ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

Performance Analysis of AODV Protocol

Gumaste S. V.[1], Dr. Kharat M. U.[2], Dr. Thakare V. M.[3]

Research Scholar, S.G.B.A.U., Amravati, Maharashtra, India[1]

Professor & Head, Department of CSE, MIT, Bhujbal Knowledge City, Nashik, India[2]

Professor & Head, Department of CSE,S.G.B.A.U., Amravati, Maharashtra, India[3]

ABSTRACT: Ad-hoc networking is a concept in computer communications characterized by connectivity through a collection of wireless nodes and fast changing network topology. In a wireless scenario, nodes are free to move hence maintaining path (route) is a difficult task comparatively wired scenario. Routing protocols have central role in a wireless scenario. We analyse AODV Protocol by extensive simulations in ns-2 simulator with various performance matrixes such as Packet Delivery Ratio, End-to-End Delay, Routing Overhead, throughput under wired and wireless scenarios.

Keywords: AODV, Routing Protocol, CBR, Request, Source, Destination, Path, Performance Evaluation.

I. Introduction

The need for Internet access through mobile devices, anywhere and anytime, has caused the development of model which is different in comparison to access based on a previously set fixed infrastructure over which wireless devices connect to the Internet nowadays. The new model is called Mobile Ad Hoc Network (MANET). MANET is a collection of wireless mobile nodes that communicate with each other using multi-hop wireless links without any existing network infrastructure or centralized administration [2]. Each node in the network behaves as a router and forwards packets for other nodes.Essentially the protocol describes the communication, i.e., sending and receiving information (called packets), between the nodes of a network. Ad-hoc networking is a rather new and hence not thoroughly explored technology. The protocol is a complex and changes constantly as the technology evolves. Therefore it offers us a good test-case for exploring requirements change. We omit a detailed description of the entire protocol and present small excerpts from it. Since the topology of an ad-hoc network is volatile, sending data from one node to another requires establishing a route between these nodes. Each node in the network is uniquely identified. It stores and updates a routing table containing routes already found from this node, called source, to the other nodes, called destinations, in the network. When the route is requested at the first time, node inserts it into its routing table with the status unknown. When the route is found it is marked as valid which means it can be used for sending packets. However, it can also become invalid when network topology changes. When node wishes to send a packet to the destination marked in the route, it sends the packet to the node which is listed as a next node from the observed source node in the route. In this way, packets are propagated toward destination nodes. Packets are buffered. Buffering allows the node to not process packets with the same identifier more than once.

II. AODV - Ad hoc On-Demand Distance Vector

AODV protocol is defined by the RFC 3561, written by Charles Perkins and Elizabeth [4]. AODV has some similar features as the Bellman-Ford distant vector algorithm, but it has been improved to work in a mobile environment [7]. AODV uses hop-by-hop routing (AODV Route Discovery Process – Figure 6). Every node forwards data packets towards a destination node according to its routing table (Figure 1). The routes in the AODV routing table are kept up to date as long as they are needed by the source. AODV maintains a single path per a destination. The routing is divided into two basic mechanisms. The first one is the route discovery. It is responsible for finding a route to the destination if none is currently available in the routing table of the node. The second one is the route maintenance which keeps the routes up-to-date, e.g. removes broken paths.AODV protocol also works in a network where the communication links are bidirectional because if an (intermediate) node receives either a Route REQuest (RREQ) packet or a Route REPly (RREP) packet, it caches the previous node in its routing table (figure 1) as a next hop to the end nodes.

Destination Id	Next hop

Figure1:AODV simpleroutingtable.

