

## International Journal of Computer Science and Mobile Computing



A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

*IJCSMC, Vol. 3, Issue. 7, July 2014, pg.474 – 486*

### **RESEARCH ARTICLE**

# **SIMULATION AND PERFORMANCE ANALYSIS OF AODV PROTOCOL IN MANET**

**Munisha<sup>1</sup>, Deepak Goyal<sup>2</sup>**

<sup>1</sup>M.Tech Student, Vaish College of Engineering, MDU, Rohtak, Haryana (India)

<sup>2</sup>Asst. Prof., Vaish College of Engineering, MDU, Rohtak, Haryana (India)

[manishabnwl@gmail.com](mailto:manishabnwl@gmail.com)

*Abstract: The Mobile Ad-hoc Networks (MANETs) is an network consisting of wireless mobile nodes without any pre-existing infrastructure or the aid of any centralized administration. MANET is a self configuring network and the topology of the network is dynamic or keeps on changing as the nodes move randomly. MANET is a collection of mobile nodes that move randomly. There are many protocols for such networks. One such protocol is Ad-hoc On Demand Distance Vector (AODV) routing protocol. Among all other protocols AODV is preferred because it minimizes the routing overhead and hence enhance the performance of the network. We have presented a simulation study which shows that Enhanced AODV works better then basic AODV when malicious node found. we have shown the performance of AODV protocol for the parameter, packet delivery ratio and packet loss ratio. As we increase the number of nodes for performing the simulation of AODV routing protocol, number of sent, routing and delivered packets changes hence the performance parameters changes.*

*Index Terms – MANET, Security, DSR, AODV*

## **1. INTRODUCTION**

Wireless networks provide mobile users with ubiquitous communication capability and information access regardless of its location and physical connection. It uses radio transmission as the means for transmitting data. Wireless communication can be classified as: Infrastructured network and Infrastructureless network. Mobile Ad-hoc network is infrastructureless network. It is a collection of nodes that move randomly and dynamically [1]. Due to the mobile and dynamic nature of the nodes the network topology keeps on changing. Each node in the network acts as a host and a router forwarding and receiving packets from the other nodes that may not be in the transmission range of the network. The nodes in mobile ad-hoc networks

discover other nodes dynamically. Routing in such networks is a difficult task due to the highly dynamic network topology. The objective of deploying these networks is to provide communication in areas where limited or no connectivity or any communication infrastructure exists. These ad-hoc networks are flexible and adaptive and can be employed in military rescue operations, interactive lectures, business sharing information and emergency situations [2]. The features of mobile ad-hoc networks are highly dynamic topology, bandwidth constrained links, limited physical security and energy constrained nodes. A MANET uses multi-hop routing for providing connectivity. Many protocols have been proposed so far. One such protocol is Ad-hoc On Demand Distance Vector (AODV) routing protocol. Among all other protocols AODV is preferred because it minimizes the routing overhead and hence enhance the performance of the network. In this paper, the performance analysis of AODV routing protocol is done on the basis of few performance metric parameters such as packet delivery ratio and packet loss ratio. The paper is structured as follows: In Section 2, MANET routing protocols are discussed. In Section 3, overview of AODV routing protocol is given. In Section 4, proposed algorithm is described and in Section 5, results and analysis are described.

## 2. Types of Routing Protocols in MANETs

MANET routing protocols are classified as following:

### Table Driven (Proactive) Routing protocols

In Table Driven protocols, every node maintains one or more tables containing routing information to every node in the network. Every node updates these tables to maintain a consistent and up-to-date view of the network. These protocols are also called as proactive routing protocols because routing information is maintained by them even before it is required. These protocols maintain node entries for each node in the form of table so it causes more overhead in the routing table which leads to more bandwidth consumption. Table Driven Protocols are: Destination Sequence Distance Vector (DSDV) routing, Cluster-head Gateway Switch Routing (CGSR) and Wireless Routing Protocol (WRP) [1]. There are some differences among these protocols on the basis of routing information being updated in each routing table.

**On Demand (Reactive) Routing protocols** In the On-Demand approach, when a node desires a route to a new destination, it will have to wait until such a route can be discovered i.e. routes are discovered whenever a source node has packets to send. The various on demand driven based routing protocols are as follows:

- a) Dynamic Source Routing (DSR)
- b) Ad Hoc On Demand Distance Vector Routing (AODV)

On demand protocols obtain routes only on demand. The routes are created when desired by the source node. Whenever a node requires a route to destination a route discovery process is initiated within the network. This process is completed once a route is found. Once a route is established, it is maintained by a route maintenance procedure. On demand routing protocols include: Dynamic Source Routing protocol, the Ad-hoc On demand Distance Vector protocol, the Temporally Ordered Routing Algorithm (TORA), and the Associativity Based Routing (ABR) protocol [1].

