# Performance Analysis and Effect of Mobility on Ad-Hoc Distance Vector Protocol in MANET

Purvi N. Ramanuj
Department of Computer Engineering
L.D. College of Engineering
Ahmedabad

Hiteishi M. Diwanji
Department of Computer Engineering
L.D. College of Engineering
Ahmedabad

## ABSTRACT
A wireless Ad Hoc network is a collection of mobile nodes that form a dynamic, autonomous network. Nodes communicate with each other without depending on any infrastructure. Hence, in these networks each node acts as a host and as a router. Reactive Protocol Ad hoc Distance Vector Protocol is one of the widely used protocols in MANET. This paper aims at study of Ad hoc On demand Distance Vector (AODV). We have done in depth Performance analysis of AODV using the OPNET simulator. Effects of node mobility are analyzed on different parameters like routing traffic overhead, throughput and route errors in AODV.

## General Terms
AODV, MANET, OPNET, TCP

## Keywords
Effects of Mobility, performance analysis of AODV.

## 1. INTRODUCTION
A wireless Ad Hoc network is a collection of mobile nodes that form a dynamic, autonomous network. Nodes communicate with each other without depending on any infrastructure (e.g. access points or base stations) [3]. Hence, in these networks each node acts as a host and as a router.

## 2. AD HOC ROUTING
Network topology in Ad Hoc networks, changes frequently and unpredictably. Such a highly dynamic nature of network, makes routing difficult and complex between mobile nodes. As routing is very important in communication between mobile nodes, study of routing protocols has become area of interest for many. Based on Routing information update mechanism, routing protocols in wireless ad-hoc networks are divided into three groups of proactive (Table-Driven), reactive (On-Demand), and hybrid routing protocols. [3]

In proactive routing protocols, each node periodically distributes routing tables throughout the network. The main disadvantages of such protocols are the large amount of routing overhead generated for maintenance and at the time of link failure, reestablishing the network is slower. The main advantage of these protocols is that a source node can get a routing path immediately if it needs one [6] [3]. DSDV (Destination-Sequenced Distance-Vector Routing) and OLSR (Optimized Link State Routing Protocol) are proactive routing protocols. In reactive routing protocols, the nodes obtain the necessary path only when it is required using connection establishment process. The main advantage of such protocol is less routing traffic being generated in network and faster route discovery which is very essential in Ad hoc networks. The disadvantage is that the node has to initiate route discovery process before sending the data if it does not have prior information about the same. AODV, DSR (Dynamic Source Routing, TORA (Temporally-Ordered Routing Algorithm) are reactive routing protocols.

In hybrid routing protocols, the merits of both proactive and reactive routing protocols are combined. The initial establishment of the routes is done with some proactively prospected routes and then additionally activated nodes are served on-demand through reactive flooding. The disadvantage of such protocols is dependence of the advantage on amount of nodes activated [6]. ZRP (Zone Routing Protocol) is a hybrid routing protocol.

## 3. AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL
Ad-Hoc On-Demand Distance Vector (AODV) routing protocol is one of the most efficient reactive routing protocol. AODV routing algorithm is suitable for dynamic self-starting network as needed by users who want to use ad hoc networks. Whenever a source is required to send data to destination, then only it initiates request for route discovery. Thus it uses an on demand approach for finding routes. AODV uses a novel concept of sequence number for each node which results into loop free route discovery. In AODV single route request may receive multiple route reply but the use of sequence number helps to find out the latest information about the route which is very important in dynamic and rapidly changing network topology. Route discovery is mainly accomplished with flooding of RREQ packet by source in the network. Expanding ring search Algorithm is used to limit the initial flooding control traffic. Route maintenance is carried out by intermediate node by using Hello messages. Whenever a link breakage is detected, local repair is carried out by intermediate node by finding alternate route. Routing table is maintained distributed that is all the intermediate nodes contain routing information for a particular route in their routing table.

Route discovery is accomplished in AODV by defining control packet, RREQ (Route Request), RREP (Route Reply), and RERR (Route Error). These message types are received via UDP, and normal IP header processing is applied.