III. AODV Protocol - Control Packets

AODV uses four types of routing messages [1]. They are explained as follows:

- RREQ : If a node wants to communicate with other node but no route is available, the source node starts a route discovery by broadcasting a Route REQuest (RREQ) message in the network.*(Figure 2 and 2-1)*

<table>
<tr><td>Type: l J l R l G l D l U</td><td>Reserved</td><td>Hop Count</td></tr>
<tr><td colspan="3">RREQ id</td></tr>
<tr><td colspan="3">Destination IP Address</td></tr>
<tr><td colspan="3">Destination Sequence Number</td></tr>
<tr><td colspan="3">Originator IP Address</td></tr>
<tr><td colspan="3">Originator Sequence Number</td></tr>
</table>

Figure 2 :AODV RREQ Format

The fields of Route REQuest message are:

Type	1
J	Join Flag
R	Repair flag; reserved for multicast.
G	Gratuitous RREP flag; indicates whether agratuitous RREP should be unicast to the nodespecified in the Destination IP Address field
D	Destination only flag; indicates only thedestination may respond to this RREQ
U	Unknown sequence number; indicates the destinationsequence number is unknown
Reserved	Sent as 0; ignored on reception.
Hop Count	The number of hops from the Originator IP Addressto the node handling the request.
RREQ ID	A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.
Destination IP Address	The IP address of the destination for which a route is desired.
Destination Sequence Number	The latest sequence number received in the past by the originator for any route towards the destination.
Originator IP Address	The IP address of the node which originated the Route Request.
Originator Sequence Number	The current sequence number to be used in the route entry pointing towards the originator of the route request.

Figure 2-1: AODV RREQ Format filed description

- RREP : If it is a destination node or an intermediate node has a valid route to the desired destination, it replies to a RREQ by unicasting a Route REPly (RREP) message back to the source node.*(Figure 3 and 3-1)*

<table>
<tr><td>Type: l R l A</td><td>Reserved</td><td>Prefix Size</td><td>Hop Count</td></tr>
<tr><td colspan="4">Destination IP Address</td></tr>
<tr><td colspan="4">Destination Sequence Number</td></tr>
<tr><td colspan="4">Originator IP Address</td></tr>
<tr><td colspan="4">Life Time</td></tr>
</table>

Figure 3: AODV RREQ Format

The fields of Route RREP message are:

Type	2
R	Repair flag; reserved for multicast.
A	Acknowledgment required;
Reserved	Sent as 0; ignored on reception.
Prefix Size	If nonzero, the 5-bit Prefix Size specifies that the indicated next hop may be used for any nodes with the same routing prefix (as defined by the Prefix Size) as the requested destination.
Hop Count	The number of hops from the Originator IP Address to the Destination IP Address. For multicast route requests this indicates the number of hops to the multicast tree member sending the RREP.
RREQ ID	A sequence number uniquely identifying the particular RREQ when taken in conjunction with the originating node's IP address.
Destination IP Address	The IP address of the destination for which a route is desired.
Destination Sequence Number	The destination sequence number associated to the route.
Originator IP Address	The IP address of the node which originated the RREQ for which the route is supplied.
Life Time	The time in milliseconds for which nodes receiving the RREP consider the route to be valid.

Figure 3-1: AODV RREQ Format filed description

- RERR: If a path breaks, the intermediate node generates a Route ERRor (RERR) message to inform its end nodes of the occurred link break. The RERR message is sent whenever a link break causes one or more destinations to become unreachable from some of the node's neighbour's. *(Figure 4 and 4-1)*

Type | N	Reserved	Destination Count
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: AODV RREQ Format

The fields of Route RERR message are:

Type	3
N	No delete flag; set when a node has performed a local repair of a link, and upstream nodes should not delete the route.
Reserved	Sent as 0; ignored on reception.
Destination Count	The number of unreachable destinations included in the message; MUST be at least 1.
Unreachable Destination IP Address	The IP address of the destination that has become unreachable due to a link break.
Unreachable Destination Sequence Number	The sequence number in the route table entry for the destination listed in the previous Unreachable Destination IP Address field.

Figure 4-1: AODV RREQ Format filed description

- HELLO: Each node broadcasts periodically a message with time to live (TTL) = 1, in order to maintain its neighbour list.

Type	Reserved

Figure 5: AODV RREQ Format

The fields of Route RERR message are:*(Figure 5 and 5-1)*

Type	4
Reserved	Sent as 0; ignored on reception.

