AODV Routing Protocol in VANET – A Survey

Vikram Ghunsar[1] Nisha V. Shah[2]

[1,2]Department of Computer Engineering

[1,2]SVIT, Vasad, Gujarat Technological University

Abstract— Vehicular Ad hoc Network (VANET) is a new way of communication which includes communication between vehicles moving at high speeds on the roads. Vehicular Ad-hoc Network (VANET) is a most critical class of mobile ad-hoc network (MANET) that enables roadside vehicles to intelligently interact with one another and with outside infrastructure anytime anywhere in the global network. In this paper, a new routing protocol for VANET is presented so the work is like that AODV. Aodv is the basically MANET protocol but it has also best performance in the VANET. Aodv protocol has the RREQ, RERR and RREP request in algoritham so in this paper a basically survey that how aodv algoritham work in the VANET scenario.

Key words: AODV protocol, VANET, MANET

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) are Special kind of Mobile Ad Hoc Networks (MANETs) that are formed between moving vehicles on an as-needed basis. VANET is an emerging technology, which enables wide range of applications, including road safety, passenger convenience, infotainment and intelligent transportation [1]. They help to create safer roads by disseminating information regarding the road conditions and traffic scenario among the participating vehicles in a timely manner. Along with the safety applications.

VANETs disseminate valuable, real-time information to the users such as transit systems, weather information, Mobile e-commerce, internet access and other multimedia applications. VANETs enable automated highway applications, where the vehicles are able to cruise without the help of their drivers, even though such applications have not yet become realistic [2].

VANETs inherit some of the characteristics such as mobile nodes and self-organizing behavior from MANETs. However, VANETs possess certain unique characteristics such as high mobility of nodes, time varying density of nodes, frequent disconnections, highly partitioned network and dynamically changing topology, which makes them more challenging.

II. TAXONOMY OF ROUTING IN VANETS

VANETs comprise of radio-enabled vehicles which act as mobile nodes as well as routers for other nodes. In addition to the similarities to ad hoc networks, such as short radio transmission range, self-organization and self-management, and low bandwidth, VANETs can be distinguished from other kinds of ad hoc networks as follows:

A. Highly Dynamic Topology

Due to high speed of movement between vehicles, the topology of VANETs is always changing.

B. Frequently Disconnected Network

Due to the same reason, the connectivity of the VANETs could also be changed frequently. Especially when the vehicle density is low, it has higher probability that the network is disconnected. In some applications, such as ubiquitous Internet access, the problem needs to be solved. However, one possible solution is to pre-deploy several relay nodes or access points along the road to keep the connectivity.

C. Sufficient Energy and Storage

A common characteristic of nodes in VANETs is that nodes have ample energy and computing power (including both storage and processing), since nodes are cars instead of small handheld devices.

D. Geographical Type of Communication

Compared to other networks that use unicast or multicast where the communication end points are defined by ID or group ID, the VANETs often have a new type of communication which addresses geographical areas where packets need to be forwarded (e.g., in safety driving applications).

E. Mobility modelling and predication

Due to highly mobile node movement and dynamic topology, mobility model and predication play an important role in network protocol design for VANETs. Moreover, vehicular nodes are usually constrained by prebuilt highways, roads and streets, so given the speed and the street map, the future position of the vehicle can be predicated.

F. Various communications environments

VANETs are usually operated in two typical communications environments. In highway traffic scenarios, the environment is relatively simple and straightforward (e.g., constrained one-dimensional movement); while in city conditions it becomes much more complex. The streets in a city are often separated by buildings, trees and other obstacles. Therefore, there isn’t always a direct line of communications in the direction of intended data communication.

G. Hard delay constraints

In some VANETs applications, the network does not require high data rates but has hard delay constraints. For example, in an automatic highway system, when brake event happens, the message should be transferred and arrived in a certain time to avoid car crash. In this kind of, instead of average delay, the maximum delay will be crucial.

H. Interaction with on-board sensors

It is assumed that the nodes are equipped with on-board sensors to provide information which can be used to form communication links and for routing purposes. For example, GPS receivers are increasingly becoming common in cars which help to provide location information for routing purposes. It is assumed that the nodes are equipped with on-board sensors to provide information which can be used to form communication links and for routing purposes.