Whenever a source node wants to send data to destination and does not have valid route to destination in its routing table, it

initiates route discovery by sending RREQ. Each RREQ contains destination sequence number – last known sequence number for the destination, destination IP address, source sequence number and source IP address. It also contains RREQ ID which identifies each RREQ uniquely originating from a source. RREQ ID is incremented each time a new RREQ message is sent. RREQ also contains hop count which shows the number of hops from source node to the node handling the request. The source node sends RREQ to its neighbor i.e. nodes directly reachable and in its radio range. Further this request is then forwarded by intermediate nodes to their neighbors, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is found. Destination sequence number is utilized by AODV to ensure loop free routes. So, if intermediate nodes have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ packet, they can reply to it. During the process of forwarding the RREQ, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received in their route tables. Thus, they establish a reverse path [5]. Each time Source waits for the reply for predefined time interval and if reply not received from destination or any other intermediate node, new request is sent with incremented RREQ ID. Such retries goes on with increased wait time for reply. This is basically done to limit initial flooding of routing traffic into the network. This technique is known as expanding ring search. Figure 1 shows the propagation of RREQ across the network. Here node N1 (source) sends RREQ to its neighboring nodes N2, N3 and N4. They further sends to N5, N6, N7 and finally to N8 (destination).

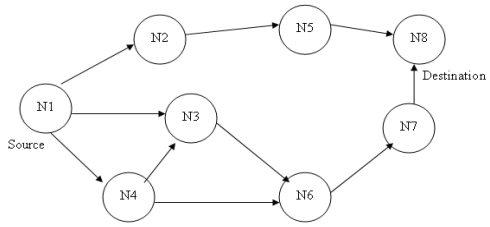


**Figure 1 Propagation of RREQ [5]**

RREP contains destination IP address, destination sequence number, source IP address and life time - the time for which nodes receiving the RREP consider the route to be valid. After the RREQ reaches the destination or an intermediate node with a fresh enough route, it responds by a route reply (RREP) packet that unicast to the neighbor which first received the RREQ packet and routes back along the reverse path [5]. Thus the routing information is stored in routing table which is distributed in all the intermediate nodes sending RREP. In this way the routing table is distributed among all the nodes in the route. The distance of source from destination is recorded in hope count field of RREP. Hello messages to neighboring nodes are used by nodes to maintain such established route. If no reply received within specified time due to the node in the network moved out

of coverage area, places and the topology is changed or the links in the active path are broken the node is declared as unreachable.

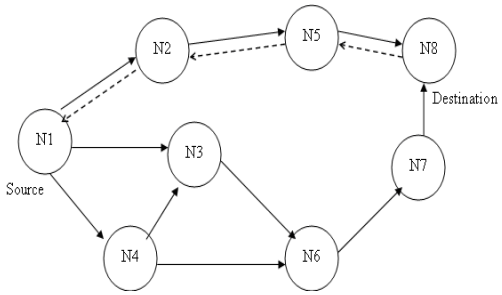


**Figure 2 Path of the RREP to the source**

The intermediate node that discovers this link breakage propagates an RERR packet that contains unreachable destination IP address and unreachable destination sequence number. Then, the source node re-initializes the path discovery if it still has data to send and desires the route [6].

## 4. SIMULATION AND RESULTS

We have used OPNET 14.0 simulator [1], for simulation purpose. A scenario for AODV is created. Mobile WLAN server is used to generate TCP traffic while operating as a FTP server and used as destination.

For simulation of AODV, office network of 2000 X 2000 meter is selected with four fixed node, one mobile node and one destination mobile server. Mobile_node_0 starts moving after 160 seconds and destination starts moving after 360 seconds. Application simulation runs for 10 minutes. Phase starts from 60 seconds. First route found through Source – Mobile_node_0 –