### Hybrid Routing Protocols

In this, various routing protocols are combined to form a single protocol. ZRP (Zone Routing Protocol) is one of the hybrid protocols which are the combination of table-driven and on-demand routing protocol. It has the characteristics of adaptive to network conditions [3]. Some of the major characteristics of mobile ad hoc routing protocols are:

**Dynamic Network topology:** When the nodes move, the topology changes rapidly and the connectivity within the network varies with time.

**Limited Bandwidth:** The available bandwidth [4] of such networks is limited than that of wired networks. The power is limited and the computation should be energy efficient.

**Distributed Operation:** Nodes collaborate them to implement functions and not a single node is solely responsible for the overall operation.

**Security:** There is a problem of security in MANET. Various attacks such as eavesdropping, replay attacks, denial of services are possible. MANETs are resource constrained, bandwidth constrained and as the nodes are mobile, the network topology changes dynamically. Therefore routing must be done and there is a need of efficient routing protocols.

### 3. AODV (AD HOC ON DEMAND DISTANCE VECTOR)

Routing protocols in MANET are divided into two basic classes:

- Proactive routing protocols and
- Reactive routing protocols

In ad hoc networks Routing protocols can be classified into two major types: proactive and Reactive protocols. Proactive protocols maintain up-to-date routing information to all nodes by periodically disseminating topology updates throughout the network. But on demand (Reactive) protocols attempt to discover a route only when a route is required. To minimize the overhead and the latency of initiating a route discovery for each packet, reactive protocols use route Caches. Due to mobility, cached routes easily become stale. In conventional wired networks Routing protocols generally use either distance vector or link state routing algorithms, both of which require periodic routing advertisements to be broadcast by each router. AODV [5] is based on DSDV and DSR protocols and It keeps Routing tables. Route between the two nodes is discovered only when needed. When a source  $S_i$  node wants to send a packet to the destination node  $D_i$ , it first checks its routing table and if there is no entry, it initiates route discovery process. It broadcasts a route request (RREQ) packet to all its neighbors [6]. The RREQ contains IP addresses of source( $S_i$ ) and destination( $D_i$ ) node, current sequence number of source( $S_i$ ) and last known sequence number of  $D_i$ , a broadcast ID from  $S_i$ , which is incremented each time  $S_i$  sends a RREQ message. The broadcast ID, IP address pair of the source  $S_i$  forms a unique identifier for the RREQ. AODV utilizes destination sequence numbers to guarantee the fresh route in the network. When a node broadcast RREQ message, it waits for RREP message. If the reply is not received within certain time limit, the source node rebroadcast the RREQ message or it assumes route is not present. When a node receives a RREQ message, it broadcast the RREQ message to its neighbour if it is not the destination route and creates a temporary reverse route to the source IP address in its routing table with next hope equal to the IP address of neighboring node that sent the RREQ message. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ. Once the RREQ reaches the destination, it generates RREP and it is unicasted back to the requesting node which eventually reaches the source node. In the networks the intermediate node records the route to the destination as the RREP follows from destination to source. The nodes are random and mobile, so they can move anytime. If the source node moves to different position, it can rediscover the route the destination node by route discovery process. If the destination node or the intermediate node moves to different position [7], it informs the upstream node through Route error message which eventually reaches the source node. The source node stops the ongoing communication and initiate route discovery process. Hello messages are used to maintain the local connectivity in the network. Ad hoc on demand distance vector protocol reduces number of routing messages in the network. It manages the dynamic behavior of the nodes. However there is possibility of various attacks on AODV routing protocol. Characteristics of AODV are Unicast, Broadcast, and Multicast communication, On-demand route establishment with small delay. Multicast trees connecting group members maintained for lifetime of multicast group, Link breakages in active routes efficiently repaired.

All routes are loop-free through use of sequence numbers, Use of Sequence numbers to track accuracy of information, Only keeps track of next hop for a route instead of the entire route, Use of periodic HELLO messages to track neighbors.