Figure5 - 1 :AODV RREQ Format filed description

IV. AODV Route Discovery

If a source has no entry for a destination in its routing cache, it starts a route discovery process. It floods a RREQ packet in the network. The RREQ includes header fields with the following parameters: request ID, source node ID, destination node ID, hop count, sequence number of the source node, sequence number of the destination node and TTL (time-to-live). If an intermediate node receives a RREQ packet, it checks if it is the destination node. If not, it checks if it has seen this RREQ before by checking the request ID and source node ID. If this is the case the node just drops the packet and does not forward the RREQ any further. This avoids loops in the route. If the RREQ packet is not dropped, the intermediate node searches in its route cache table. If there is an active route to the destination, it sends back a RREP with its route entity. Otherwise it just rebroadcasts the received RREQ. If the destination node has received the RREQ, it generates a RREP packet and sends it back in reverse way to the source [8].

If an intermediate node receives either a RREQ or a RREP packet, it stores information about the previous node from which the packet was received in its routing table (Figure 1). With this mechanism, hop-by-hop routing, a node can therefore decide which next hop it can use to reach a destination node. [1]

AODV Route Maintenance

If a node tries to forward a message, but detects that there is a link break, i.e., the next node is not more reachable, the forwarding node sends back a RERR message towards the source node. Whenever a node receives a RERR message, it deletes all routes containing this broken link in its routing table. When the source receives the RERR packet, it also updates its routing table, but it does not send the RERR packet anywhere. If the data session has not yet been completed and the source does not have any other route to the destination, the node starts the route discovery process [2].

Caching in AODV

We saw that AODV finds new routes by making a route request broadcast which travels through various intermediate nodes before reaching the destination node. These requests carry a lot of information about the network topology as they pass through different nodes but due to lack of caches at intermediate nodes, this information cannot be tapped by the nodes to be used later. So by providing all the nodes with an extra cache and by making changes in the RREQ packet such as to enable them to carry the information about the nodes through which they pass, intermediate nodes can save the information about the network topology contained in the RREQ packets. This reduces the time and overhead to find new routes in cases of route failure. From now on, we will call the AODV with cache enabled as AODV-WC and AODV without caching as AODV-WOC.

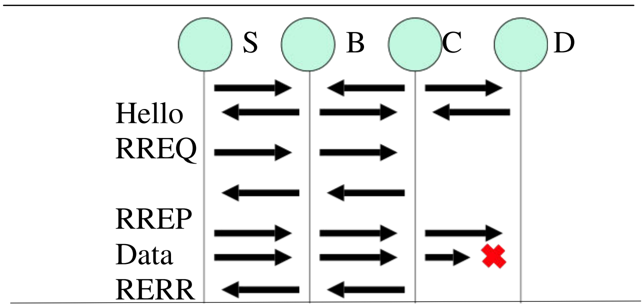


Figure 6. AODV Protocol Messaging

V. Performance Matric & Network Parameters:

The simulations were performed using Network Simulator Ns-2 (www.isi.edu/nsnam/ns), popular in the ad-hoc networking community. The mobility model used is Random Way point Model. The traffic sources are CBR (continuous bit –rate), number of data connections is 10, data packet size is 512 byte and data sending rate is 4 packet/second. The source-destination pairs are spread randomly over the network in a rectangular filed of 700 m X 500 m. During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. The simulation time is 500 seconds and maximum speed of nodes is 10 m/s. The interface queue is 150- packet drop-tail priority queue. Three types of network scenario are generated [3].

1. Wireless scenario with fixed position of nodes.
2. Wireless scenario with movable nodes (traffic generated by cbrgen and setdest.
3. Wireless scenario with movable nodes giving time slices for communication.

For network simulation, there are several performance metrics which is used to evaluate the performance. In simulation purpose we have used three performance metrics [5],[6].

1. Packet Delivery Ratio: Packet delivery ratio is the ratio of number of packets received at the destination to the number of packets sent from the source. The performance is better when packet delivery ratio is high.

$$PDR[\%] = \frac{\sum_i^n CBR\_received}{\sum_i^m CBR\_sent} X\ 100$$

2 Average end-to-end delay: This is the average time delay for data packets from the source node to the destination node. To find out the end-to-end delay the difference of packet sent and received time was stored and then dividing the total time difference over the total number of packet received gave the average end-to-end delay for the received packets. The performance is better when packet end-to-end delay is low.

$$\text{Average End to End Delay} = \frac{\sum_1^n(\text{CBR Sent } time - \text{CBR Received Time})}{\text{CBR Received}}$$

Where n is number of received packets.