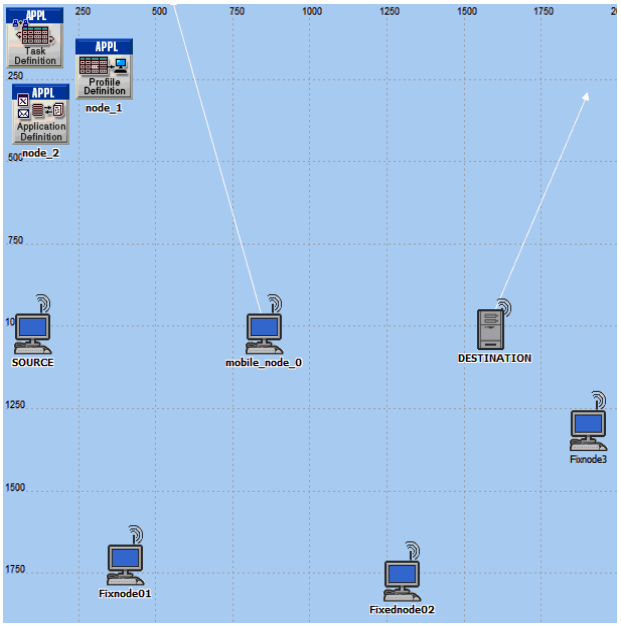


**Figure 3 Network topology**

Destination i.e. two hops. As mobile node starts moving after 160 seconds, new route established from Source – FixedNode01- FixedNode02 – Destination i.e. three hops. Destination starts moving after 6 minutes and another route is found from Source – FixedNode01- FixedNode02 – FixedNode03 – Destination i.e. 4 hops. As shown in Figure. 4.

The TCP traffic is generated by originating node sending one FTP request to destination i.e. FTP server. In reply to same, destination sends 1400 packets of data with each packet size of 50000 bytes continuously to originator.

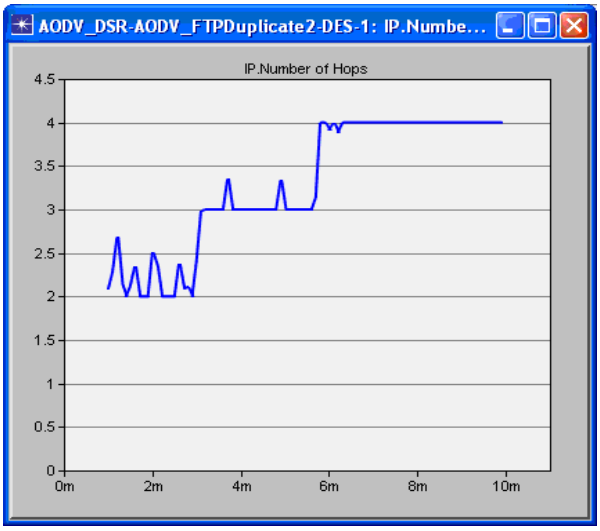


**Figure 4 Number of Hops**

## 4.1 AODV Routing Traffic

Source node initiates the route discovery process by sending the FTP request packet to the destination (i.e. WLAN server) for downloading the files by broadcasting the RREQ packet towards destination. As a response, destination is sending the corresponding RREPs. When the route is established between source and destination, destination also started sending the data continuously in response to the FTP request. While sending the data, there are more chances of link breakages due to the lost at the link layer and also delay in processing hello messages exchange between neighbors. Because of these link breakages, we can see more RREQs sent by the destination again to establish the link between the source and the destination. Source also sends corresponding RREPs. The destination has started more route discoveries during the data communication in order to make the link active again.

Once route is established routing traffic flows in a continuous way along data between wireless nodes of ad hoc network. Each hop in discovered route, adds some routing traffic to data. Traffic received is combination of all hops occurs in route from source to destination. Therefore routing traffic received is very high as compared to traffic sent.

## 4.2 IP Traffic sent by each node

IP traffic sent by destination and intermediate nodes is higher than IP traffic sent and received by source because more traffic is sent from destination to originating source. The pattern of IP traffic clearly indicates the node movement and hence involvement of other nodes to establish new route to destination. Initially from 60 to 160 seconds, route to the destination was completed in one hope i.e. through mobile node hence the maximum IP traffic is sent / received. During 160 – 360 seconds, two hopes are utilized which lowers the traffic sent / received. After 360 second when destination starts moving,

