AODV Routing Protocol in VANETs in Comparison with OLSR and DSR

Rajan B. Upadhyay[1] Hitesh C. Patel[2]
[1]P.G Student [2]Assistant Professor
[1,2]Department of Information Technology
[1,2]Kalol Institute of Technology and Research Centre, Ahmedabad

Abstract— Vehicular Ad hoc Network (VANET) is a new communication paradigm that enables the communication process between these vehicles which acts as nodes in the network. Various methods of data dissemination in VANET are used to inform the vehicles about the dynamic road traffic conditions for achieving safe and efficient transportation. Ad-hoc On-demand Distance Vector (AODV) is a reactive routing protocol designed for the ad-hoc networks. AODV is an unicast routing protocol which establishes a route only when a node wants to send data packets. AODV involves route discovery and route maintenance process. Due to large delay in the route discovery process and due to route failure which may require a new route discovery process, the data transmission rate decreases and network overhead increases. In this paper we have discussed AODV protocol and its comparison with OLSR and DSR routing protocol.

Key words: VANET, AODV, OLSR, DSR

I. INTRODUCTION

Since their arrival in the 1970s, the use of wireless communication technology has increased. An ad hoc wireless network consists of mobile nodes which communicate with each other without any infrastructure. Vehicular Ad hoc Network (VANET) is a new technology integrating ad hoc network, WLAN and cellular technology to achieve intelligent inter-vehicle communications and improve road traffic safety and efficiency. IEEE formed the IEEE 802.11p task group for Wireless Access in Vehicular Environments (WAVE)[1].

VANET is a new distinctive form of Mobile Ad Hoc Network (MANET). Without having any infrastructure and legacy client and server communication, VANET is a highly autonomous network where each vehicle in it acts as a wireless router or a node to communicate with nearby vehicles and fixed roadside equipment. In VANET the movement of vehicles is affected by the factors like the structure of the road, traffic congestion and traffic rules. VANET involves topology which changes very rapidly and also the network gets disconnected frequently.

Intelligent Transportation Systems (ITS) is the main application of VANET. ITS includes a variety of applications such as traffic monitoring, control of traffic flows, blind crossing, prevention of collisions and nearby information services. Another application of VANETs is to provide internet connectivity to vehicular nodes while on the move, so the users can download videos, music and can send E-mails [8]. Proper communication between vehicle-vehicle and vehicle-infrastructure depends on efficient routing schemes. But it is a difficult task to design an efficient routing scheme due to unpredictable node density, fast movement of vehicles and constrained mobility.

II. AD HOC ON DEMAND DISTANCE VECTOR (AODV)

An ad hoc network is the cooperative engagement of a collection of mobile nodes without the required intervention of any centralized access point or without any existing infrastructure. Proactive routing protocols are not suitable for the nodes (vehicles) having high mobility in VANET. Proactive routing protocols may fails in VANET due to the large routing table information and consumption of more bandwidth [3]. AODV is a reactive routing protocol, so a route is created when a node wants to send a packet to another node. AODV provides loop-free routes even while repairing the broken links. Further, a node does not have to discover and maintain a route to another node until the two needs to communicate with each other unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between the other two nodes [2]. The algorithm's primary objectives are as following:

(1) To broadcast discovery packets only when a need arises.
(2) To distinguish between local connectivity management neighborhood detection and topology maintenance.
(3) To disseminate information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information about it [2].