III. AODV ROUTING PROTOCOL AND OPTIMIZATION IN VANET

AODV is a reactive kind of protocol where the route from a source to a destination is created only when it is needed and it keeps these routes as long as they are desirable by the sources. AODV uses sequence numbers to ensure the freshness of routes and uses Hello messages to detect and monitor links to neighbours. Each active node periodically broadcasts a Hello message to all its neighbours. Since the Hello messages are periodically sent, when a node fails to receive several Hello messages from a neighbour, it detects a link failure. Every node of the network maintains a routing table which stores routing information.

Routing tables

Each routing table entry contains the following information [2] as destination, next hop, number of hops, destination sequence number, and active neighbors for this route and expiration time for this route table entry. Expiration time, also called lifetime, is reset each time the route has been used. The new expiration time is the sum of the current time and a parameter called active route timeout. This parameter, also called route caching timeout, is the time after which the route is considered as invalid, and so the nodes not lying on the route determined by RREPs delete their reverse entries.

A. *Control Messages*

1) *Routing Request*

When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ contains the following fields [3]:

Source addres s	Reques t id	Source Sequenc e number	Destin -ation addres s	Destinatio n Sequence number	Hop coun t

Table 1. The RREQ Contain the Following Fields.

The request ID is incremented each time the source node sends a new RREQ, so the pair (source address, request ID) identifies a RREQ uniquely. On receiving a RREQ message each node checks the source address and the request ID. If the node has already received a RREQ with the same pair of parameters, the new RREQ packet will be discarded. Otherwise the RREQ will be either forwarded (broadcast) or replied (unicast) with a RREP message: if the node has no route entry for the destination, or it has one but this is no more an up-to-date.

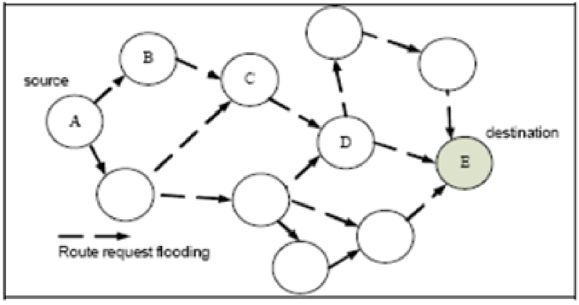

Fig. 1: Route Request (RREQ) flooding route [4],

the RREQ will be rebroadcasted with incremented hop count and if the node has a route with a sequence number greater than or equal to that of RREQ, a RREP message will be generated and sent back to the source. The number of RREQ messages that a node can send per second is limited.

2) *Routing Reply*

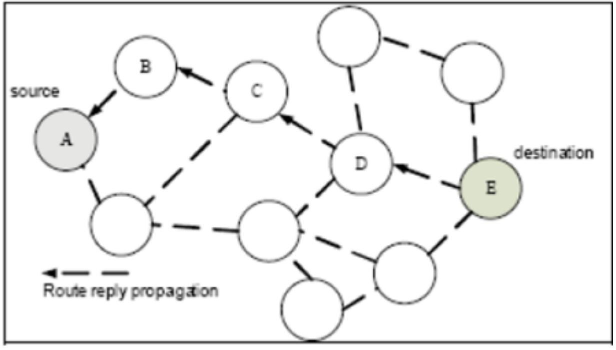

Fig. 2: Route Reply (RREP) propagation[4]

If a node is the destination, or has a valid route to the destination, it unicasts a route reply message (RREP) back to the source. This message has the following format[3]

Source address	Destination address	Destination Sequence number	Hop count	lifetime

Table 2. This message has the following format[3]

3) *Route Error*

All nodes monitor their own neighborhood, when a node in an active route gets lost, a route error message (RERR) is generated to notify the other nodes on both sides of the link of the loss of this link.

4) *HELLO Messages*

Each node can get to know its neighborhood by using local broadcasts, so-called HELLO messages. Nodes neighbors are all the nodes that it can directly communicate with. Although AODV is a reactive protocol it uses these periodic HELLO messages to inform the neighbors that the link is still alive. The HELLO messages will never be forwarded because they are broadcasted with TTL = 1. When a node receives a HELLO message it refreshes the corresponding lifetime of the neighbour information in the routing table. This local connectivity management should be distinguished from general topology management to optimize response time to local changes in the network.