### 4. Enhanced AODV Protocol in MANET

If there is any malicious nodes present in the system it can easily corrupt the system. The Stale routes cause packet losses if packets cannot be salvaged by intermediate nodes. AODV fails to protect the destination from malicious node or misbehaving node. Any node that exists in same network can easily corrupt other nodes. Therefore we enhance the basic AODV algorithm.

#### Enhance AODV Algorithm

- 1) Call Root Discovery Algorithm ( $S_i$ ,  $D_i$ )
- 2) Malicious node Identification
  - a) Delay period  $d = D \times (h-1 + r)$   
 $D$  : small constant delay,

- h: number of hops
- r : random number (0~1)
- b) Call AODV Failure-Node Detection (I)

3) Proposed Algorithm for blocking the malicious node

First **ROOTDISCOVERY (Si, Di)** is called to find the root from source to destination.

**1. Algorithm for RootDiscovery(Si,K, Di)**

```

/* Define the Source Node Si and Destination Node Di. K is the intermediate node*/
{
If (Si=Di)
{
Then Return "Success"
}
Else
{ Message will be broadcast by node Si to all surrounding nodes and get Response time and Load
Find Node with Minimum Load and Minimum Cost called Node K
If (Reply Status (K) = true)
{
set K= Current Node
RootDiscovery(K,Di)
}
}
}

```

**2. Malicious Node Identification**

This algorithm is developed to enhance the performance. There we calculate the delay and also numbers of hops are present which used to send the data to destination. If any nodes deliver the packets beyond delay time then we block that node temporarily and that node is not used for sending the data.

**Algorithm for AODV Failure-NodeDetection(I)**

```

DSR Failure-NodeDetection(I)
/* I is the Node over the network*/
{
A node will send a packet to Node I with defined hop time and wait for the acknowledgement.
if (Check(REPLY)!=NULL)
{
If (Reply Time (IO)< Hop Time)
{
Then Return True;
}
else
{
Return False;
}
}
else
{
return Failure Node in network;
}
}
if(Forward(Message)=true)
{
Then return true;
}
else

```

```
return failure node in network;  
}
```

If REPLY send by any node is not NULL then Hop Time will be checked. In this maximum Hop Time is 1.2ms. If the packet received by the nodes beyond the Hop Time then that node get failed. In this Forward (Message) is checked if it is not true then that node get failed.

## 5. Proposed Algorithm for blocking the malicious node in network (I0, K0)

```
/*I0 is the node that is detected as the malicious node. The misbehavior is either in case of broken link, or  
in terms of some attack on it.*/
```

```
{  
As the Failure Node Detected by Node K0 it will request to block this node.  
It set the Reply status of Node I0 at No. it seems all neighboring nodes not to use this node as part of  
network  
}
```

In this network nodes misbehave when nodes does not send the packets within Hop Time then node is misbehaving. If node is misbehaving then it means that it has the packet delivery ratio less than 98 %. The nodes which are misbehaving in the network are blocked temporarily. Its neighboring node informs the nodes about blocked node and the Route table is updated. The table is updated in such a way all nodes in the path are informed about the failed node.

### Performance Measuring Parameters

The performance is measured on the basis of some parameters which are described as follows:

**Average end-to-end delay-** Average end-to-end delay specify how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, propagation delay and transfer time [8]. This parameter is useful in understanding the delay caused while discovering path from source to destination.

**Throughput-** Throughput is the ratio of number of packets sent and total number of packets. It describes the average rate of successful message delivery over a communication channel [9], [10]. Throughput measures the efficiency of the system.

**Packet Loss Ratio-** Packet loss ratio defines the number of packets that are dropped or lost due to congestion in the network.

**Packet Delivery Ratio-** Packet delivery ratio is defined as the number of packets actually delivered to the destination to the number of data packets supposed to be received [8]. The better the packet delivery ratio, the more complete and correct is the routing protocol.