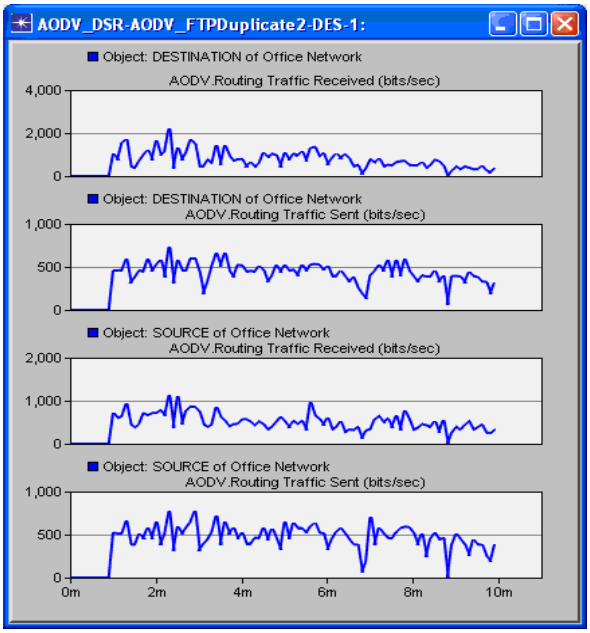


**Figure 5 Routing traffic received/ sent by destination / source**

another fixed node 3 comes into picture and new hope count becomes three and traffic sent / received further degrades. Thus the number hops in a route has direct impact on traffic being exchanged between destination and source.

Figure 6 and 7 clearly shows the movement of mobile node as well as that of destination itself. We can also clearly see that how fixed node 3 had come into the picture after the movement of destination.

## 4.3 Throughput

Wireless LAN throughput represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network. Figure 8 shows various throughput levels at different time of simulation. We can clearly see that the throughput decreases as the number of hop in active route increases. Initially when route was available only through mobile node 1, the throughput was highest which decreased after, the mobile node started moving. Through put further decreases when route had three in between nodes to send the traffic. Thus the throughput degrades as the number hops in the route increases.

## 4.4 Route Errors

During the simulation, route errors occur due to network specific characteristics. Because of these link breakages, more RREQs are sent by the destination again to establish the link between the source and the destination. Source also sends corresponding RREPs. Route error occurs when link breakage happens. AODV detects link breaks based on HELLO messages, as implemented in OPNET. When detecting link breaks using HELLO messages, each node waits to receive at least one HELLO message for the duration of "HelloInterval*HelloLoss". And also, each AODV node should process each packet (both data & control messages) to update the route lifetime. When having more data at the link layer, the probability of Hello

packets to be lost is higher. And also, when processing more data packets (by the AODV