3. Normalized Routing Load: Number of routing packets "transmitted" per data packet "delivered" at destination. Each hop-wise transmission of a routing is counted as one transmission. It is the sum of all control packet sent by all node in network to discover and maintain route.

$$\text{NRL} = \frac{\sum_1^k \text{Routing Packet}}{\sum_1^n \text{Received Packets}}$$

Where n is number of received packets and k is number of routing packets.

4. Average throughput: It is the ratio of total amount of data which reaches the receiver from sender to the time it takes for receiver to receive the last packet. It is represented in bits per seconds.

$$\text{Throughput (bits/sec)} = \frac{\text{(Received Size)}}{\text{(Stop time} - \text{start time)}} * \frac{8}{1000}$$

Where n is number of received packets and m is number of send packets.

VI. Result and Discussion

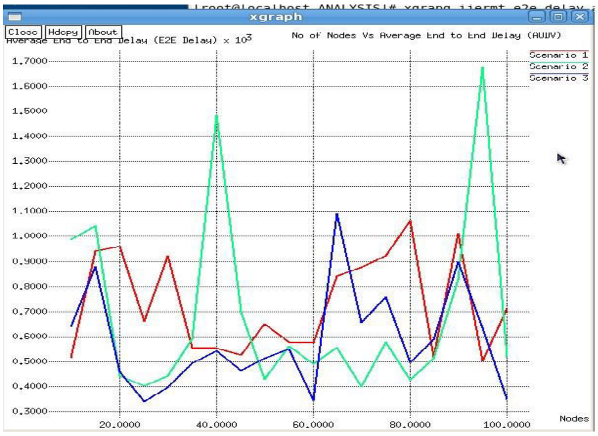
Average end-to-end Delay: Average end–end delay in AODV is low with fixed position of ad-hoc nodes (Scenario-1) as compared to movable nodes/ large number of nodes particularly (Scenario-2). *(Figure 7)*

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013



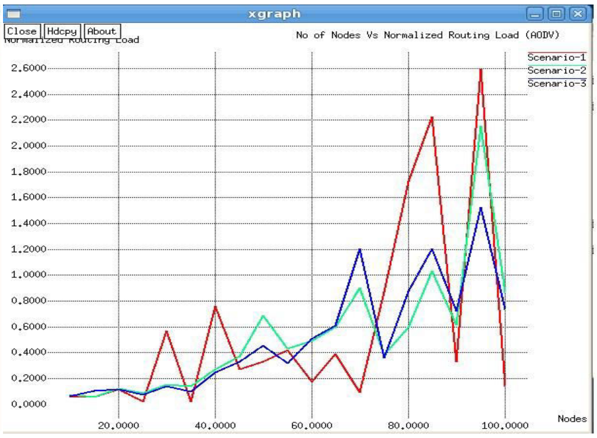
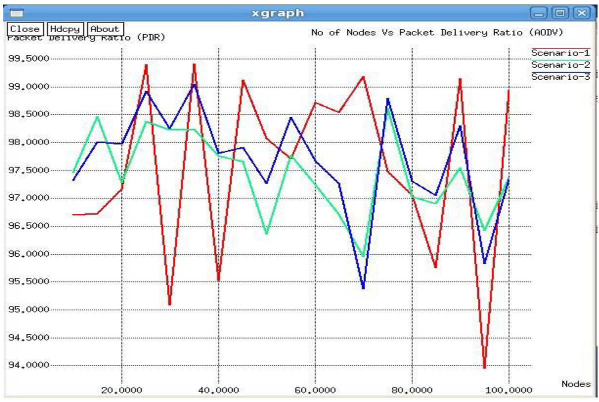


Figure 7: Number of Nodes V/S End to end Delay

Figure 8: Number of Nodes V/S Normalized Routing Load

Normalized Routing Load: With low number of sources/nodes (say 10) AODV performs better. But as mobility and large number of nodes/sources, performance of AODV concerned to normalized routing load degrades *(Figure 8).*

Packet delivery ratio:AODV shows consistence performance in mobile nodes as compared to nodes with fixed positions. In case of fixed nodes (wireless), an AODV protocol fluctuates (Scenario-1 of Figure 9)