A. AODV Path Discovery:

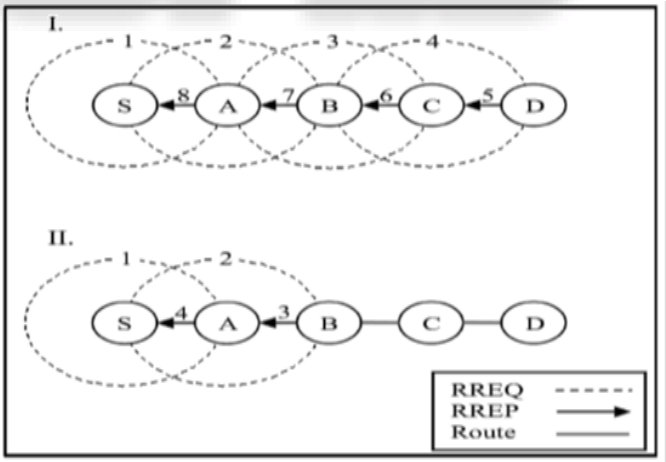

Fig. 1: Route Discovery Process

AODV path discovery process is originated whenever a source node needs to communicate with another node for which it has no routing information in its routing table. Every node maintains two separate counters: a node sequence number and a broadcast ID number. The source node initiates path discovery by broadcasting a Route Request (RREQ) packet to its neighbor nodes. The broadcast RREQ contains addresses of source and destination node, their sequence numbers, broadcast ID and a counter, which counts how many times a RREQ, has been generated from a particular specific node [10]. When an

intermediate node receives an RREQ, if it has already received an RREQ with the same broadcast ID and source address, it drops the redundant RREQ message and does not rebroadcast to make communication loop free from repeating.

Figure 1-I shows the route or path discovery process. A route is initiated at that time only when there is need. It happens at that period only when a source needs to communicate and the source is not having any route information of another node to which it wants to communicate.

Figure 1-I shows the route discovery process, in which the source node S broadcasts the route request (RREQ) and the destination node D unicasts the route reply (RREP) to the source S. If the node receives the RREQ message and it has the valid route to the destination in the routing table, then it unicasts the RREP to the source node in place of the destination node.

For example- Figure 1-II shows this process, in which the node B unicasts the RREP towards the S node in place of the destination node D. In route discovery phase when the node in the process receives the RREQ that it has already processed, it discards or drops the RREQ. After broadcasting a RREQ message, a node waits for a RREP for NET TRAVERSAL TIME milliseconds with current information regarding a route to the suitable destination. This waiting time increases in accordance to the binary exponential back off algorithm, if that node broadcasts more RREQ messages. If a route is not established in NET TRAVERSAL TIME milliseconds, the node may again try to discover a route by broadcasting another RREQ message up to a maximum of RREQ RETRIES times at the maximum TTL value.

B. AODV Reverse Path Setup:

There are two sequence numbers included in an RREQ message: the source sequence number and the destination sequence number known to the source node. The source sequence number is used to maintain freshness information about the reverse route to the source path, and the destination sequence number specifies how fresh a route to the destination path must be before it can be accepted by the source [7]. As the RREQ travels from a source node to various destinations, it automatically sets up the reverse path from all nodes back to the source node or path. To set up a reverse path, a node records the address of the neighbor node from which it received the first copy of the RREQ message.

C. AODV Forward Path Setup:

Finally, an RREQ will arrive at a node (possibly the destination itself) that possesses a current route to the destination node. If an intermediate node has a route entry for the desired destination path, then it determines whether the route is current by comparing the destination sequence number in its own route entry to the destination sequence number in the RREQ [7]. If the RREQ's sequence number for the destination path is greater than that recorded by the intermediate node, the intermediate node must not use its recorded route to respond to the RREQ message. Instead, the intermediate node rebroadcasts the RREQ message.

D. AODV Route Table Management:

Routing table entries associated with reverse-path entries is a timer known as "route request expiration timer". The main purpose of this timer is to avoid reverse-path routing entries from those nodes that do not exist on the path from the source to the destination [9]. In each routing table entry, the address of the active neighbor's node through which packets for the given destination are received is also maintained. A neighbor node is considered active for that destination if it originates at least one packet for that destination within the most recent active timeout period.

E. AODV Path Maintenance:

If the source node moves during an on-going session, it can re initiate the route discovery procedure to establish a new route to the destination node. When either the destination node or some intermediate node moves, a special RREP is sent to the affected source nodes. Periodic Hello messages can be used to ensure symmetric links, as well as for the detection of link failures. When the node does not receive any packets from a neighbor node during a few seconds, it assumes a link break to the neighbor and such failures could be detected by using link layer acknowledgments (LLACKs).

