Research Journal of Applied Sciences, Engineering and Technology 8(14): 1648-1655, 2014
DOI:10.19026/rjaset.8.1146
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: May 31, 2014 Accepted: July 01, 2014 Published: October 10, 2014

Research Article

Advanced AODV Protocol for Identify Victim Nodes Using Divide and Conquer Strategy-in MANET

[1]S. Hemalatha and [2]Paul Rodrigues
[1]Anna University,
[2]DMI College of Engineering, Chennai, Tamil Nadu, India

Abstract: Objective of this study is there are many protocols have been proposed in Ad-hoc network, but none of the protocol is working under the principle of handling and checking on packet delivery. We have developed a routing protocol called the Advanced Ad-hoc on demand Vector protocol. The working principle of this protocol is checking the packet delivery to the destination. If any one of the nodes in the route is not forwarding the packet, that corresponding node will be identified and redirect the packet to the new route. For doing this checking this protocol uses divide and conquer strategy. The number hop between the source to destination is divided into two halves and check whether the up to the middle node the packet are flowing in a proper order or not. Recursively doing the divide and conquer of the route path, can identify the node which is not forward the packet to the next node. The design of this protocol contains several stages from path discovery, packet transmits, apply divide and conquer strategy on route, identify the victim node which is not forward the packet, redirect the new path, alert all the nodes about the victim node. Finally performance graph has been given compared with AODV protocol.

Keywords: AAODV protocol, AD-HOC network, AODV protocol, divide and conquer

INTRODUCTION

A Collection of nodes formed a network under the working principles of move freely, organized themselves arbitrarily and without any administration is called Mobile Ad-hoc network (Wikipedia, 2004). In a common, a route between the sources to destination through the Ad-hoc network is established by the routing protocol. The packets have followed this route to transfer the data. Packets are moved from a node to another node called the hop, until to reach the destination. A Routing protocol an Ad-hoc network is classified into two types is uniform protocol and non Uniform protocols. In uniform protocol each node sends and responds a routing control message. In non uniform type protocol reduces the number of nodes participating in routing computation (Murthy and Garcia-Luna-Aceves, 1996).

Routing protocols describe the state information into two ways like topology based protocol and destination based protocol (Kuosmanen, 2002; Stojmenovic and Wu, 2003; Murthy and Garcia-Luna-Aceves, 1996). The routing in topology based protocol each node makes a decision based on the topology information. This type based on link state protocol (Chiang *et al*., 1997; Jacquet *et al*., 1998). Routing in destination based protocol is maintaining a distance to a destination. A Routing protocol in an Ad-hoc network is divided into two main categories of proactive and reactive protocol. In proactive protocol nodes maintain routing information for all other nodes in the network is stored in a table is called a routing table. So this protocol is also named as a table driven protocol.

In the second type of protocol, route information is established when a packet transfers between the nodes. In the table driven protocol are Destination Sequence Distance Vector (DSDV) protocol (Perkins and Bhagwat, 1994), every node maintain a routing table of all other nodes is based on the shortest path from source to destination. When any topological changes occur in the network, the route table also changes. The maximum number of changes in maintain by a counter which is increment by one when any router table changed.

Wireless Routing Protocol (WRP) is a proactive protocol which maintains a four kind of table hold a detail like distance, link cost and route and message transmission information (Perkins and Bhagwat, 1994). Clustered Gateway Switch Protocol is an extension of Destination Sequence Distance Vector routing protocol which includes clustering to increase the protocol scalability (Murthy and Garcia-Luna-Aceves, 1996). This protocol performance is improved by including methods like priority token scheduling, gateway code scheduling and path recursion.

Optimization link state routing protocol (Chiang *et al*., 1997) optimized the multipoint relay. Each node

Corresponding Author: S. Hemalatha, Anna University, Chennai, Tamil Nadu, India

identifies its multipoint relay, by flooding message to MRP will be received by the destination. Topology dissemination Based on Reverse Path Forwarding (TBRPF) (Bellur *et al*., 2001) is a link state routing with overhead reduction technology (Jacquet *et al*., 1998). Each node computes its shortest path tree to all other nodes, but to optimize bandwidth Fish Eye State routing Protocol (Bellur *et al*., 2001) is under the technique of Fish Eye state information about other nodes is based on how far away the defined nodes are.

In source initiated routing protocols Dynamic Source Routing Protocol (Johnson and Maltz, 1996) each node maintains a route cache contain a route learned by the node. AODV (Perkins and Royer, 1999; Abd Rahman and Zukarnain, 2009; Perkins and Royer, 2000; Perkins and Royer, 1998; Giannoulis *et al*., 2007; Perkins *et al*., 2003) node create a route on demand to maintain a complete a route using DSDV algorithm.

TORA (Park and Corson, 1998) is another source initiated on Demand protocol, in a concept of link reversal of direct Acyclic Graph. TORA has the capacity of routing repair. ABR (Park and Corson, 1997) routing protocol is on demand protocol route selection is based o n the signal strength in the link.

Even though, there are many protocols have been proposed in Ad-hoc network, but none of the protocol is working under the principle of handling and checking on packet delivery. We have developed a routing protocol called the Advanced Ad-hoc on demand Vector protocol. The working principle of this protocol is checking the packet delivery to the destination. If any one of the nodes in the route is not forwarding the packet, that corresponding node will be identified and redirect the packet to the new route. For doing this checking this protocol uses divide and conquer strategy.