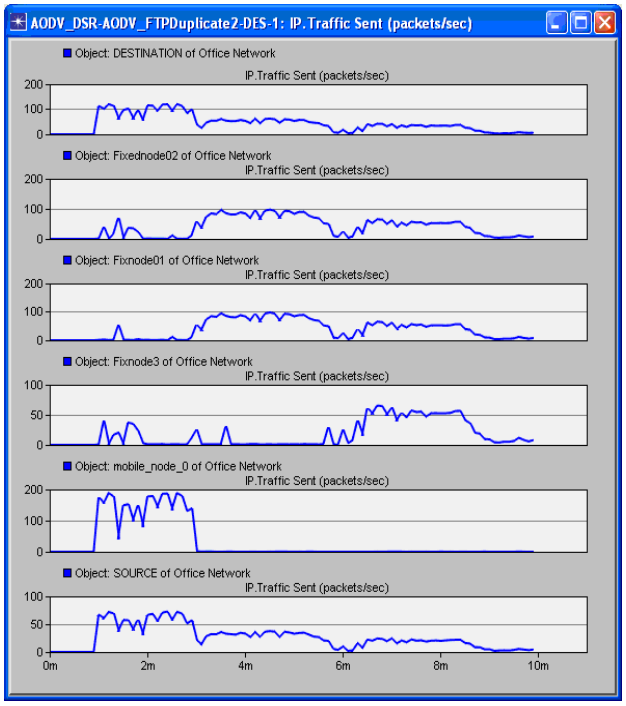


**Figure 6 IP Traffic sent by different nodes**

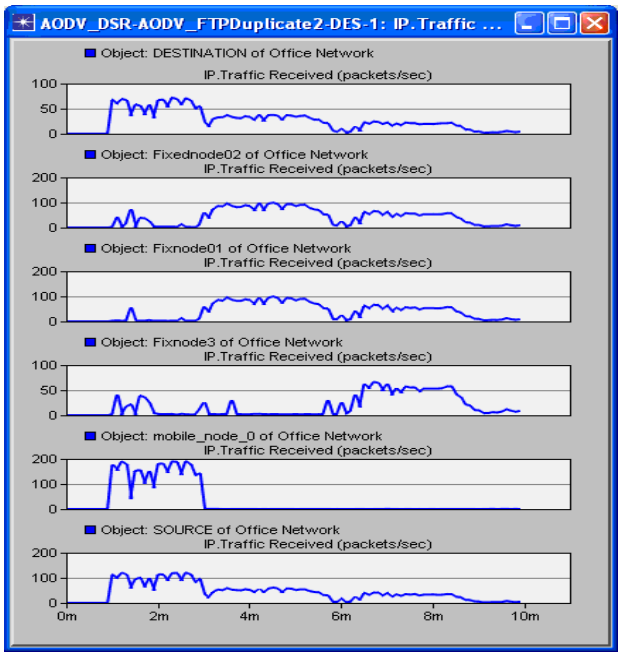


**Figure 7 IP traffic received by different nodes**

Protocol handler), the node takes a long time to process the HELLO message. Moreover as the number of nodes increases in the active node the chances of route error increases. If a Hello message is not received within the pre-defined interval (i.e. If the mobility is less in AODV network, it is better to use a higher value for HelloLoss, when transmitting higher data rates. HelloInterval*HelloLoss), the node invalidates the active route and decides that the neighbor is not reachable.

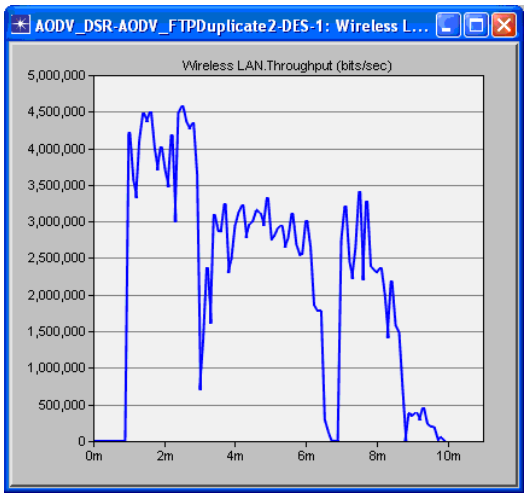


**Figure 8 WLAN Throughput**

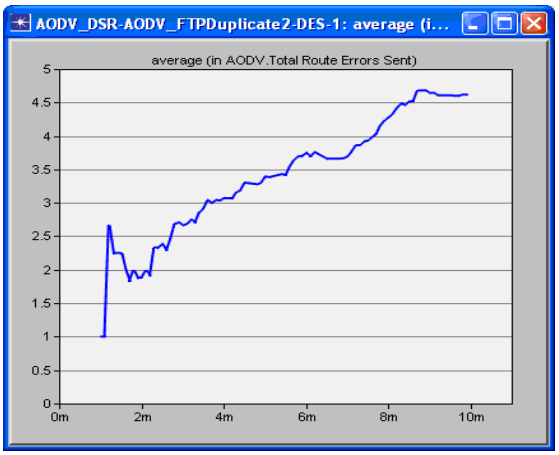


**Figure 9 Route Error**

As shown in figure 9, the route errors increases as the number of nodes increases in the active route.

## 5. Conclusion

In this work, performance analysis of AODV network using OPNET simulator is done. Clear understanding of protocol functioning regarding route discovery and maintenance is established. AODV routing traffic includes RREQ, RREP, RERR and Hello Massages. Network topology parameters like number of nodes in active route and mobility influence the performance of AODV protocol. With increase in number hops in active route, throughput degrades due to higher round trip time (RTT) delay. Increased number of nodes also increases the route errors in network.

## 6. REFERENCES

[1] OPNET Technologies. www.opnet.com.

[2] C. Perkins, B.-R. E., and D. S., "Ad hoc On-demand Distance Vector routing ,"Request For Comments (Proposed Standard) 3561, Internet Engineering Task Force

http://www.ietf.org/rfc/rfc3561.txt?number=3561, July 2003.

[3] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications, New York, Auerbach Publications, 2007.

[4] J. Broch et al., "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols," in Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking, Dallas, Texas, United States, October 1998, pp. 85–97.

[5] E. Royer and C. Toh, "A Review of Current Routing Protocols for Ad-hoc Mobile Wireless Networks," IEEE Personal Communication Magazine, vol. 6, pp. 46-55, April 1999.

[6] K. Gorantala, "Routing Protocols in Mobile Ad-hoc Networks," M.S. Thesis, Umeå University, Sweden, 2006.

[7] List of ad-hoc routing protocols [online]. Available: http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols.