

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

A Study on the Applicability of AOMDV Protocol for MANET

P.Sudarsun, Suresh Raj, Venkatesh Prashanth, V.Vignesh

Department of ECE, Paavai Engineering College, Namakkal, TamilNadu, India

Department of ECE, Paavai Engineering College, Namakkal, TamilNadu, India

Department of ECE, Paavai Engineering College, Namakkal, TamilNadu, India

Asso. Prof, Department of CSE, Paavai Engineering College, Namakkal, TamilNadu, India

I. INTRODUCTION

In the present research the performance of the AOMDV is evaluated. The different existing reactive routing protocols such as AODV, AOMDV, DSR and TORA are compared with the proactive routing protocol such as DSDV based on the performance parameters such as energy consumption, packet delivery ratio, packet lost, end to end delay and throughput. It proved that the most efficient protocol among the above five routing protocols is AOMDV. The result shows the suitability of using AOMDV for efficient routing in MANET. The main reason behind this is that AOMDV is a multipath routing protocol and if a particular route fails due to congestion it can use other routes.

II. DESTINATION SEQUENCE DISTANCEVECTOR

DSDV is a proactive routing protocol and is based on the distance vector algorithm (Pravin Ghosekar et al 2010). In proactive or table driven routing protocols, each node continuously maintains up-to-date routes to every other node in the network. Routing information is periodically transmitted throughout the network in order to maintain routing table consistency. The routing table is updated at each node by finding the change in routing information about all the available destinations with the number of nodes to that particular destination. Also, to provide loop freedom DSDV uses sequence numbers, which is provided by the destination node. In case, a route has already existed before traffic arrives, transmission occurs without delay. Otherwise, traffic packets should wait in queue until the node receives routing information related to its destination. However, for a highly dynamic network topology, the proactive schemes require a significant amount of resources to keep routing information up-to-date and reliable.

In case of failure of a route to the next node, the node immediately updates the sequence number and broadcasts the information to its neighbors. When a node receives routing information, it checks in its routing table for the same and if it does not find such entry in the routing table, then it updates the routing table with routing information received. In case, the node finds that the entry is already in the routing table, then it compares the sequence number of the received information with the routing table entry and updates the information. If it has a sequence number that is less than that of the received information then it discards the information with the least sequence number. If both the sequence numbers are the same, then the node keeps the information that has the shortest route or the least number of hops to that destination.

The advantages of DSDV are:

- Simple (almost like DistanceVector)
- Loop-free through destination sequencenumbers

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

- No latency caused by route discovery
- DSDV was one of the earliest algorithms available. It is quite suitable for creating ad hoc networks with a small number of nodes.

The disadvantages of DSDV are:

- No sleeping nodes.
- Overhead: more routing information never used.
- DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.
- Whenever the topology of the network changes, a new sequence number is necessary before the network re-converges; thus, DSDV is not suitable for highly dynamic networks.

III. DYNAMIC SOURCE ROUTING

DSR is a reactive protocol. This protocol is one of the examples of an on-demand routing protocol that is based on the concept of source routing (Pravin Ghosekar et al 2010). It is designed for use in multi-hop ad hoc networks of mobile nodes. DSR uses no periodic routing messages like AODV, thereby it reduces network bandwidth, overhead, conserves battery power and avoids large routing updates. However, it needs the support from the MAC layer to identify a link failure. The DSR routing protocol discovers routes and maintains information regarding the routes from one node to another by using two main mechanisms: (i) Route discovery – Finds the route between a source and destination and (ii) Route maintenance – In case of route failure, it invokes another route to the destination. DSR has a unique advantage by virtue of source routing. As the route is part of the packet itself, routing loops, either short – lived or long – lived, cannot be formed as they can be immediately detected and eliminated. This property of DSR opens up the protocol to a variety of useful optimizations. If the destination alone can respond to the route requests and the source node is always the initiator of the RREQ, then the initial route will be the shortest. The packet in DSR carries all information pertaining to route in its preamble (header) thus permitting the intermediate nodes to cache the routing information in their route tables for their future use.

In DSR Protocol, route discovery is the process in which a source, in order to send data to a destination, obtains the route to the destination, even if it does not have a route to the destination. Route maintenance is the mechanism by which the node keeps the record of dynamic changes of the network topology. In other words, source node checks for any link failure between source and destination. If a link failure is found between the source and destination, the source node tries to find another route to the destination or invokes route discovery, thereby the communication between source and destination continues to establish.

