ISSN 2348 – 7968

Comparison of AODV and AOMDV routing protocols

Ms. Akshata Prabhu[1], Mrs. Shoba Krishnan [2]
[1]Department of Electronics & Telecommunication, Mumbai University, Chembur
Email: akshata.n.prabhu@gmail.com
[2]Department of Electronics & Telecommunication, Mumbai University, Chembur

ABSTRACT

A mobile ad-hoc network is multi hop wireless network that consists of mobile nodes that communicate with each other. The nodes communicate with each other by means of the air as the medium. Each node in the network moves freely and so the topology changes continuously. One of the challenges of MANET is to design robust routing algorithms so that they adapt to frequently changing network topology. Simulation of variety of routing protocols has been carried out extensively. In this paper, we will study the performance of two types of On demand routing protocols-Ad-hoc On-demand Distance Vector (AODV) and Ad-hoc On-demand Multi path Distance Vector (AOMDV).

Keywords – Routing protocols, Network Simulator-2, AODV. AOMDV. Performance evaluation

I. INTRODUCTION

Mobile ad-hoc network is a wireless network which consists of mobile nodes. MANETs are composed of autonomous nodes and hence they do not require any central node to manage the network. Communication is based on the mutual agreement and understanding between the nodes. Each node sometimes acts as a router and sometimes act as a host. When the nodes initiate the communication they act as host. When the nodes discover and maintain routes to other nodes they act as routers.[1]As the nodes are mobile in nature, the topology of the network changes continuously over period of time. Transmission power and location of the nodes determine the topology of the network.

Mobile elements such as laptop, smart phone, tablet etc form a mobile ad-hoc network.[2] MANETS do not have a clear boundary as there is no preset infrastructure. Nodes co-operation is one of the important factors for the successful communication in the MANET. Range of wireless networks can be extended by extending the range of mobile nodes. Range depends on the concentration of wireless users. [2]

Efficient delivery of data packets between mobile nodes is one of the problems in ad-hoc networking. As the topology changes continuously routing in ad-hoc network is one of the challenges in MANETs.

II. ROUTING PROTOCOLS

Because of the absence of central co-ordinator, routing in ad-hoc networks is a crucial task. A routing protocol is used to provide communication between the nodes. Whenever a packet needs to be send to the destination a routing protocol is used. Various types of protocols have been designed based on the applications and type of network. Routing protocols in mobile ad-hoc networks can be classified into three categories as shown in Figure 1.

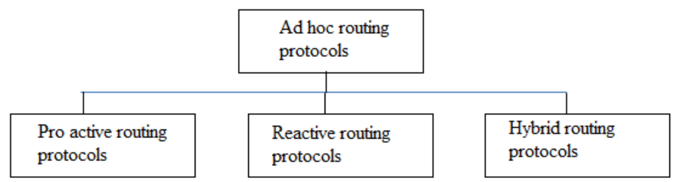

Figure 1 Classification of routing protocols[3]

A. Pro active routing protocols

Pro active protocols perform routing operations between source and destination pairs periodically, irrespective of the need of such routes.[4] By using periodically updated views of the network topology these protocols attempt to maintain shortest path routes. The main advantage of these protocols is providing lower latency in delivering data and hence used in applications which require high quality-of-service. As the update packets are send continuously even when there is no need it leads to wastage of bandwidth. Fish-eye State Routing (FSR), Destination-Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR) are some examples of pro active routing protocols

B. Reactive routing protocols

Reactive protocols minimize routing overhead by determining routes only when needed. When the source needs to send a data packet to the destination, these protocols perform a route discovery operation. The route is maintained as long as the existing link doesn't break. Reactive routing protocols have a less routing overhead as compared to pro active routing protocols. However, it has the disadvantage that a route discovery may involve flooding the entire network with query packets.[4] The different types of reactive protocols are Dynamic Source Routing Protocol (DSR),Ad-hoc On-demand Distance Vector (AODV) and Ad-hoc On-demand Multi path Distance Vector (AOMDV).

C. Hybrid routing protocols

The hybrid routing protocol combines the advantages of pro active routing and reactive routing to overcome the defects of them.[5] Table driven approach is used for table driven approach and on demand approach is used for inter-domain routing. Zone Routing Protocol (ZRP) is an example of Hybrid routing protocol.

Our discussion is limited to two on-demand ad-hoc routing protocols AODV and AOMDV.

III. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. AODV allows mobile nodes to respond to link breakages and changes in network topology in timely manner. [3]

To maintain each route entry destination sequence number is used by AODV. Sequence numbers serve as time stamps. They allow nodes to compare how fresh their information on other nodes is.[6] Destination creates the destination sequence number. The route having the greatest sequence number is selected by the requesting node. Sequence number ensures the freshness of the routes. Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RRERs) ate the three message types of AODV.