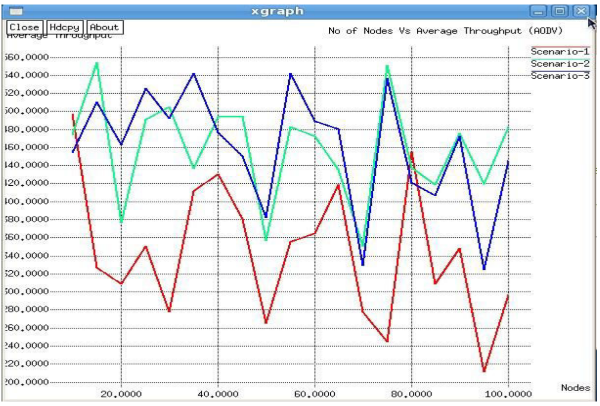


Figure 9: Number of Nodes V/S Packet Delivery Ratio

Figure 10: Number of Nodes V/S Throughput

Throughput:AODV gives better throughput performance for less number of source/nodes under mobility *(Figure 10).*

VII. CONCLUSION

AODV shows low routing load and high packet delivery ratio for less number of sources, and better throughput for less number of mobile nodes. AODV is a flat reactive (or on-demand) protocol, set up a path between the sender and the receiver only if a communication is waiting. An advantage of a reactive protocol is its scalability as long as there is only light traffic and low mobility. The disadvantages are: (a) the initial search latency may degrade the performance of the interactive applications, (b) the quality of the path is unknown in advance, and (c) route caching mechanism is useless in high mobility networks as routes change frequently.

VIII. FUTURE WORK

Performance analysis of AODV, DSR, DSDV routing protocols for performance measures like throughput, end to end delay, packet delivery ratio, normalized routing load. Then to analysis these parameters by varying pause time / mobility of nodes (speed).

REFERENCES

1. http://www.ietf.org/rfc/rfc3561.txt
2. Ian D. Chakeres and Elizabeth M. Belding-Royer. AODV Routing Protocol Implementation Design, International Journal of Wireless and Mobile Computing (IJWMC) Issue 2/3, 2005
3. Gao, Fang, Lu, Yuan, Zhang, Qingshun and Li, Chunli. Simulation and Analysis for the Performance of the Mobile Ad Hoc Network Routing Protocols.
4. Charles E. Perkins and Elizabeth M. Belding-Royer, Ad hoc On-Demand Distance Vector (AODV) Routing, 19 January 2002, [Online] http://tools.ietf.org/html/draft-ietf-manet-aodv-10
5. Wang Lin-zhu, FANG Ya-qin and SHAN Min, “Performance comparison of Two Routing Protocols for Ad Hoc Networks”, WASE International conference on Information Engineering, 2009.
6. Mohammed Bouhorma, H.Bentaouit and A.Boudhir, “Performance comparison of Ad hoc Routing protocols AODV andDSR” ,IEEE 2009.
7. MainakChaudhuri, Mark Heinrich, Chris Holt, “Latency, Occupancy, and Bandwidth in DSM Multiprocessors: APerformance Evaluation”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 7, JULY 2003
8. Amita Rani and Mayank Dave, “Performance Evaluation of Modified AODV for Load Balancing”, Journal of Computer Science 3 (11): 863-868, 2007

BIOGRAPHY

S. V. Gumaste, BE (CSE), ME (CSE), was graduated at BLDEAssociations College of Engineering & Technology, Bijapur(Karnataka University, Dharwar), completed his post-graduation from COE, Badnera (SantGadge Baba Amravati University,Amravti).

Dr. M. U. Kharat, BE, MS, Ph.D. was educated at AmravatiUniversity. Presently he is working at the Institute of Engineering,Bhujbal Knowledge City, Nashik, Maharastra, India, as Professor &Head of the Computer Engineering Department.

Dr. V. M. Thakare, Head, Department of CSE, SantGadgeBaba Amravati University, Amravati. He has worked invarious capacities in academic institutions at the level ofProfessor, Head of Computer Engineering Department. Hisareas of interest include Digital image/Signal Processing,Computer Networks.