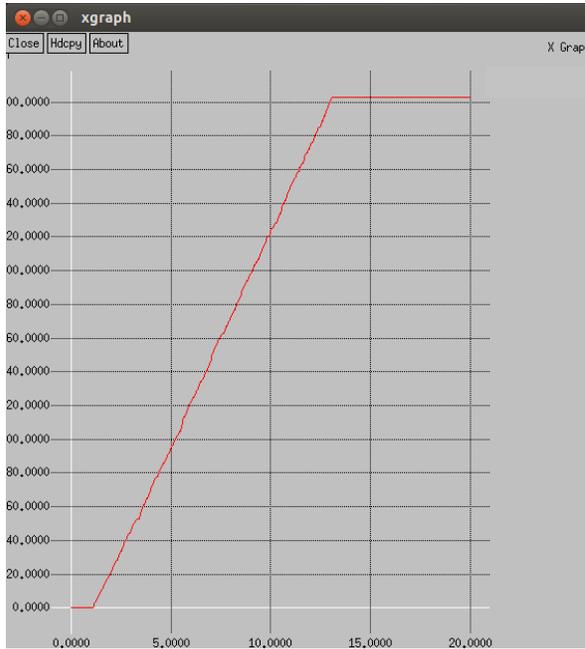
## 6. Results and Analysis

These algorithms are implemented in NS2 Simulator. X-graph gives the results. X-graph gives the graphs for basic AODV and enhanced AODV. When comparison between these graphs done then packet received of Enhance AODV is increases than the basic AODV and packet lost is reduced than basic AODV. In this results are shown for 25, 50 nodes.

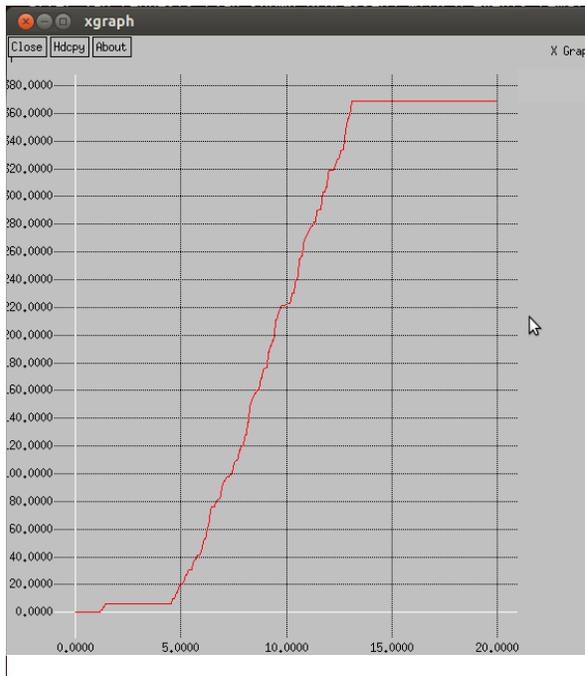
The result is as follows:

### 1 .Graph for 25 nodes

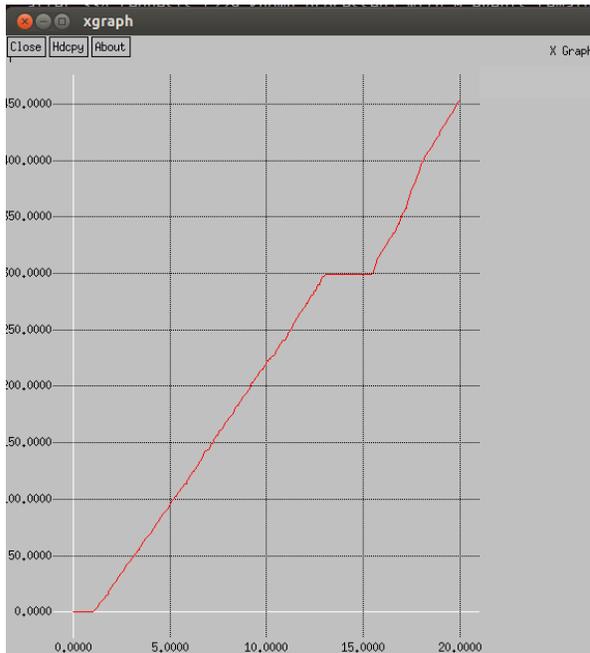
Graph for the packet received of the 25 nodes of the basic AODV



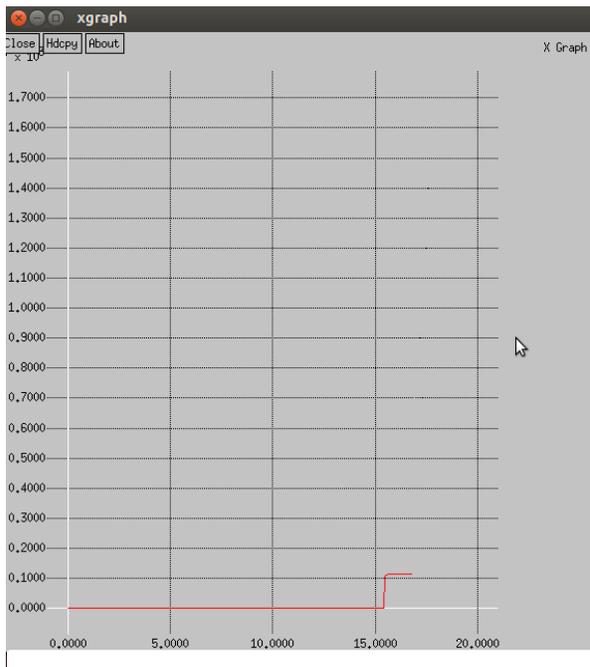
Graph for the packet lost of the 25 nodes of the basic AODV