The design stages of this protocol is the number hop between the source to destination is divided into two halves and check whether the up to the middle node the packet are flowing in a proper order or not. Recursively doing the divide and conquer of the route path, can identify the node which is not forward the packet to the next node. The design of this protocol contains several stages from path discovery, packet transmits, apply divide and conquer strategy on route, identify the victim node which is not forward the packet, redirect the new path, alert all the nodes about the victim node. Finally performance graph has been given compared with Advanced on Demand Routing protocol with the performance factors of through put, packet delivery ration and end to end delay.

MATERIALS AND METHODS

Advanced AODV protocol design stages: This protocol implementation is divided into several stages are:

- Decide the path using AODV protocol
- Packet Transmit

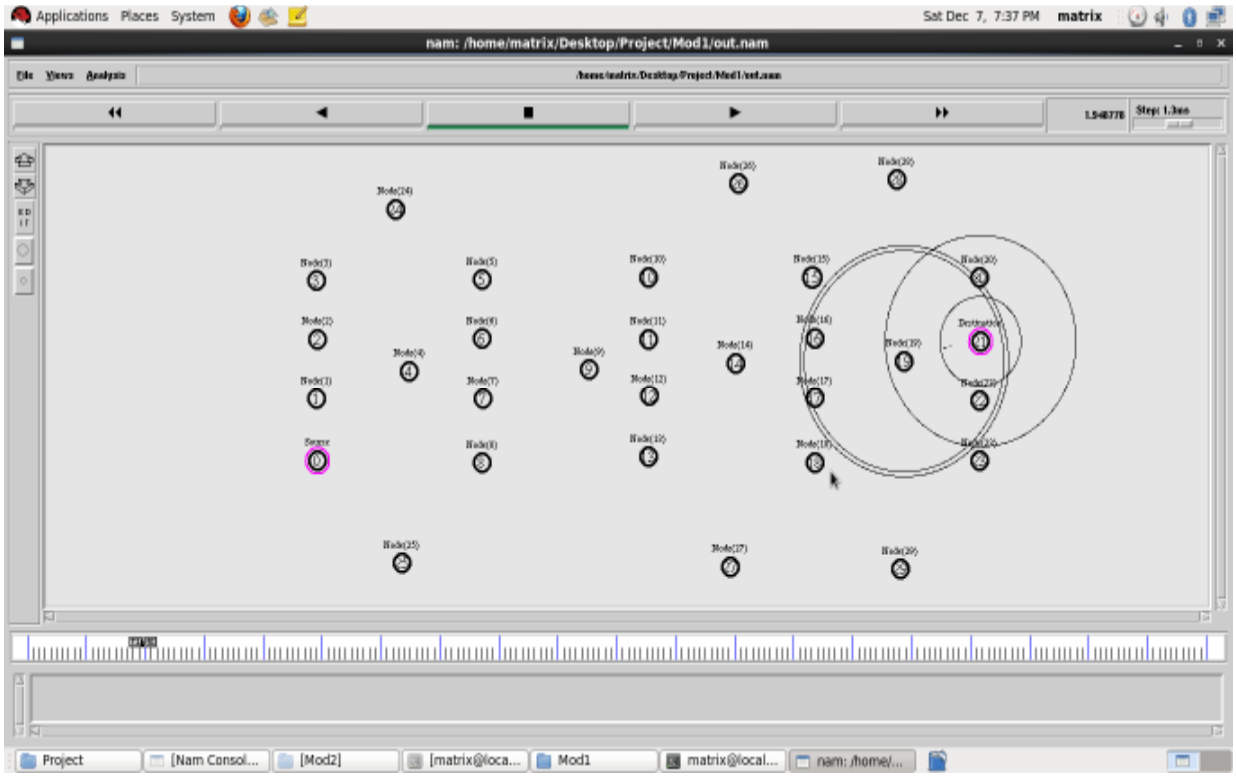

Fig. 1: Decide the path using AODV protocol

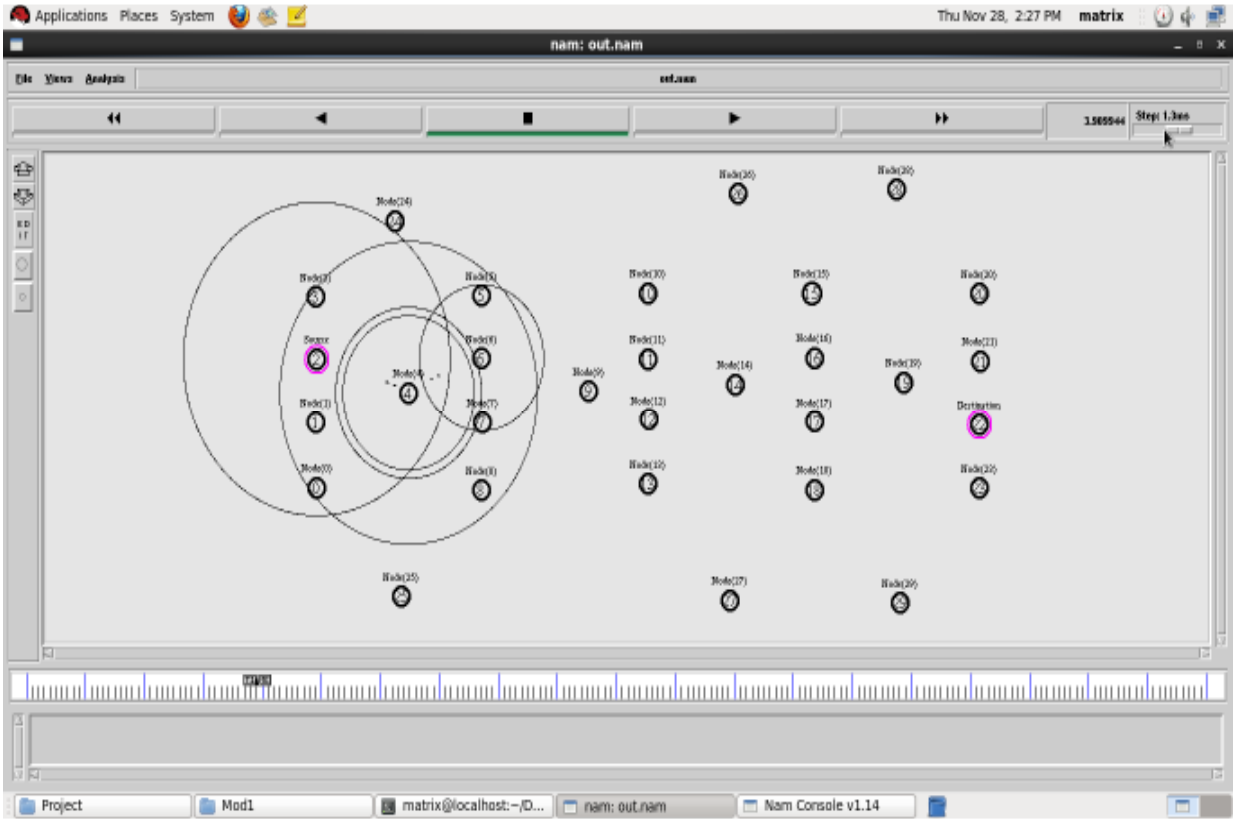

Fig. 2: Packet transmit

- Establish the Divide and Conquer Strategy
- Identify the victim node
- Redirect the new route
- Sending alarm message to all the node

Decide the path using AODV protocol: Route discovery of this protocol will be based on Ad-hoc On Demand Vector protocol principle. Steps involved in Route Discovery:

- Node S (Source) needs a route to D (Destination)
- Creates a Route Request (RREQ): Enters D's IP addr, seq#, S's IP addr, seq#, hop count (= 0)
- Node S broadcasts aRREQ to neighbours
- Node A receives RREQ: Makes a reverse route entry for S dest = S, next hop = S, Hop count = 1 It has no routes to D, so it rebroadcasts RREQ
- Node C (intermediate node say C) receives RREQ: Makes a reverse route entry for S dest = S, nexthop = A, hopcount = 2 It has a route to D and the seq# for a route to D is > = D's seq# in RREQ

This module is processed with discover the route by using the AODV protocol as in Fig. 1 implemented in NS2. It can be done based on the route request and unicasting reply.

Packet transmits: Once the route between source to destination was identified, the packet is transferred from source to destination. This module is processed with packet transmission the packet can be transmitted via the route which is discovered by the AODV protocol as in Fig. 1. If the packet is reached properly to the destination, then the route is perfect and the route does not have any victim. If and packet loss or any delay occurred means it considers that the route have victimized. Identification purposes we are transmitting packet (Fig. 2).

Establish the divide and conquer strategy: Customized protocol forwards the packet from source to identified destination. Then calculate the number of nodes and do the operation for giving divide and conquer strategy. In this strategy, the network can calculate the number of nodes and then it calculates the middle node, which the middle node will act as the temporary destination. Then the packet can be transmitted from the source to the temporary destination. If the temporary destination receives the packet then that node is not a victim. Then it will again calculate the number of remaining nodes. And find the middle node. That old middle node is acting as a temporary source and a new middle node will act as the temporary destination and do the process again. Else