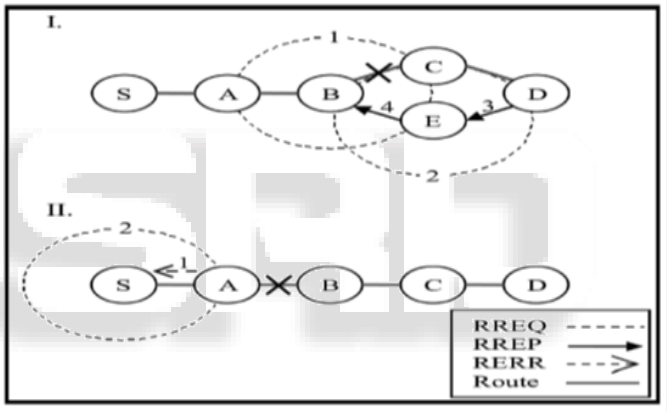

Fig. 2: Route Maintenance Process

Figure 2-I shows the process of the local repair after the route breaks between the node B and C. The route break is closer to the destination path than the source hence local repair is initiated here. But when the node that detects route break is farther from the destination as in the Figure 2-II the local repair is not initiated at that time instead a node propagates a route error message (RERR) towards the source node. RERR messages possess the address of the unreachable destinations. When each intermediate node receives the RERR message, the routes which have the unreachable destination node and have the next hop which is sending node of the RERR, those routes are made invalid in the process, and that intermediate node propagates the RERR message again. For example, Figure 2-II shows the process of the route maintenance after the link breakage between the node A and the node B. After the route break node A sends RERR message to S.

1) Pros:

(1) An up-to-date path to the destination node because of using destination node sequence number.
(2) AODV reduces excessive memory requirements and the route redundancy.

(3) AODV responses to the link breakage or failure in the network.
(4) AODV can be applied to large scale ad hoc network [5].

2) Cons:

(1) More time is needed for the connection setup & initial communication to establish a route between nodes compared to other approaches.
(2) If intermediate nodes contain old entries it can lead inconsistency in the route mechanism.
(3) For a single route reply packet if there has multiple route reply packets this will lead to heavy control overhead in the network [5].
(4) Because of periodic beaconing in the on-going process it consumes extra bandwidth.

III. OPTIMIZED LINK STATE ROUTING PROTOCOL (OLSR)

The OLSR protocol is a proactive routing protocol which maintains link state information about the whole network. OLSR uses multipoint relaying that is an efficient link state packet forwarding mechanism. OLSR protocol is an optimized version of the link state routing protocol. In optimization process, OLSR decreases the size of the control packets and the number of links. The size of the link state packets is reduced by mentioning only a subset of links in the link state updates. OLSR routing protocol implement the link state strategy; it keeps a routing table that contains information about all possible routes to network nodes. Once the network topology gets changed each node must send its updated information to some selective nodes, which retransmit this information to its other selective nodes in the network [4]. The nodes which are not in the selected list can just read and execute the packet. OLSR protocol may cause network congestion; because of frequent control packets which sent to handle topology changes and moreover OLSR ignore the high resources capabilities of nodes (like transmission range, bandwidth and so on). Therefore, some researchers propose Hierarchical Optimized Link State Routing (HOLSR) protocol as an enhancement of the OLSR protocol, which decreases routing control overhead in the large size networks which also maximizes the routing performance.

OLSR protocol periodically exchanges different messages to maintain the topology information of the entire network in the presence of mobility and failures. The main functionality is performed by using three different types of messages: HELLO, Topology Control (TC) and multiple interface declaration (MID) messages. HELLO messages are exchanged between neighbor nodes. They are employed to accommodate link sensing, neighborhood detection. OLSR is a classical link state routing protocol that relies on employing an efficient periodic flooding of control information using special nodes that act as multipoint relays (MPRs).

Multipoint Relays (MPRs): The idea of multipoint relays is to minimize the overhead of flooding messages in the network by reducing redundant retransmissions in the same area. Each node selects a set of nodes in its symmetric 1-hop neighborhood which may retransmit its messages. This set of selected neighbor nodes is called as the "Multipoint Relay" (MPR) set of that node. In Figure 3 black circles represents the Multipoint Relays. Selection of MPR reduces the number of re-transmissions in the network.