A. RREQ packet

RREQ packet is created by the sender when it wants to communicate with a node. This packet is broadcasted to find a route to the destination. Frame format of RREQ packet is as shown in Figure 2.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |J|R|G|D|U|   Reserved          |   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            RREQ ID                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination IP Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP Address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Originator Sequence Number                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2 Frame format of RREQ packet[3]

B. RREP packet

The RREQ message is received by the intermediate nodes in the network. Each node receiving the RREQ message will forward it to the neighboring node. RREP is prepared by the destination and unicast it to the source node. Frame format of RREP packet is as shown in Figure 3.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |R|A|    Reserved     |Prefix Sz|   Hop Count   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Destination IP address                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Destination Sequence Number                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Originator IP address                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           Lifetime                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3 Frame format of RREP packet[3]

C. RRER packets

If a link break is detected in the active route RER message is generated. Frame format of RREQ packet is as shown in Figure 4.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |N|          Reserved           |   DestCount   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Unreachable Destination IP Address (1)             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Unreachable Destination Sequence Number (1)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-|
|  Additional Unreachable Destination IP Addresses (if needed)  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Additional Unreachable Destination Sequence Numbers (if needed)|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4 Frame format of RRER packet[3]

IV. AD-HOC ON-DEMAND MULTI PATH DISTANCE VECTOR (AOMDV)

AOMDV is an extension of AODV protocol. The routing entry for each destination node contains a list of the next-hops along with the corresponding hop counts. All the next hops have the same sequence number. [1]AOMDV uses hop-by-hop routing approach and is based on distance vector concept. AOMDV shares several characteristic with AODV.

The main difference between AODV and AOMDV lies in the number of routes found in each route discovery.[7]In AOMDV, multiple reverse paths are formed at intermediate nodes as well as destination nodes as the RREQ propagates from source toward the destination.

Multiple paths are discovered in AOMDV which are loop-free and disjoint. A flood-based route discovery method is used for finding such paths. In AOMDV, the overhead incurred is limited by relying on the routing information already available in AODV protocol. [7]

Routing table entry structure is different for AOMDV as compared to AODV. A new field called advertised hop count is present in AOMDV route table. To store additional information about each alternate path a route list is used which includes next hop, last hop, hop count and expiration time out. Last hop information is useful in checking the disjointness of alternate paths. [7]

V. PERFORMANCE EVALUATION

Implementation of wireless ad-hoc networks in the real world is quite difficult. Hence simulation software is used which can mimic the real-life scenarios. The real life factors such as wind, humidity and human behavior cannot be generated in the scenarios but most of the characteristics can be programmed into the scenario. [1]

A. *Simulation tool*

For comparing the protocols Network Simulator-2 (NS-2) is used. NS-2 is an event driven network simulator program, developed at the University of California Berkley. NS-2 has been proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless networks can be done using NS-2. [4] It includes many network objects such as protocols, applications and traffic source behavior. NS-2 is freely distributed. It is used as a network simulation tool for hypothesis testing. NS-2 provides faithful implementation of network routing protocols.

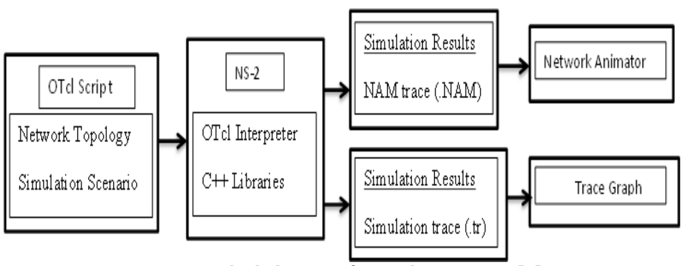

Figure 5 Block diagram for implementation [8]

NS-2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). C++ is used at the backend. It defines the internal mechanism of the simulation objects. OTcl is used at the frontend. It assembles and configures the objects as well as schedules the discrete events. OTcl and C++ are linked together. Outputs from NS-2 are either text-based or animation-based. To interpret these results, tools such as NAM (Network Animator) and XGraph are used. [4]

B. *Simulation environment*

We have done the comparison of AODV and AOMDV protocols. Simulation work is done in NS2 environment. Protocols have been analyzed under practical conditions to evaluate its performance in ad-hoc network.[9] Various scenarios are created. To analyze protocols various contexts are created by varying number of nodes. Movement of nodes is also one of the factors to be considered while analyzing the protocol. Table 1 shows the parameters which have been used in performing the simulation.