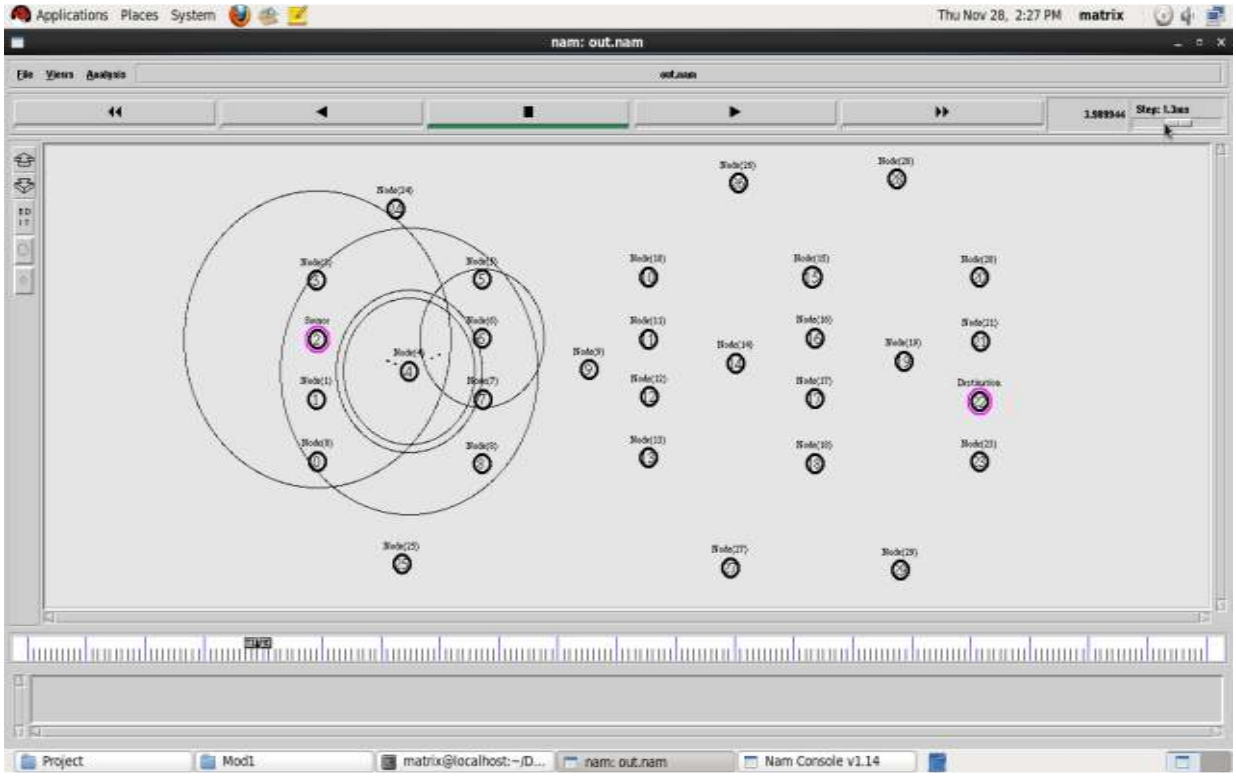

Fig. 3: Route discovery and number of node calculation

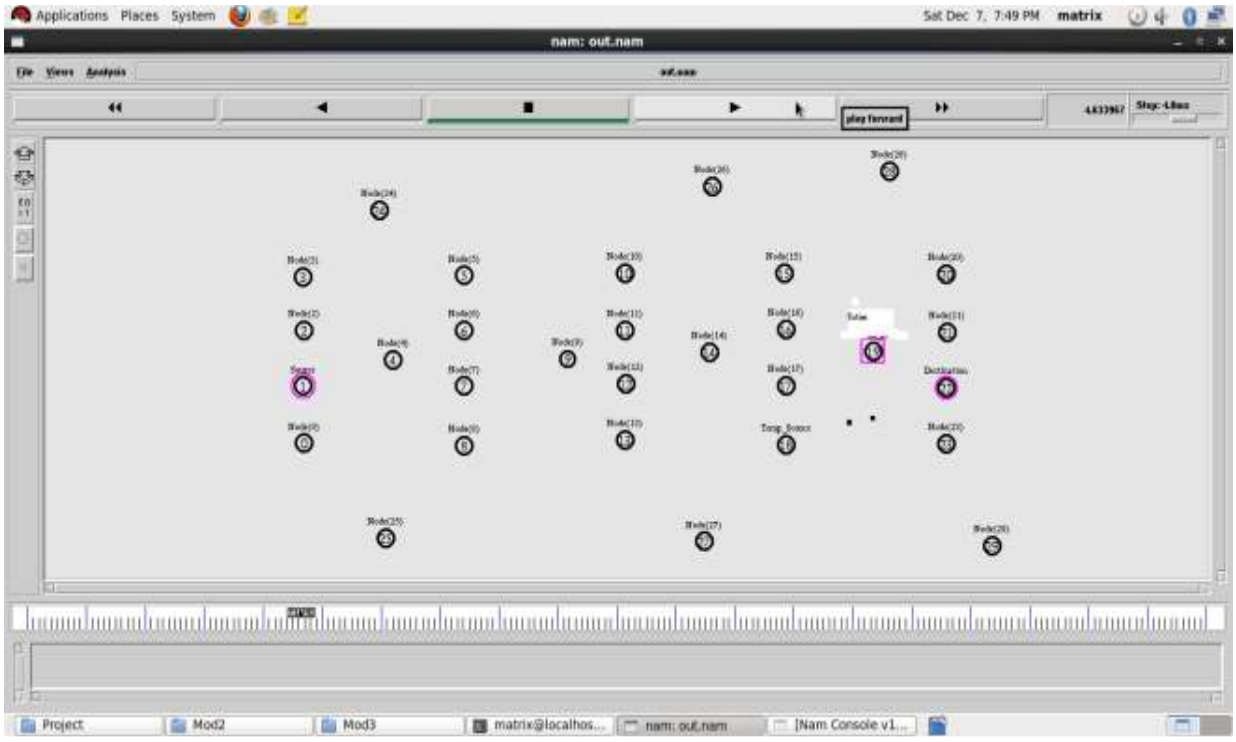

Fig. 4: Victim node identification

calculate the source node to middle node hop count and again do the new middle node and that will act as the temporary destination:

Divide and conquer strategy algorithm: Procedure (Source, Dest, G)-Divide and Conquer strategy:
Consider the ordered Set G = {1……..N}

Step 1: Initialize source = 1, dest = N
Step 2: Calculate middle = No of hops (source to dest)/2
Step 3: (i) Check the packet is passed the middle node if yes the calculate the new middle form old middle (source = old middle) to dest, go to step 2

(ii) Otherwise calculate the new middle for source to middle (Dest = middle)

(iii) Repeat the process

// assume there is no flow of data then suspect the node may be the intruder.

Process whether the middle node is intruder

If True Set victim = Middle and initiate route discovery process.