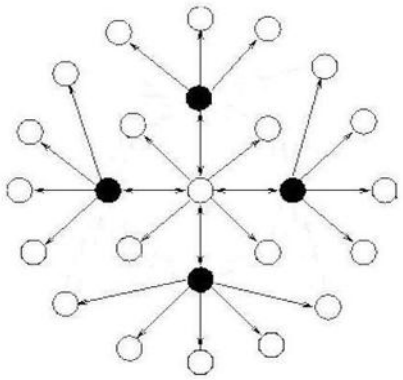

Fig. 3: Packet flooding using MPR

IV. DSR ROUTING PROTOCOL

Dynamic Source Routing (DSR) is a reactive routing protocol as AODV. DSR helps to maintain the source routing in which every neighbor node in DSR maintains the entire network route from source to the destination. DSR protocol aims to provide a highly reactive routing mechanism; by implementing a routing mechanism with an extremely low overhead and rapid reaction to the frequent network changes, to guarantee successful data packet delivery regardless of network changes[5]. DSR is a multi-hop protocol which decreases the network overhead by reducing periodic messages. DSR routing protocol has two main processes: route discovery and route Maintenance. In the route discovery, when a source needs an unavailable route, it initially broadcasts a route request message [6]. All intermediate nodes which received this message from source will rebroadcast it, except if it was the destination node or it has a route to the destination. In the latter case the node will send a route replay message back to the source, later the received route is cashed in the source routing table for future use. If a route is failing, the source node will be informed by a route error (RERR) message. In DSR routing protocol, every data packet contains a complete list of the intermediate nodes; so the source node should delete the failed route from its cache, and if it stores other successful route to that particular destination in its cache, it will exchange the failed one by the other successful route [5]. But if there is no alternative route then it will initiate a new route discovery process .The advantage of DSR protocol is clearly shown in a network with low mobility because it can use the alternative route before starting a new process for route discovery mechanism. In DSR routing protocol, cache route mechanism is used in case of link breakage process. For instance, suppose the source node S has route to the destination node D, and the link <C, D> encountered a failure due to node`s movement. In such case, the source node S looks up in its cache route for another route to destination node D.

The cache route mechanism results in lifting up the data transmission. Upon receiving the RERR message by the source node, the new route discovery procedure will be initiated at that time only.

The RERR message will be originated and sent to the source node by the very first node which is closer to the source node than others. Thereafter, the source node applies

the piggyback strategy based on the RERR message received and the new RREQ message will be broadcasted to all the other nodes used to deploy the failed link. Figure 4 illustrates the transmission of pair of <RREQ, RREP> while executing the route discovery procedure until receiving the reply message.

Dashed lines in the process represent the route stored in cache route memory for further utilization when the link failure happens. The size of the packets in the DSR protocol increases due to adding of any arrived node specifications into packet header. This can be considered as a possible drawback when the number of nodes increases in the scenario. Another issue that must be taken into consideration is being unaware of neighbor list or their link status.

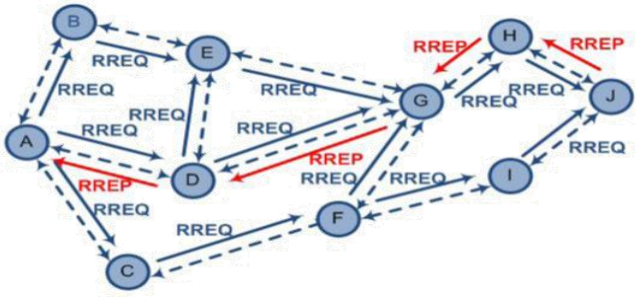

Fig. 4: Route Discovery in DSR

V. Simulation

We have collected simulations results from [10] in which AODV, DSR and OLSR were simulated using QualNet simulator [13] version 5.0.QualNet is a commercial tool and it was released by scalable network technologies in 2000. Qual Net is based on C++ language.