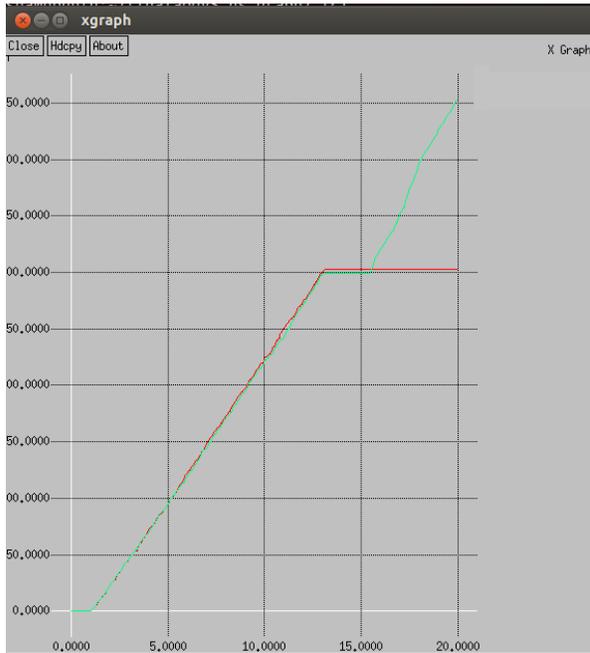
Graph for the packet received of the 25 nodes of the enhanced AODV



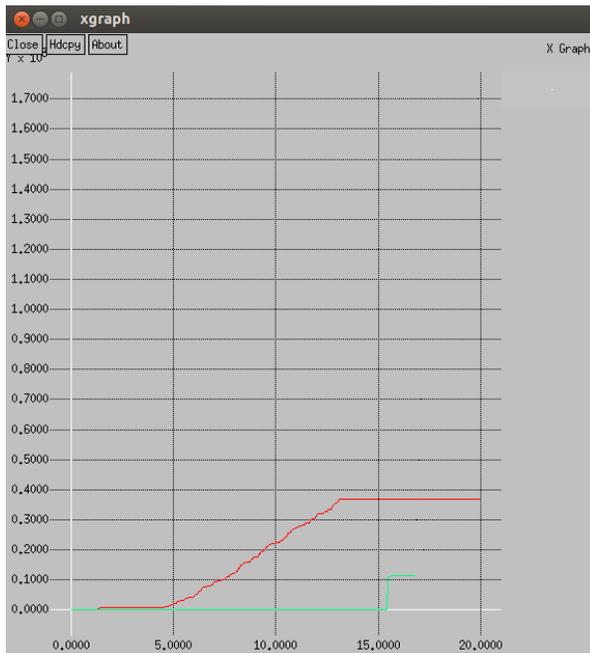
Graph for the packet lost of the 25 nodes of the enhanced AODV



Graph of the Comparison of packet received of the 25 nodes of the basic AODV and enhance AODV

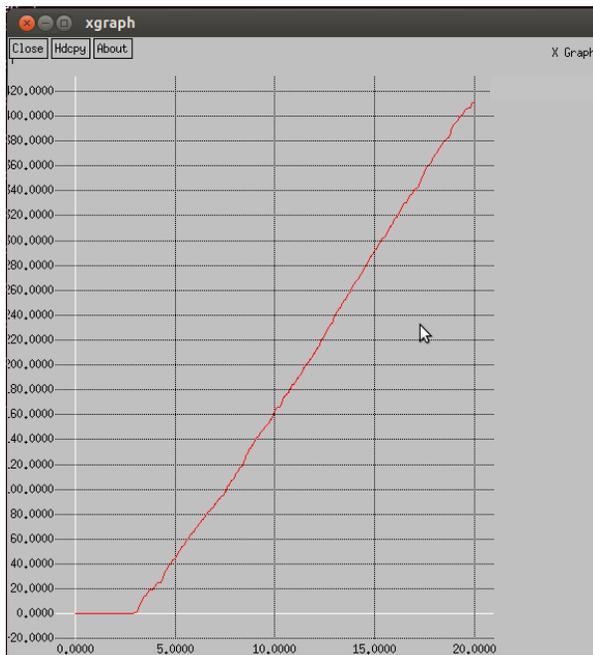


Graph of the Comparison of packet lost of the 25 nodes of the basic AODV and enhance AODV