Step 4: Process to conform victim node
Step 5: Process the flow of data in middle node
Step 6: If the flow is delayed, set Dest = prev (middle) and go to step 2
Step 7: If the flow is normal set source = next (middle) and go to step 2
Step 8: Stop

This module is processed with the strategy of divide and conquers; the packet can be transmitted via the route which is discovered by the AODV protocol as in Fig. 1. It can be calculate the number of nodes in the route as in Fig. 3. It can send the packet to the destination. If the packet is not reached to the destination, then the route is divided and middle node will act as the temporary destination as in Fig. 3. After a transmit ion that temporary destination receives the packet, then that node act as the temporary source as in Fig. 4.

Identify the victim node: Using AAODV Routing protocol divide and conquer strategy can be done. Based on this strategy it can identify the victim node which does not forward the packet to the next node.

Send alert message: This module is focused for sending alters the message to entire node after the victim node identified using divide and conquer strategy.

Route re-direction: This module is focused in the route redirection, after send an alert message it will redirect the route from source to the destination. This will be reflected in the Fig. 5 and 6.

RESULTS AND DISCUSSION

Compare AAODV with AODV: In the previous chapter discuss the implementation of AAODV protocol. This protocol implementation was based on the AODV protocol design principles. We made a performance comparison with AODV protocol. Three performance measures we have taken are throughput, packet delivery ratio, End to End delay.

Through put between AODV and AAODV: Throughput refers to how much data can be transferred from one location to another in a given amount of time (Fig. 7).

