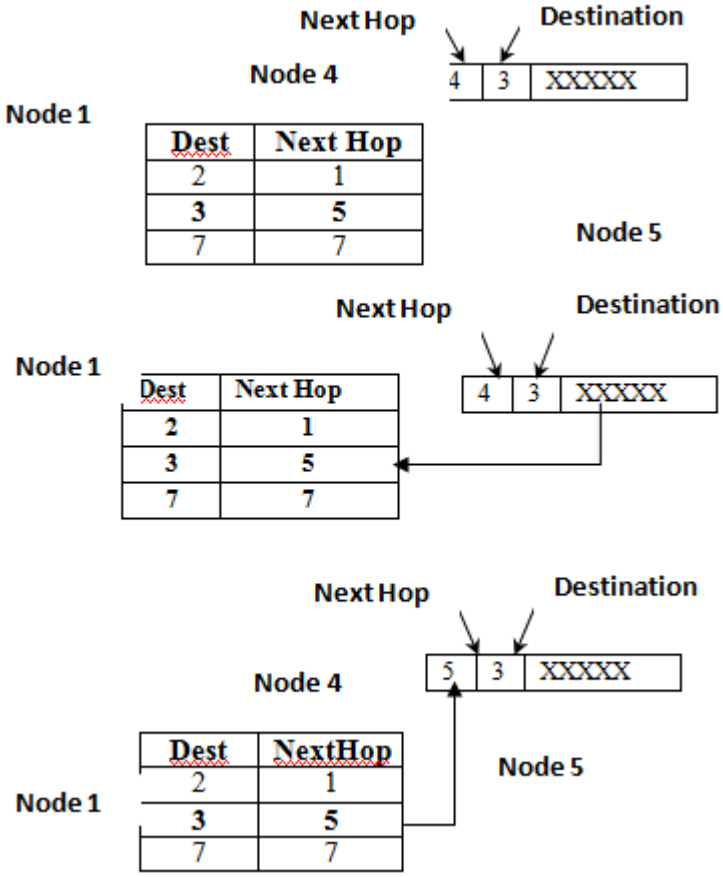
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Node 3 sends a TC message to nodes in MS (3) = {2, 4, and 5}. Since Node 3 is in MS (4) = {1, 3, 5, 6}, Node 4 will forward Node 3's TC (3) message to the rest of MS(4). Node 6 also forwards TC (3) message from Node 4 since Node 4 is in MS (6) = {4, 5, 7}.

***D. DESTINATION-SEQUENCED DISTANCE-VECTOR ROUTING (DSDV)***

It is an adaptation of conventional IP routing protocols to ad hoc networks. DSDV is based on RIP, used for routing in parts of the Internet. In DSDV, packets are routed between nodes of an ad hoc network using routing tables stored at each node. Each routing table contains a list of the addresses of every other node in the network. Along with each node's address, the table contains the address of the next hop for a packet to take in order to reach the node. In this example, a packet is being sent from node 1 to node 3 (node 3 is not shown). From node 1, the next hop for the packet is node 4 a). When node 4 receives the packet, it looks up the destination address (node 3) in its routing table b). Node 4 then transmits the packet to the next hop as specified in the table, in this case node 5 c). This procedure is repeated as required until the packet finally reaches its destination.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

## IV.RESULTS AND DISCUSSION

Our experiments using NS-2 version 2.34, a scalable simulation environment for network systems. The routing protocol we use is AODV. Our simulated network consists of 100 mobile nodes placed randomly within a 1000 m x 1000 m area. All nodes have the same transmission range of 250 meters. The channel capacity is 2 Mbps. The random waypoint model was used in the simulation runs. In this model, a node selects a destination randomly within the roaming area and moves towards that destination at a predefined speed 10, 20, 30, 40 and 50m/s.

Once the node arrives at the destination, it pauses at the current position for 10 seconds. The node then selects another destination randomly and moves towards it, pausing there for 10seconds, and so on. Each simulation executed for 70 seconds of simulation time. The traffic used is UDP/CBR traffic between random node pairs. The size of data payload is 512 bytes. Multiple runs with different seed numbers were conducted for each scenario and measurements were averaged over those runs.

In our experiment we have assumed 5 percent of the number of nodes as malicious i.e. 3 nodes are malicious for 50 nodes, 5 nodes are malicious for 100 nodes and 7 nodes are malicious for 150 nodes. We study the detecting technique of the packet delivery ratio, overhead and response time for 50 node network, 100 node network and 150 node network. We run the simulation 5 times and all the data are plotted using MATLAB, averaged from the 5 runs.

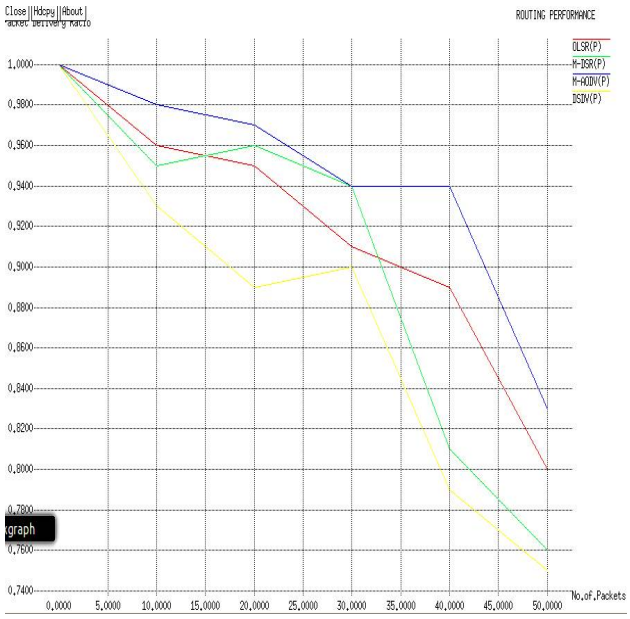



**Fig.7. Routing Performance analysis**

Fig.7 shows that the routing performance where the comparison with proactive and reactive protocols were AODV routing has decrease in increase with the number of malicious node. Since the graph explains the performance of routing in varies proceeded routing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

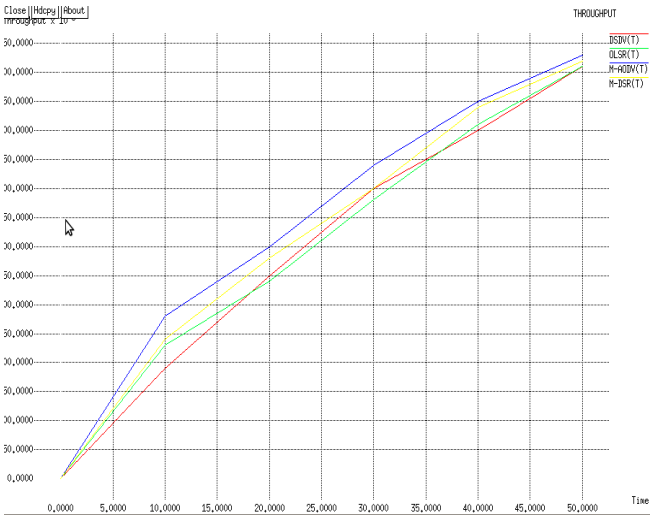



**Fig.8. Average-End to End Delay**

The Fig 8 shows the packet delivery ratio for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively. The packet delivery ratio is shown as a function of mobility speed. As the number of nodes increases and malicious node increases, the packet delivery ratio decreases with the varying of mobility speed.

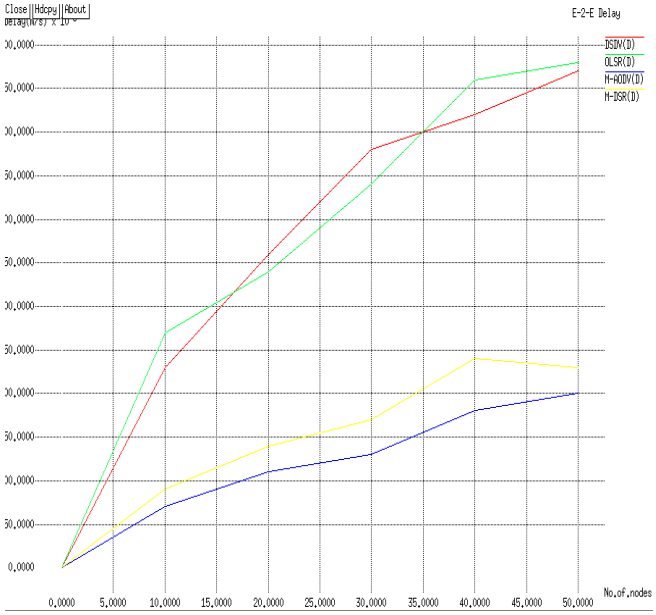



**Fig.9 Comparison of Throughput**

The Fig 9 shows the throughput for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively. The throughput is shown as a function of mobility speed. As the number of nodes increases and malicious node increases, the throughput decreases with the varying of mobility speed.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

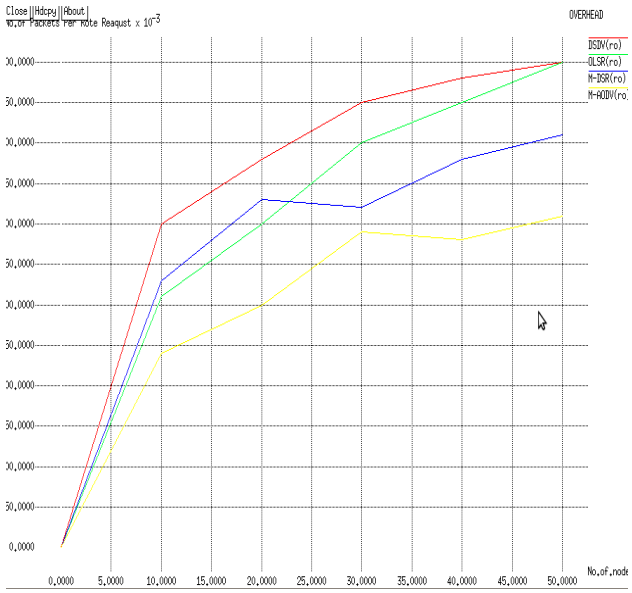



**Fig.10 Comparison of Routing Overhead**

The Fig 10 shows the routing overhead for the network having 50 nodes, network having 100 nodes, network having 150 nodes respectively. The response time is shown as a function of mobility speed. In our experiment we have taken the random way point model which changes the position of the node arbitrarily. So the routing overhead arbitrarily when the number of nodes increases and malicious node increases.

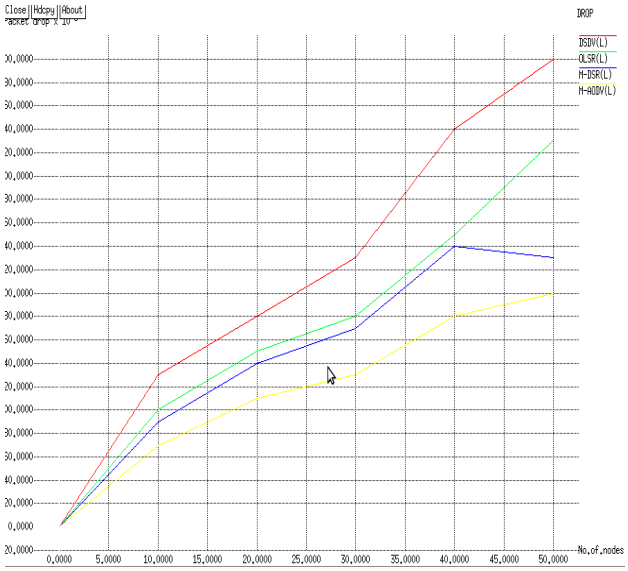



**Fig.11 Comparison of Packet loss ratio**

Fig 11 shows the packet loss ratio in two different scenarios i.e. for proposed model and the existing model As the mobility speed increases, the packet loss ratio increases in both the cases. But from the graph it is cleared that the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 4, Issue 2, February 2016**

packet delivery ratio for the mobility speed 10, 20, 30 m/s of the proposed model is improved as compared whereas for the mobility speed 40 and 50 m/s, it is decreasing as compared to the existing one.

## IV. CONCLUSION AND FURTURE WORK

Black hole attack is one of the most important security problems in MANET. The black hole attack causes dropping of data packets by malicious nodes in the path source to destination. In this paper, we have analyzed the black hole attack and detected the malicious nodes. This paper is proposed to minimize the number of data packet dropping. Also it reduces false detection rate. This is a reliable algorithm since all mobile nodes cooperate together to analyze and detect possible multiple black hole nodes. The proposed scheme in this thesis work has been implemented to minimize the number of data packet dropping in the network and improves the efficiency of the network.

## REFERENCES

[1] Kiran Salunke, Gajanan Rawalkar, Prof. S.J. Bhosale, "Implementing And Comparing DSR And DSDV Routing Protocols For Mobile Ad Hoc Networking" International Journal of Advanced Technology & Engineering Research (IJATER), Volume 2, Issue 2, May 2012

[2] Yi Wang et.al, "Cluster based Location - Aware routing Protocol for Large Scale Heterogeneous MANET", in Proceeding of the Second International Multi symposium on Computer and Computational Sciences, IEEE Computer Society, 2007, pp.366-373

[3] Mayur Tokekar and Radhika D. Joshi "Extension Of Optimized Linked State Routing Protocol for Energy Efficient Applications" International Journal on Adhoc Networking Systems (IJANS) Vol. 1, No. 2, October 2011.

[4] Philip J. Taylor, "Specification of policy languages for network routing protocols in the Bellman-Ford family", Sept 2011.

[5]K.Thamizhmaran, R.Santosh Kumar Mahto, V.SanjeshKumarTripathi, "Performance analysis of secure routing Protocols in MANET" Vol. 1 Issue 9, pp 651-654, Nov 2012.

[6] A. Boomarani, V.R.Sarma Dhulipala , and RM.Chandrasekaran" Throughput and Delay Comparison of MANET Routing Protocols" Int. J. Open Problems Compt. Math., Vol. 2, No. 3, September 2009 ISSN 1998-6262

[7]Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas "Routing Protocols in Wireless Sensor Networks" 26 October 2009

[8] M. Sharma, Prof. Rajeshwar Lal, V.M. Shrimal,"Comparison Of Different Routing Protocols (DSR & AODV)On Behalf Of Evaluation Of Different Routing Parameters With Constraints", IJCNWC, ISSN: 2250-3501 Vol.2, No.3, June 2012

[9] Banoj KumarPanda , Bibhudatta Dash , Rupanita Das , Ajit Sarangi "Mobility and its impact on Performance of AODV and DSR in Mobile Ad hoc Network", IEEE -2012

[10] Mrs. Geetha V, Dr. Sridhar Aithal, Dr. k.chandraSekaram "Effect of Mobility over Performance of the Ad hoc Networks", IEEE-2006

[11]Kapil Suchdeo, Durgesh Kumar Mishra "Comparison of On-Demand Routing Protocols" IEEE FourthAsia International Conference on Mathematical /Analytical Modeling & Computer Simulation, pp 556-560, 2010

[12] Mohammed Bouhorma, H. Bentaouit, A. Boudhir "Performance Comparison of Ad hoc Routing Protocols AODV & DSR" IEEE-2009.