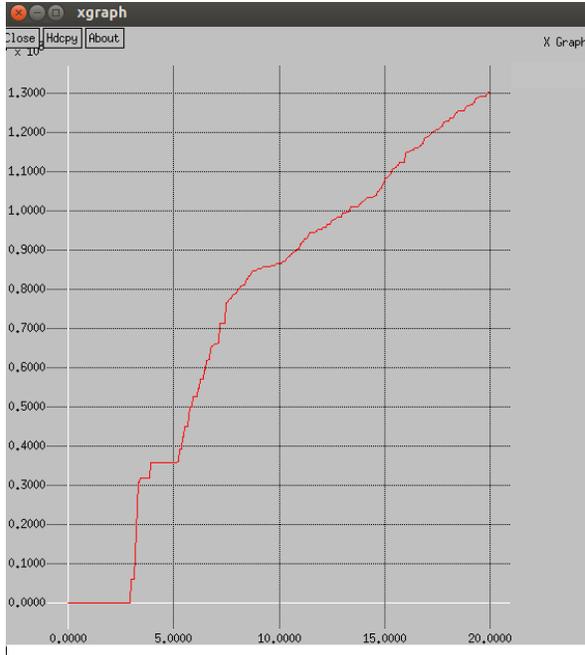


### Graph for 50 nodes

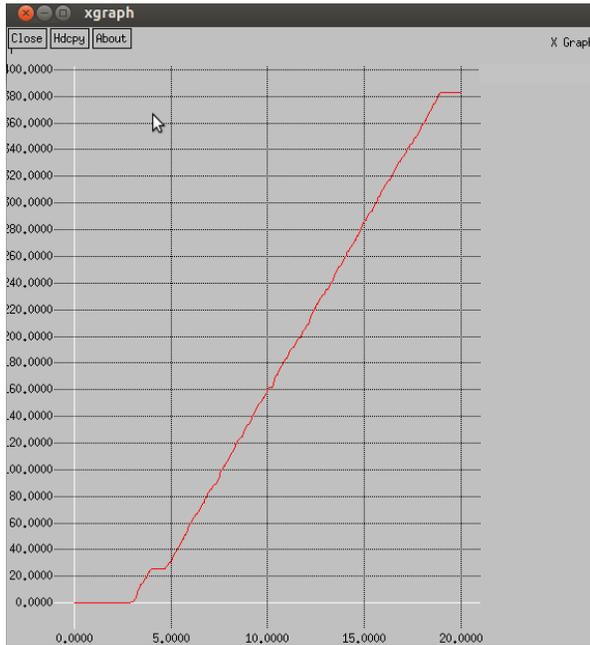
Graph for the packet received of the 50 nodes of the basic AODV



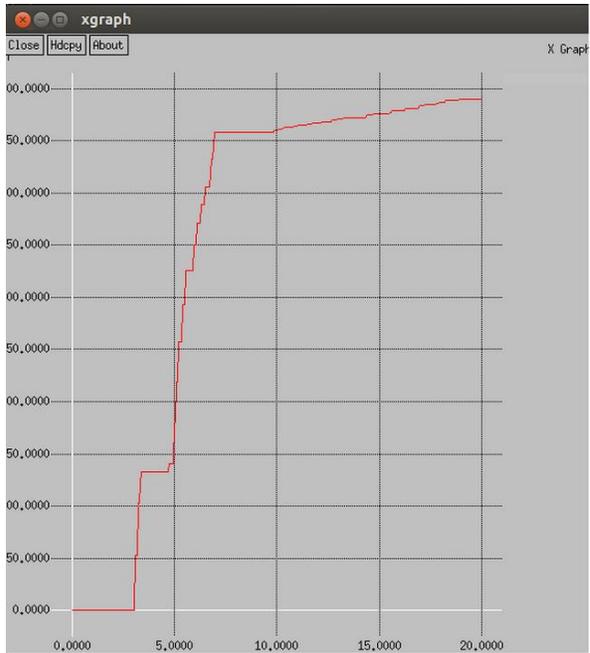
Graph for the packet lost of the 50 nodes of the basic AODV