The advantages of DSR are:

- It does not make use of periodic routing advertisements
- Save the bandwidth
- The overhead of DSR is potentially larger

IV. AD HOC ON-DEMAND DISTANCE VECTOR

The AODV routing protocol builds on the DSDV algorithm, it is an on demand routing algorithm, but in contrast to DSR it is not a source based routing scheme rather every hop of a route maintains the next hop information by its own. Operation of the protocol here is also divided into two functions, route discovery and route maintenance. At first, all the

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

nodes send HELLO messages on its interface and receive HELLO messages from its neighbors. This process repeats periodically to determine neighbor connectivity. When a node is in need of a route to a destination, the protocol starts route discovery. The source sends RREQ Message (Kanakaris et al 2010) to its neighbors. If a neighbor has no information about the destination, it will send messages to its neighbors and the process continues. Once the request reaches a node that has information about the destination (either the destination itself or some node that has a valid route to the destination), that node sends Route Reply message (RREP) to the RREQ Message initiator. In the intermediate nodes (the nodes that forward RREQ Message), information about the source, destination and the address of the neighbors in the RREQ Message is saved. In this method, the RREQ message reaches a node which has the information to answer the RREQ Message and records a path the in the intermediate nodes. This path identifies the route that the RREQ Message took and is called reverse path as shown in Figure 3.1.

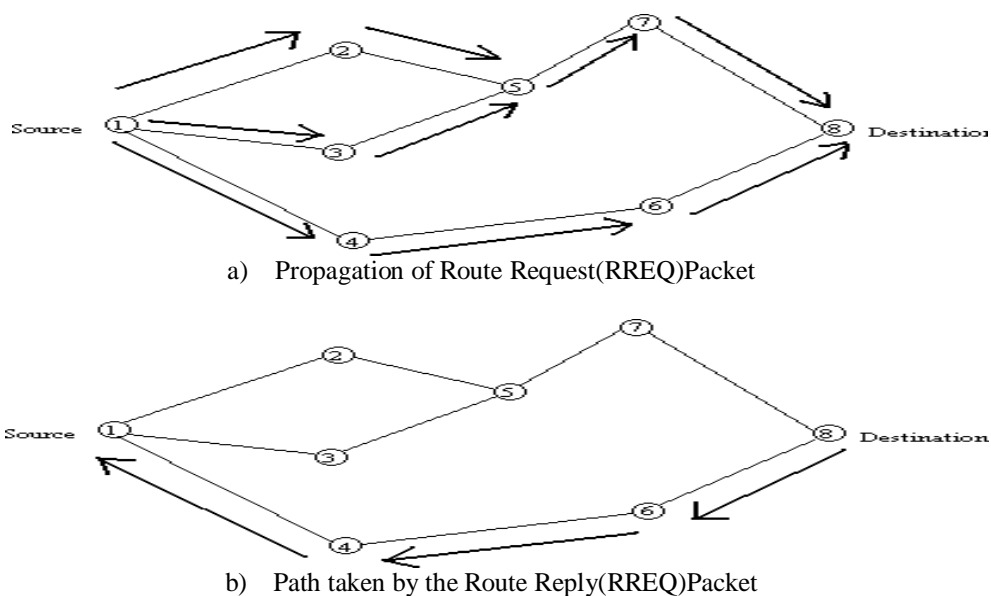


Figure 3.1 Route discoveries in AODV

As each node forwards the RREQ message to all of its neighbors, more than one copy of the original RREQ message can arrive at a node. The RREQ message created at the initiator has assigned a unique id. When a node receives the RREQ message, it will check the unique id and the address of the initiator and discards the message if it had been already processed. The route will be ready when a route reply message reaches the initiator, and the initiator starts sending datapackets.

If a link on the forward path breaks, the intermediate node just before the link sends a new Route Error (RERR) message to all the sources that are using the forward path to inform them of the link failure. It does this by sending the message to its neighbors using this forward path and the neighbors will send the same to their neighbors until all the upstream nodes that use this forward path are informed. The RREQ is initiated if the node still need to route packets to the destination (Yumei Liu 2008).

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

The Merits of AODV are:

The AODV routing protocol does not need any central administrative system to control the routing process. It tends to reduce the control traffic message overhead at the cost of increased latency in finding new routes. AODV reacts relatively fast to the topological changes in the network and updates only the nodes affected by these changes. The HELLO messages supporting the route maintenance are range-limited, so they do not cause unnecessary overhead in the network. There is only one entry per destination in the routing table. If a node has to choose between two routes, the updated route with a greater destination sequence number is always chosen. If the routing table entry is not used for a period of time, the entry will be expired. An invalid route is deleted and the error packets reach all nodes using a failed link on its route to any destination. Routes are established on demand and destination sequence numbers are used to find the latest route to the destination and lower delay for connection setup.

The Drawbacks of AODV are:

It is possible that for a valid route to expire and determining a reasonable expiry time is difficult, because the nodes are mobile and sources sending rates may differ widely and can change dynamically from node to node. Moreover, AODV can gather only a very limited amount of routing information. This causes AODV to rely on a route discovery flood more often, which may carry significant network overhead. Uncontrolled flooding generates many redundant transmissions which may cause so-called broadcast storm problem. The performance of the AODV protocol without any misbehaving nodes is poor in larger networks. The main difference between small and large networks is the average path length. A long path is more vulnerable to link breakages and requires high control overhead for its maintenance. Furthermore, as the size of a network grows, various performance metrics starts decreasing because of the increasing administrativework.

AODV is vulnerable to various kinds of attacks, because it is based on the assumption that all nodes will cooperate. There are two main types of uncooperative nodes: malicious and selfish. Malicious nodes are either faulty and cannot follow the protocol, or are intentionally malicious and try to attack the network. Selfish nodes are non-cooperative in certain network operations and drops packets which may affect the performance, but can save the battery power. Multiple route reply packets in response to a single RREQ packet can lead to heavy control overhead. Periodic beaconing leads to unnecessary bandwidth consumption.

V. TEMPORALLY ORDERED ROUTINGALGORITHM

TORA routing protocol is based on “link reversal” algorithm. Every node has information regarding its adjacent nodes. In this way, TORA provides multiple routes for any pair of nodes. Moreover, it has the ability to quickly follow the topological changes that may occur and re-create valid routes. Hence, when a node seeks a route to a given destination, it sends a Query message which includes the address of the destination node. This packet travels through the network until it reaches the destination or an intermediate node that has a route to the destination node. The receiver node, then broadcasts an updated packet, listing the number of direct links that has been used in order to reach the destination. As this node propagates this updated information packet through the network, each node updates its list by adding another pair of nodes (source-destination). This creates a series of direct links from the node that originated the Query to the destinationnode.

When the node finds a specific destination which is unreachable, it sets a local maximum value of direct links to that destination. If the node cannot find any adjacent node which has a list of direct links to the destination, it attempts to search for a new route. If there is a network partition, then the node sends a clear message that resets all routing states and removes invalid routes from the network. TORA operates on top of Internet MANET Encapsulation Protocol (IMEP) providing reliable delivery of route- messages and informs the routing protocol about the changes to the links to its neighbors. IMEP tries to aggregate IMEP and TORA messages into a single packet (called a block) in order to reduce overhead. For link-status sensing and list maintenance, IMEP sends out periodic Beacon messages which are

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

answered by each node that hears it with a HELLO reply message (Pravin Ghosekar et al2010).

VLAD HOC ON DEMAND MULTI PATH DISTANCEVECTOR

AOMDV shares several characteristics with AODV and is an extension to the AODV protocol. Moreover, AOMDV also finds routes on demand using a route discovery procedure. The main difference lies in the number of routes found in each route discovery. It computes multiple loop-free and link-disjoint paths. In AOMDV, RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple route replies traverse through these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing the route discovery frequency (Padmini Misra 2004).

The routing entries for each destination contain a list of the next hops along with the corresponding hop counts. All the succeeding hops have the same sequence number to keep track of a route. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count for all the paths, which is used for sending route advertisements of the destination. Each duplicate route advertisement received by a node defines an alternate path to the destination.

Loop freedom is assured for a node by accepting alternate paths to the destination if it has a less hop count than the advertised hop count. As the maximum hop count is used, the advertised hop count therefore does not change for the same sequence number. When a route advertisement is received for a destination with a greater sequence number, the next hop list and the advertised hop count are reinitialized.

AOMDV can be used to find node-disjoint or link-disjoint routes. To find node-disjoint routes, each node does not immediately reject duplicate RREQs. Each RREQs arriving via a different neighbors of the source defines a node-disjoint path. This is because nodes cannot broadcast the duplicate RREQs, so any two RREQs arriving at an intermediate node via a different neighbor of the source could not have traversed the same node. In an attempt to get multiple link-disjoint routes, the destination only replies to RREQs arriving via unique neighbors. After the first hop, RREPs follow the reverse paths, which are node-disjoint and thus link-disjoint. The trajectories of each RREP may intersect at an intermediate node, but each takes a different reverse path to the source to ensure linkdisjointness.

6.1 Detailed ProtocolDescription

AOMDV protocol has four components: routing table structure, route discovery, route maintenance, and data packet forwarding.

6.2 Routingtable

The key distinguishing feature of AOMDV over AODV is that it provides multiple paths to the destination. These paths are loop-free and mutually link-disjoint. In both AODV and AOMDV, receipt of a RREQ initiates a node route table entry in preparation for receipt of a returning RREP. In AODV the routing table entry contains the fields as shown in Figure 3.2(a) where, time out gives the time after which, a corresponding RREP has not been received, the entry is discarded. The routing table entry in AOMDV is slightly modified to allow for maintenance of multiple entries and multiple loop-free paths. Firstly, advertised hop count replaces hop-count and advertised hop-count forms the maximum paths from the current node to the destination node (n_d), so, only one value is advertised from that node for a given destination sequence number. Secondly, next-hop IP address is replaced by a list of all next-hop nodes and corresponding hop counts of the saved paths to n from that node, as shown in Figure 3.2 (b).d

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

To obtain link-disjoint paths in AOMDV n can reply to multiplied copies of a given RREQ, as long as they arrive via different neighbors. AOMDV relied as much as possible on the routing information already available in the underlying AODV protocol, thereby limiting the overhead incurred in discovering multiple paths. In particular, it does not employ any special control packets. In fact, extra RREPs and RERRs for multipath discovery and maintenance along with a few extra fields in routing control packets constitute the only additional overhead in AOMDV relative to AODV.

Destination	Sequence no	Hop-count	Next-hop	Time-out
-------------	-------------	-----------	----------	----------

a) AODV

Destination	Sequence no	Advertised hop count	Route list			
			Next-hop1	Last-hop1	Hop-count 1	Time-out 1
			Next-hop 2	Last-hop 2	Hop-count 2	Time-out 2
		
		

b) AOMDV

Figure 3.2 Routing table entry structure in (a) AODV (b) AOMDV

6.3 Routediscovery

As in AODV, when a traffic source needs a route to a destination, the source initiates a route discovery. When an intermediate node obtains a reverse path via a RREQ copy, it checks whether there are one or more valid forward paths to the destination. If so, the node generates a RREP, and sends it back to the source along the reverse path; the RREP includes a forward path that was not used in any previous RREPs for this route discovery. In this case, the intermediate node does not propagate the RREQ further. Otherwise, the node re-broadcasts the RREQ copy if it has not forwarded any other copy of this RREQ previously and this copy results in the formation/updation of a reversepath.

When the destination receives RREQ copies, it also forms reverse paths in the same way as intermediate nodes. However, it adopts a somewhat „looser“ policy for generating a RREP. Specifically, the destination ~~generates~~ ^{sends} a RREP in response to every RREQ copy that arrives via a loop-free path. The reason behind the looser RREP generation policy at the destination is: The RREQ flooding mechanism, where each node locally broadcasts a RREQ once, suppresses some RREQ copies at intermediate nodes and duplicates other RREQ copies. As a result, multiple disjoint paths can get coalesced at intermediate nodes and appear as a single path at the destination. Therefore, the destination sends back a RREP along each loop-free reverse path even though it is not disjoint with previously established reverse paths. Such additional RREPs alleviate the route cutoff problem and increase the possibility of finding more disjoint forwardpaths.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

6.4 Routemaintenance

Route maintenance in AOMDV is a simple extension of AODV route maintenance. Like AODV, AOMDV also uses RERR packets. A node generates or forwards a RERR for a destination when the last path to the destination breaks. AOMDV also includes an optimization to salvage packets forwarded over failed links by re-forwarding them over alternate paths. This is similar to the packet salvaging mechanism in DSR as per Kanakaris et al (2010). The timeout mechanism similarly extends from a single path to multiple paths, although the problem of setting proper timeout values is more difficult for AOMDV compared to AODV. With multiple paths, the possibility of paths becoming stale is more likely. But using very small timeout values to avoid stale paths can limit the benefit of using multiple paths. In AOMDV, a moderate setting of timeout values is used and additionally uses HELLO messages to proactively remove staleroutes.

6.5 Data packetforwarding

For a data packet forwarding at a node having multiple paths to a destination, a simple approach of using a path is adopted until it fails and then switches to an alternate path. The paths are used in the order of their creation.

Advantages

- It allows intermediate nodes to reply to RREQs, while still selecting disjointpaths
- Minimum energy is consumed compared to many other protocols
- Better packet deliveryratio
- Lowerdelay

Disadvantage

- AOMDV has more message overheads during route discovery due to increased flooding and since it is a multipath routing protocol, the destination replies to the multiple RREQs that results in longeroverhead.

VII. METRICS CONSIDERED FOREVALUATION

RFC 2501 describes a number of quantitative metrics that can be used for evaluating the performance of a routing protocol for mobile wireless ad hoc networks. The snapshots for measurement of these metrics are given in Appendix 1. Some of these quantitative metrics are defined as follows:

1. Packet delivery ratio

The packet delivery ratio is defined as the ratio of the number of data packets received at the destinations over the number of data packets sent by the sources as given in Equation (3.1). This performance metric is used to determine the efficiency and accuracy of MANET routing protocols.

$$\text{Packet Delivery ratio} = \frac{\text{Total data packets received}}{\text{Total data packets sent}} \times 100 \quad (3.1)$$

2. Energy consumption

This is the ratio of the average energy consumed in each node to total energy as given in the Equation (3.2).

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

$$\text{Energyconsumption} = \frac{\text{Energyremaininginthenode}}{\text{Total energy}} \quad (3.2)$$

3. End to enddelay

This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets as given in Equation (3.3). This metric is important in delay sensitive applications such as video and voicetransmission.

$$\text{Average EndtoEnddelay} = \frac{\sum \text{Time received} - \text{time sent}}{\text{Totaldatapacketsreceived}} \quad (3.3)$$

4. Throughput

The throughput metric measures, how well the network can constantly provide data to the sink. Throughput is the number of packets arriving at the sink per ms. A network throughput is the average rate at which message is successfully delivered between a destination node (receiver) and source node (sender). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination. Throughput can be measured as bits per second (bps), packets per second or packet per time slot. For a network, it is required that the throughput is at high level. Some factors that affect MANET's throughput are unreliable communication, changes in topology, limited energy and bandwidth.

5. Number of Packetsdropped

This is the number of data packets that are not successfully sent to the destination during the transmission. Packet loss occurs when one or more packets being transmitted across the network fail to arrive at the destination. It is defined as the number of packets dropped by the routers during transmission. It can be shown by Equations (3.4) to (3.6).

$$\text{Packet Loss} = \text{Total DataPacketsDropped} \quad (3.4)$$

$$\text{Packet Loss} = \text{Total Data Packets Sent} - \text{Total Data PacketsReceived} \quad (3.5)$$

$$\text{Packet loss (\%)} = \frac{\text{Total data packets dropped}}{\text{Total data packets sent}} \times 100 \quad (3.6)$$

VIII. SIMULATION

The aim of these simulations is to analyze the AOMDV protocol by comparing it with other protocols (AODV, DSR, TORA and DSDV) for its efficiency in terms of power as well as throughput. The simulation tool that has been used in this study is NS2. Communication Management Unit (CMU's) wireless extension to NS2 provides the implementation of the DSR, TORA, AODV, DSDV and AOMDV routing protocols. So, the simulation is carried out in NS2 under Linux platform for analyzing the performance of existing routing protocol for MANET. The Table 3.1 shows the important parameters chosen for the NS2 simulation. The performances of the five routing protocols with network size of 50 nodes with mobility (mobility 20 m/s) have been assessed.

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 3, March 2019

Table 8.1 Simulation parameters

Simulation Time	100s
Topology Size	1000m x 1500m
Number of Nodes	50
MAC Type	MAC 802.11
Radio Propagation Model	Two Ray Model
Radio Propagation Range	250m
Pause Time	0s
Max Speed	4m/Sec-24m/Sec
Initial Energy	1000J
Transmit Power	0.4W
Receive Power	0.3W
Traffic Type	Constant bit rate (CBR)
CBR rate	512 bytes x 6 per second
Number of Connections	50