Parameters	Value
Simulator	NS-2 (version 2.34)
Simulation time	50 (s)
Number of mobile nodes	5,10,20,25,30
Routing protocol	AODV, AOMDV
Traffic rate	Constant bit rate
Packet size	512 bytes

Table 1 Simulation parameters

VI. SIMULATION RESULTS AND ANALYSIS

Performance of AODV and AOMDV can be analyzed by different simulation metrics such as end to end delay, packet delivery ratio, throughput and dropped packets. The results are summarized below with their corresponding graphs.

A. *Packet delivery ratio (PDR)*

It is the ratio of number of packets received at the destination to the number of packets generated at the source. Packet loss rate limits the maximum throughput of the network. [4] Packet delivery ratio evaluates the ability of the protocol to deliver data packets. [10]
Packet delivery ratio is given by

$$PDR = (Pr / Ps)$$

Where Pr is the number of packets received and Ps is the number of packets sent. Figure 6 shows the comparison of AODV and AOMV on the basis of Packet delivery ratio.

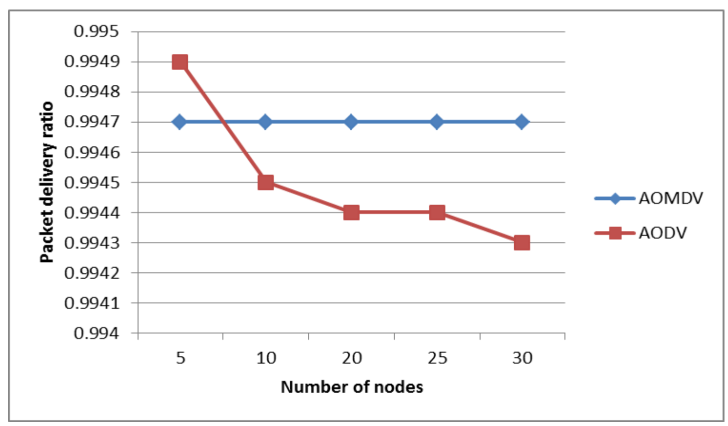

Figure 6 Packet delivery ratio for AODV and AOMDV

It can be seen from the above graphs that AOMDV has a better packet delivery ratio as compared to AODV. This is because when a link is broken in AOMDV an alternate path can be found whereas AODV is rendered useless. It can be seen that the packet delivery ratio decreases with increase in number of nodes for AODV

B. *End to end Delay*

This metric represents average end-to-end delay. It indicates how long it takes for the packet to travel from source to tha application layer of the destination. It is the difference between the receiving time and sending time. [10]It includes all possible delay caused by buffering during route discovery latency, transmission delays at the MAC, queuing at interface queue and propogation time. It is measured in seconds.[4] Figure 7 shows the comparison of AODV and AOMV on the basis of end to end delay.

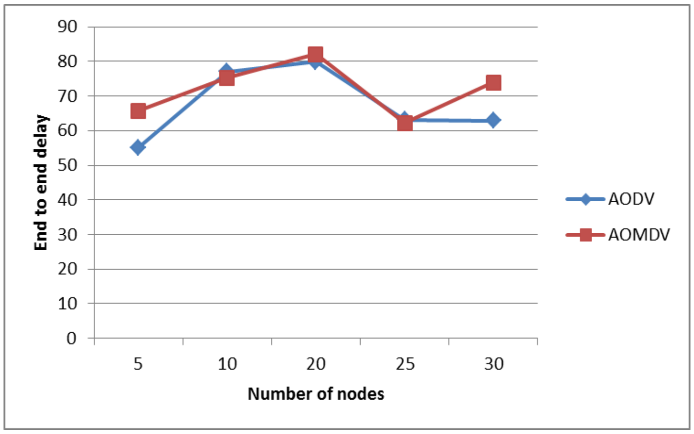

Figure 7 End to end delay for AODV and AOMDV

It can be seen from the above graphs that AODV has a better delay than AOMDV. This is because if a link breakage occurs in the network AOMDV will try to find an alternate route which exists among backup routes and so it results in delay in sending the packet from source to destination. In comparison, if a link breakage occurs in AODV, the packet will not reach the destination due to unavailability of another path.

C. *Dropped packets*

These are the number of packets which are dropped in the network due to collision. Figure 8 shows the comparison of AODV and AOMV on the basis of dropped packets.

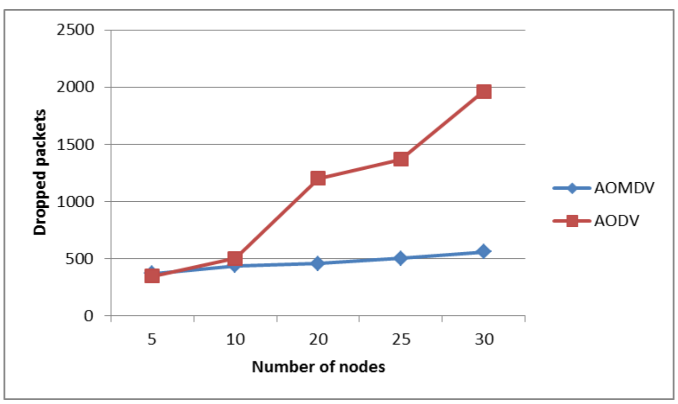

Figure 8 Dropped packets for AODV and AOMDV

It can be seen from the above graphs that number of packets dropped in AODV are more as compared to number of packets dropped in AOMDV. This is because AODV is a uni-path routing protocol and hence if the link is broken, the packet will not be delivered to the destination. So the packet will be dropped. In case of AOMDV, even if the link breaks the network will find another path and so there are better chances of packet delivery.

D. *Throughput*

Throughput is total packets delivered to the destination over total time divided by total time. It is also defined as the number of bits received over the difference between the first and last received packets.[8] It is measured in kbps. Figure 9 shows the comparison of AODV and AOMV on the basis of throughput.

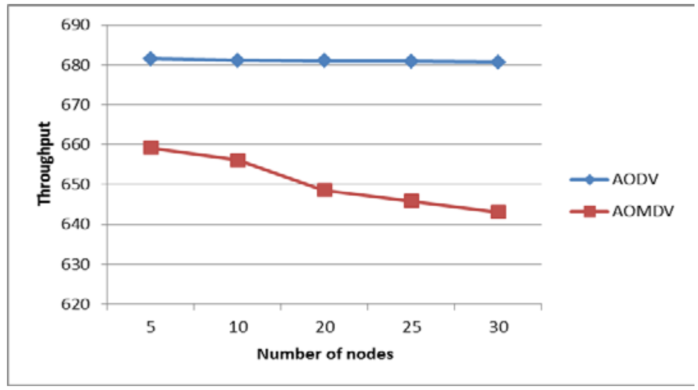

Figure 9 Throughput for AODV and AOMDV

It can be seen from the above graphs that throughput for AODV is better as compared to that of AOMDV. This is because time taken for packets to reach in AODV is less as compared to AOMDV. Also the number of bits transmitted per second in AODV is more than AOMDV.

VII. CONCLUSION

This paper evaluated the performance of AODV and AOMDV using NS-2. Based on the comparison on packet delivery ratio, throughput and end-to-end delay, we conclude that AOMDV is better than AODV. This is because of the ability of AOMDV to search alternate paths when a link breaks down. AODV shows better performance than AOMDV with respect to throughput. Hence we can say that AOMDV is better on-demand routing protocol than AODV since it provides better statistics for packet delivery ratio and dropped packets.

VIII. REFERENCES

[1] R.Balakrishna, U.Rajeswar Rao, N Geethanjali, " Performance issues on AODV and AOMDV for MANETs", International Journal of Computer Science and Information Technologies,Vol,1(2),2010

[2] Aditya Bakshi, A.K.Sharma, Atul Mishra ,"Significance of Mobile AD-HOC Networks (MANETS)," International Journal of Innovative Technology and Exploring Engineering (IJITEE),Volume-2,Issue-4,March 3013

[3] Neelam Khemariya, Ajay Khuntetha, "Efficient algorithm for detection of Black hole attack in AODV based MANETs", International Journal of Computer Applications (0975-8887) Volume 66-No.18, March 2013

ISSN 2348 – 7968

[4] Manveen Singh Chadha,Rambir Joon, Sandip, " Simulation and Comparison of AODV, DSR and AOMDV Routing Protocols in MANETs", International Journal of Soft Computing and Engineering (IJSCE), Volume-2, July-2012

[5] Fan-Hsun Tseng, Li-Der Chou, Han-Chieh Chao, " A survey of black hole attacks in wireless ad hoc networks", Human-centric Computing and Information Sciences 2011, Springer Open Journal.

[6] Luke Klein Berndts, 'A quick guide to AODV routing' Wireless Communication Technologies Group, National Institute of Standards and Technology

[7] Mahesh Karina, Samir Das, " Ad hoc on-demand multipath distance vector routing", Wiley InterScience, DOI:10,1002/wcm.432

[8] Vasanthavalli.S, R.Bhargava Rama Gowd , Dr.S.Thenappan, "Peruse Of Black Hole Attack and Prevention Using AODV on MANET ",International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Issue 5, May 2014

[9] Jaspal Kumar, M. Kulkarni, Daya Gupta, " Effect of Black Hole Attack on MANET Routing Protocols", I.J. Computer Network and Information Security, 2013,5.

[10] Pooja Jaiswal, Dr. Rakesh Kumar, "Prevention of Black Hole Attack in MANET", International Journal of computer Networks and Wireless Communications", ISSN: 2250-3301, Volume 2, No 5,October 2011

[11] http://www.isi.edu/nsnam/ns/tutorial/