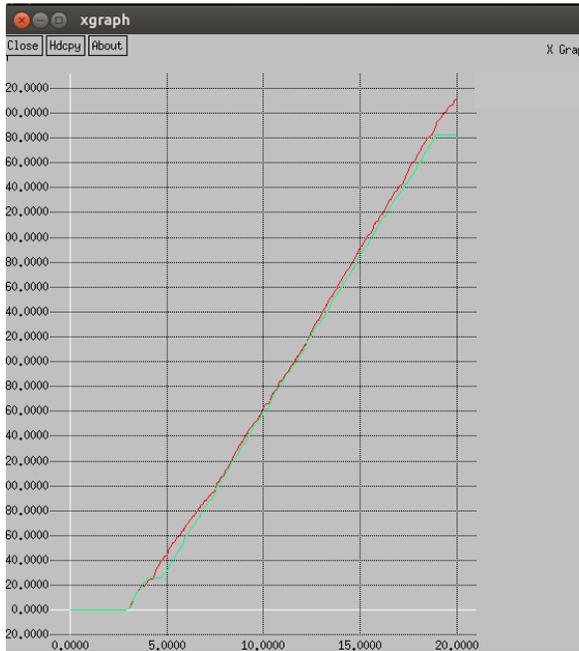
Graph for the packet received of the 50 nodes of the enhanced AODV



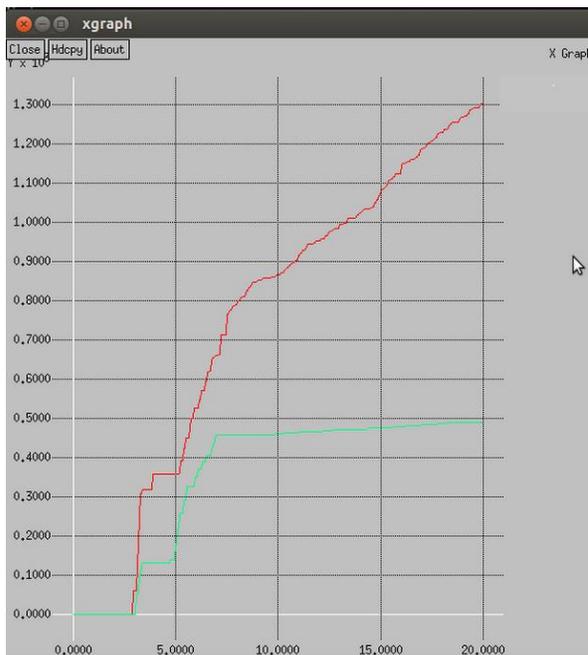
Graph for the packet lost of the 50 nodes of the enhanced AODV



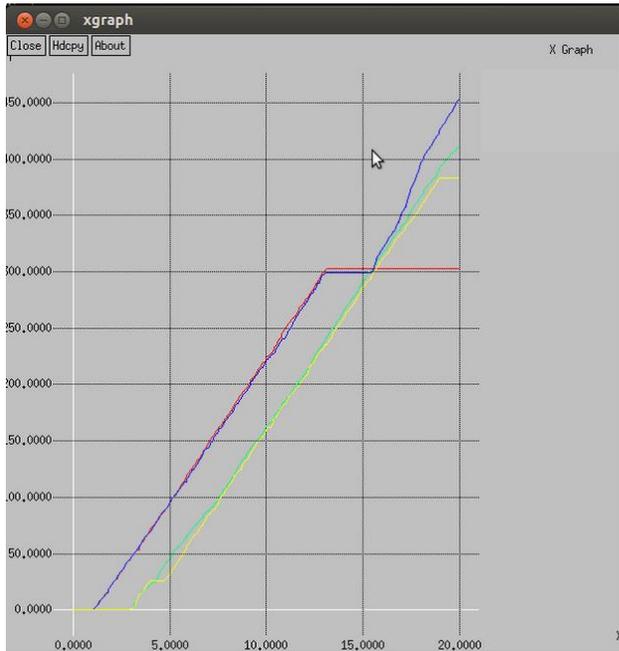
Graph of the Comparison of packet received of the 50 nodes of the basic AODV and enhance AODV



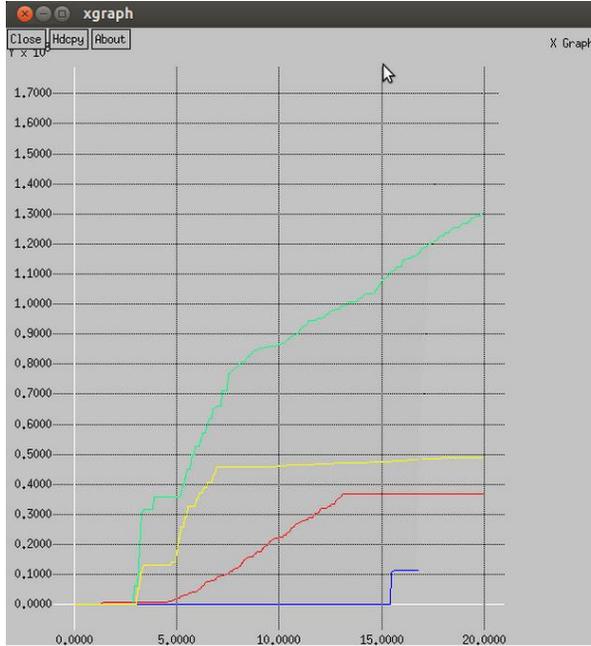
Graph of the Comparison of packet lost of the 50 nodes of the basic AODV and enhance AODV



Graph of the packet received of the 25,50 nodes of the basic AODV and enhance AODV



Graph of the packet lost of the 25,50 nodes of the basic AODV and enhance AODV



## Conclusion and Future Work

In this paper, an effort has been made to concentrate on the study and analysis of on demand (reactive) routing protocol AODV. We have presented a simulation study which shows that Enhanced AODV works better than the basic AODV when malicious node found. we have shown the performance of AODV protocol for the parameter, packet delivery ratio and packet loss ratio. As we increase the number of nodes for performing the simulation of AODV routing protocol, number of sent, routing and delivered packets changes hence the performance parameters changes. The algorithm improves packet delivery ratio and reduces packet loss ratio. The improvement demonstrates the benefits of the algorithm. Although the results were obtained under a certain type of mobility and traffic models, we believe that the results apply to other models, as the algorithm quickly removes stale routes no matter how nodes move and which traffic model is used. As with other applications, there is certainly a scope for improvement in this application too. There exist a lot of properties which can helpful in optimization of performance evaluation of routing protocols. The performance of AODV can be further enhanced using fuzzy logic by taking different input parameters to reduce the uncertainty for finding an optimal path. This will drastically reduce the packet loss and average end to end delay and thereby making an efficient AODV routing protocol.

## REFERENCES

- [1] E. M. Royer and C. K. Toh, "A Review of Current Routing Protocols Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, April 1999, Volume 6, Number 2, pp: 46-55.
- [2] S.A.Ade and P.A.Tijare, "Performance Comparison of AODV, DSDV, OLSR, DSR Routing Protocols in Mobile Ad Hoc Networks ", International Journal of Information Technology and Knowledge Management, July- December 2010, Volume 2, Number 2, pp: 545-548
- [3] Ravinder Ahuja, "Simulation Based Performance Evaluation and Comparison of Reactive, Proactive and Hybrid Routing Protocols Based on Random Waypoint Mobility Model", International Journal of Computer Applications, October 2010, Volume 7, Number 11, pp: 20-24
- [4] Robinpreet Kaur & Mritunjay Kumar Rai "A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012
- [5]Sunil Taneja and Ashwani Kush "A survey of Routing Protocols in Mobile Ad Hoc Networks", International Journal of Innovation, Management and Technology, Vol. 1, No. 3, August 2010 ISSN: 2010-0248
- [6] Elizabeth M. Royer, "A Review of current routing protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communication \* April 1999
- [7] Dr.D.Siva Kumar "Review: Swarm Intelligent based routing Protocols for Mobile Adhoc Networks" International Journal of Engineering Science and Technology Vol.
- [8] S.P. Setti, K. N. Raju and K. N. Kumar, "Performance Evaluation of AODV in Different Environments", International Journal of Engineering Science and Technology, 2010, Volume 2, Number 7, pp: 2976-2981.
- [9] A.K.Sharma and N Bhatia, "Behavioral Study of MANET Routing Protocols by using NS-2", International Journal of Computational Engineering and Management, April 2011, Volume 12.
- [10] Jie Gao, "Analysis of Aloha and Slotted Aloha", Available at: [www.cs.sunysb.edu](http://www.cs.sunysb.edu), (Accessed on: 25 June 2012).