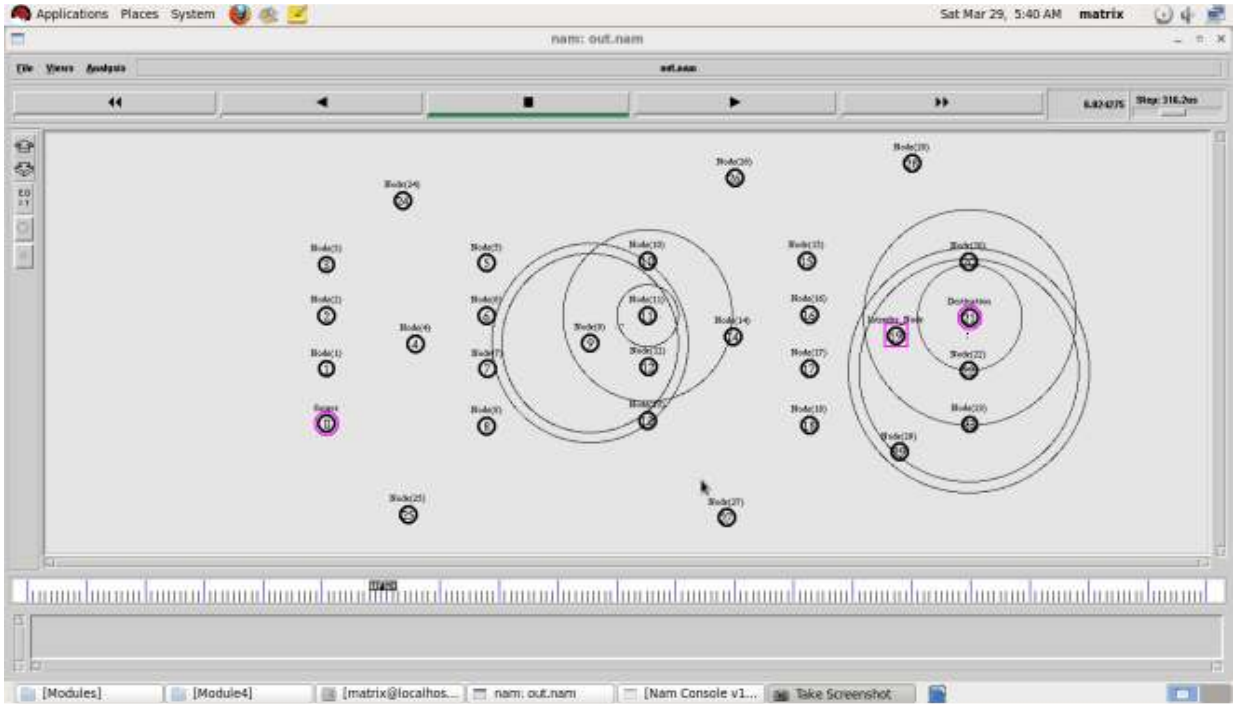

Fig. 5: Route re-direction initiation

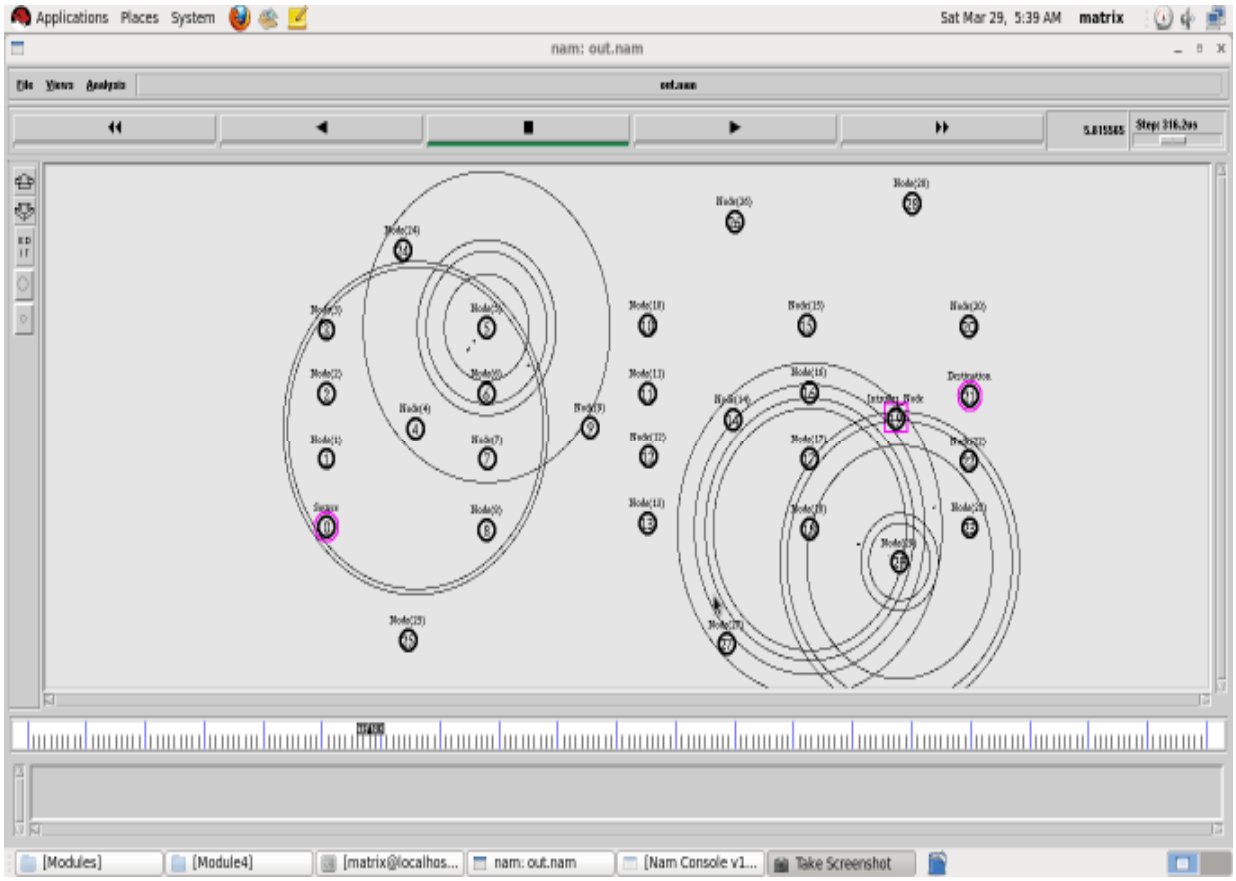

Fig. 6: Through redirection packet reached at destination

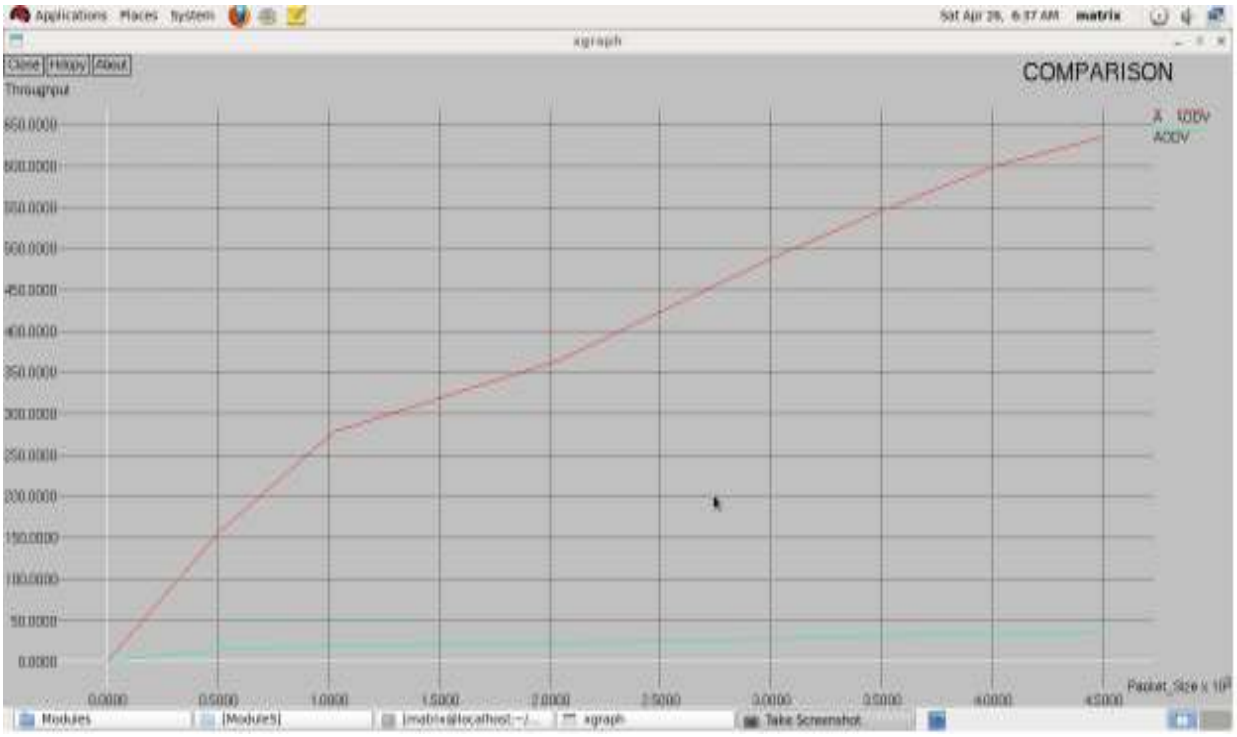

Fig. 7: Graph for throughput evolution

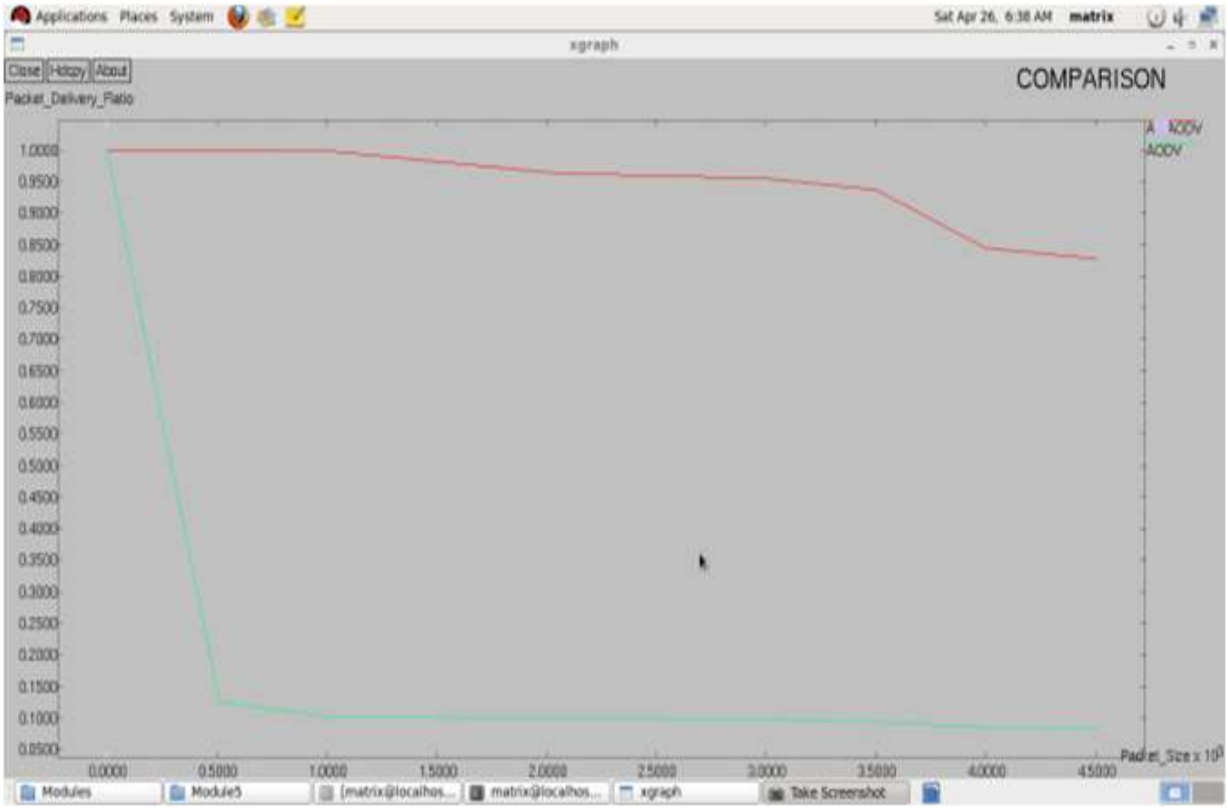

Fig. 8: Graph for packet delivery ratio

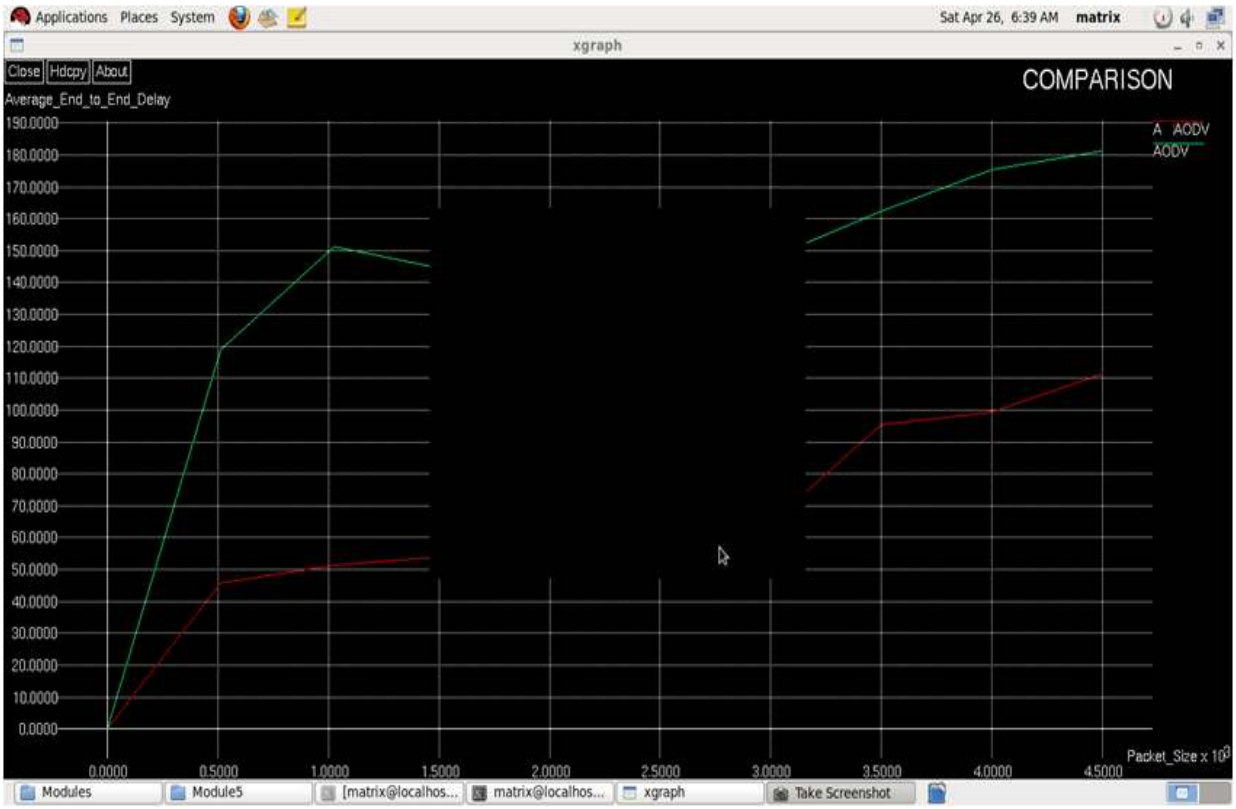

Fig. 9: Graph for end to end delay

Packet delivery ratio: The ratio of the number of delivered data packets to the destination. This illustrates the level of delivered data to the destination (Fig. 8):

$$\sum \text{Number of packets receive} / \sum \text{Number of packets send}$$

End-end delay: The average time is 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 (Fig. 9):

$$\sum (\text{arrive time-send time}) / \sum \text{Number of connections}$$

CONCLUSION

This study presents the implementation of Advanced AODV protocols using the divide and conquers strategy and also given a performance comparison with AODV protocol. Comparing AAODV with ADOV protocol, in all the cases AAODV protocol provides the best result. In future this protocol can also be used for identifying a malicious users present in the network. This malicious user may be intruder present in the network who plays a role of participating in a routing discovery, but not cooperate to forward a packet to the next hop.

REFERENCES

Abd Rahman, A.H. and Z.A. Zukarnain, 2009. Performance comparison of AODV, DSDV and I-DSDV routing protocols in mobile ad hoc networks. Eur. J. Sci. Res., 31(4): 556-576.

Bellur, B, R.G. Ogier and F.L. Templin, 2001. Topology Broadcast Based on Reverse-Path Forwarding (TBRPF). IETF Internet Draft, draftietf-manet-tbrpf-01.txt. Retrieved form: http://www.ietf.org/ internet-draft/draft-ietf-manet-tbrpf-01.txt (Accessed on: 2 March, 2001).

Chiang, C.C., H.K. Wu, W. Liu and M. Gerla, 1997. Routing in clustered multi-hop mobile wireless networks with fading channel. Proceeding of IEEE SICON-97, pp: 197-211.

Giannoulis, S., C. Antonopoulos, E. Topalis and S. Koubias, 2007. ZRP versus DSR and TORA: A comprehensive survey on ZRP performance. IEEE T. Ind. Inform., 3(1): 63-72.

Jacquet, P., P. Muhlethaler, A. Qayyum, A. Laouiti and L. Viennot, 1998. Optimized Link State Routing Protocol. Internet Draft, draft-ietf-manetolsr- 00.txt. Work in Progress, June 2001.

Johnson, D.B. and D.A. Maltz, 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. In: Imielinski, T. and H. Korth, (Eds.), Mobile Computing. Kluwer Academic Publishers, Dordrecht, The Netherlands, pp: 153-181.

Kuosmanen, P., 2002. Classification of ad hoc routing protocols. Finnish Defence Forces, Naval Academy, Finland. Retrieved form: <http:// keskus.hut.fi/opetus/ s38030/k02/ Papers/12-Petteri.pdf.

Murthy, S. and J.J. Garcia-Luna-Aceves, 1996. An efficient routing protocol for wireless networks. Mobile Netw. Appl., 1(2): 183-197.

Park, V.D. and M.S. Corson, 1997. A highly adaptive distributed routing algorithm for mobile wireless network. Proceedings of 16th Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution INFOCOM-97, 3: 1405-1413.

Park, V. and S. Corson, 1998. Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification. IETF Internet Draft. Retrieved form: http://www.ietf.org/internet-drafts/draft-ietf- manet –tora–spec-01.txt1998.

Perkins, C.E. and P. Bhagwat, 1994. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. ACM Comput. Commun. Rev., 24(4): 234-244.

Perkins, C.E. and E.M. Royer, 1998. Ad Hoc on demand distance vector (AODV) routing. Internet-Draft, Aug-1998.

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on demand distance vector routing. Proceeding of 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp: 90-100.

Perkins, C.E. and E.M. Royer, 2000. Ad Hoc On-demand Distance Vector (AODV) Routing. Internet Draft, MANET Working Group, draft-ietf-manetaodv-05.txt, March 2000.

Perkins, C.E., E.M. Royer and S. Das, 2003. Ad hoc On-demand Distance Vector (AODV) Routing. Internet Draft, RFC 3561. IETF Network Working Group, July 2003.

Stojmenovic, I. and J. Wu, 2003. Broadcasting and Activity-scheduling in Ad Hoc Networks. In: Basagni, S.M. Conti, S. Giordano and I. Stojmenovic, (Eds.), Ad Hoc Networking. IEEE Press, Wiley, New York.

Wikipedia, 2004. The Free Encyclopedia. Retrieved form: http://en.wikipedia.org/wiki/Mobile_ad-hoc_network (Accessed on: Oct. 2004).