A. *Simulation Scenario:*

Parameter	Value
Simulation run time (sec)	1200
Simulation area (meter square)	1000×1000
Number of mobile nodes	100
Packet generator at each source node	Super-Application
Packet size (bytes)	1024
Number of packets from each source node	5000
Inter arrival time of data packets (millisecond)	100
Velocity model	Random way point
Mobility pause time (sec)	200
Bandwidth (Mbps)	2
Node Communication range (meter)	340
Energy model	MICAZ
Battery model	durcell-mx1500
Path-loss Model	Two Ray
Shadowing Model	Constant
Shadowing Mean (db)	4.0

Table 1: Simulation Parameters

The simulation scenario was also collected from [10]. The simulated ad hoc network scenario was shown in the Table 1. Initially 100 nodes were placed randomly in 1000×1000 meter square area of the network. Random way point model was used for movement of nodes in the network. In this model a node obtains its velocity from [0.3 10] m/s randomly and it selects a random point in the network to move towards it after reaching the selected point the node waits for a duration of time, specified as pause time and again repeats the same process during all the simulation run. To make a realistic scenario two-ray path loss model was used and shadowing model provided with qualnet simulator. Also the simulation parameters were taken from [10].

VI. Results Comparison of AODV with OLSR and DSR

We compare the well-known routing protocols AODV, DSR and OLSR with three parameters.

A. *Average Packet Delivery Ratio:*

This is the ratio of total data packets successfully delivered to destination node and total packets sent by source node in the network. Our aim behind this comparison was to show relative efficiency of routing protocols related to successful delivery of data packets in a dynamic ad hoc network. Figure 4 shows that AODV protocol gives maximum average packet delivery ratio compare to other two routing protocols. The reason behind this is that the AODV protocol uses hop by hop routing and has a better path repair mechanism compare to other routing protocols. The below graph is obtained by simulation results from [10].

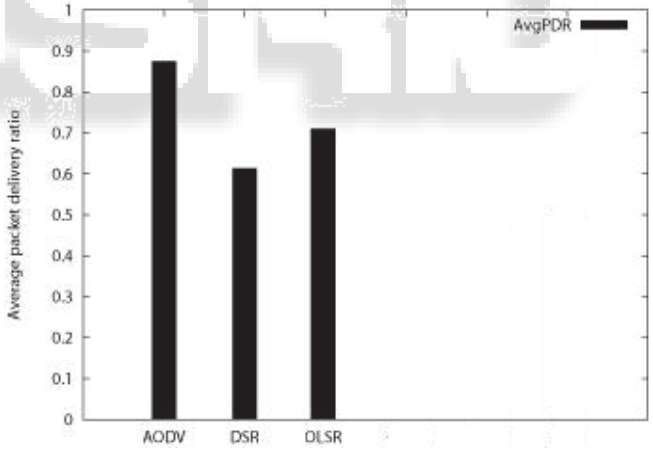

Fig. 5: Average Packet Delivery Ratio of Routing Protocols

B. *Average End-To-End Delay:*

It is define as the calculation of the total time from the source end to the destination end taken by the packet in the network. It covers all of the potential delays such as route discovery, buffering processes, various in-between queuing stays, etc. during the entire journey of transmission of the packet. For this metric, lower the time taken by the packet, more privileged is the routing protocol. This parameter shows packet routing speed of a particular routing protocol. Large end to end delay represents congestion in the network or less efficient routing mechanism of a protocol in the network. A large number of control packets can be charged for congestion in the network. The AODV routing protocol uses hop by hop routing mechanism and maintains shortest path between a source and destination pair. AODV uses

very less control information in a data packet. So due to less control information and short path between nodes, end to end delay is less in case of AODV protocol compares to OLSR and DSR routing protocols. Simulation results in Figure 5 obtained from [10] shows that the AODV protocol has very less end-to-end delay, so it does packet delivery faster than OLSR and DSR routing protocols.

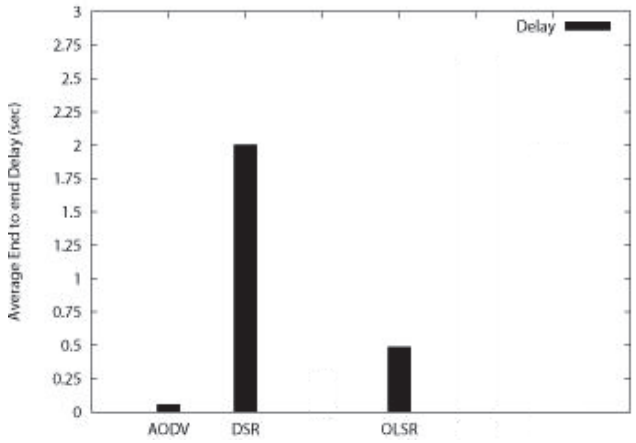

Fig. 6: Average End-to-End Delay (sec) of Routing Protocols

C. Packets Drop Due To Retransmission:

Third parameter is number of dropped data packets due to Retransmission limit exceed. Retransmission limit value 4 has been taken for all the simulated routing protocols. Congestion in the network or path loss of data packets is responsible for the retransmission of the data packets. Network congestion can be due to high rate of control packets of a routing protocol. Packets dropping can be due to path loss if a routing protocol does not have better path recovery mechanism. Simulation results in Figure 6 obtained from [10] shows that AODV routing protocol have very less packet drop compare to DSR and OLSR routing protocols. In AODV, if path gets broken then error message is used by an intermediate node to inform the source node. So in AODV dropped data packets due to retransmission is less compare to other routing protocols.

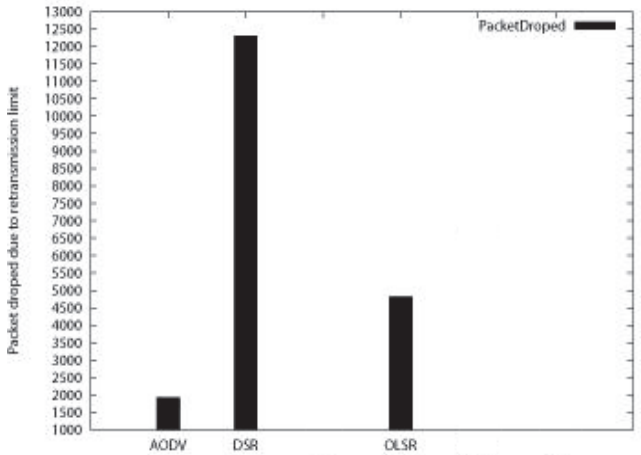

Fig. 7: Average No. of Drop Packets due to Retransmission

VII. Conclusion

Many routing protocols have been proposed for ad hoc networks. A protocol can perform worse or better than other protocols depending upon scenario of ad hoc networks. After reviewing different approaches we can conclude that AODV is better than OLSR and DSR in terms of packet delivery ratio and end-end delay.

Though some improvement needed in AODV routing protocol because the route discovery process on route failure causes a great delay.

References

[1] Marc Emmelmann, Bernd Bochow, C. Christopher Kellum,Vehicular Networking-Automotive Applications and Beyond, Published by John Wiley & Sons Ltd, 2010.

[2] C. E. Perkins and E. M. Royer, Ad hoc On-Demand Distance Vector Routing,, In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, New Orleans, LA,1999.

[3] Himanshu Saini, Rajarshi Mahapatra,Implementation and Performance Analysis of AODV Routing Protocol in VANETs, IJESE 2014.

[4] Jamal Toutouh, José García-Nieto, Enrique Alba, Intelligent OLSR Routing Protocol Optimization for VANETs, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 4, MAY 2012.

[5] Marwa Altayeb, Imad Mahgoub, A Survey of Vehicular Ad hoc Networks Routing Protocols, International Journal of Innovation and Applied Studies,ISSN 2028-9324 Vol. 3 No. 3 July 2013, pp. 829-846.

[6] Elizabeth m . Royer, SANTA BARBARA CHAI-KEONG TOH, A Review of Current Routing Protocols Ad Hoc Mobile Wireless Networks, IEEE Personal Communications, April 1999.

[7] Elizabeth M. Royer, Charles E. Perkins, An Implementation Study of the AODV Routing Protocol , IEEE 2000.

[8] Marc Bechler, Lars Wolf Oliver Storz, Walter J. Franz, Efficient Discovery of Internet Gateways in Future Vehicular Communication Systems, IEEE 2003.

[9] Omid Abedi, Reza Barangi, M. Abdollahi Azgomi, Improving route stability and overhead of the AODV routing protocol and makeing it usable for VANETs , 2009 29th IEEE International Conference on Distributed Computing Systems Workshops.

[10] Naveen Bilandi , Harsh K Verma, Naresh Kumar, Comparative Analysis of Ad Hoc Routing Protocols Based on User's Point of View, IEEE 2012.