B. *Sequence Numbers*

1) *Counting to Infinity*

The core of the problem is that when X tells Y that it has a path somewhere, Y has no way of knowing whether it itself is on the path. So if Y detects a link to Z is broken, but X still has”valid” path to Z, Y assumes X in fact does have a path to Z. So X and Y will start updating each other in a loop, and the problem named” counting to infinity” arises. AODV avoids this problem by using sequence numbers for every route, so Y can notice that X’s route to Z is an old one and is therefore to be discarded.

2) *Time Stamping*

The sequence numbers are the most important feature of AODV for removing the old and invaluable information from the network. They work as a sort of timestamps and prevent the AODV protocol from the loop problem (see

Appendix). The destination sequence number for each destination host is stored in the routing table, and is updated in the routing table when the host receives the message with a greater sequence number. The host can change its own destination sequence number if it offers a new route to itself, or if some route expires or breaks.

3) *Route Discovery*

Route discovery process starts when a source node does not have routing information for a node to be communicated with. Route discovery is initiated by broadcasting a RREQ message. The route is established when a RREP message is received. A source node may receive multiple RREP messages with different routes. It then updates its routing entries if and only if the RREP has a greater sequence number, i.e. fresh information.

4) *Reverse Path Setup*

While transmitting RREQ messages through the network each node notes the reverse path to the source. When the destination node is found the RREP message will travel along this path, so no more broadcasts will be needed. For this purpose, the node on receiving RREQ packet from a neighbor records the address of this neighbor.

5) *Forward Path Setup*

When a broadcast RREQ packet arrives at a node having a route to the destination, the reverse path will be used for sending a RREP message. While transmitting this RREP message the forward path is setting up. One can say that this forward path is reverse to the reverse path. As soon as the forward path is built the data transmission can be started. Data packets waiting to be transmitted are buffered locally and transmitted in a FIFO-queue when a route is set up. After a RREP was forwarded by a node, it can receive another RREP. This new RREP will be either discarded or forwarded, depending on its destination sequence number: if the new RREP has a greater destination sequence number, then the route should be updated, and RREP is forwarded, if the destination sequence numbers in old and new RREPs are the same, but the new RREP has a smaller hop count, this new RREP should be preferred and forwarded, and, otherwise all later arriving RREPs will be discarded.

6) *Optimal TTL Sequence*

Expanding ring search strategies for AODV were recently extensively studied, and different schemes were proposed. In a RREQ is initiated with a small TTL value, followed by RREQs with incremented TTL values until a certain threshold is reached. Then, if no route is found, a RREQ is flooded across the whole network

7) *Link Breakage*

Because nodes can move link breakages can occur. If a node does not receive a HELLO message from one of his neighbors for specific amount of time called HELLO interval, then the entry for that neighbor in the table will be set as invalid and the RERR message will be generated to inform other nodes of this link breakage RRER messages inform all sources using a link when a failure occurs.

IV. Related Work

AODV protocol in which the active route is maintained by locally updating active route information to 1-hop neighbors, multiple backup routes are built .in this survey paper how adov can use decrease the route time and make fast algoritham for vanet is done.This process is done in the two step.

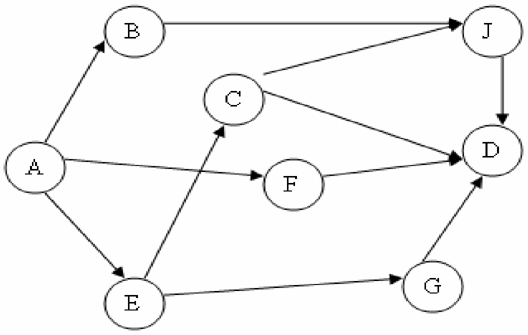

Fig. 3. Overhead routes [3]

A. *Restricting Route Request Packets*

First way to restrict routes is restricting of RREQ packets. Therefore, we reduce number of routes by limiting number of discovered routes based on a route boundary. For this, if a node is source node, it will generate and send RREQ packet. Otherwise, if node receives RREQ packet and wants to broadcast it to its neighbors, it is not allowed to send RREQ packets to all neighbors and it can only send RREQ packets to its neighbors until number of selected neighbors are less than or equal to route boundary.

B. *Restricting Routes Based On Distance*

Another way for restricting routes is restricting neighbors based on distance. In this strategy neighbor of nodes are not similar. Restricting based on distance has some advantages such as reducing number of hops and finding short routes between any source and destination. In addition, broken links along a route will be reduced. Transmission range of node A is R and threshold distance is R1. Therefore, overhead zone is the zone around node A with radius R1 and prior zone is the zone

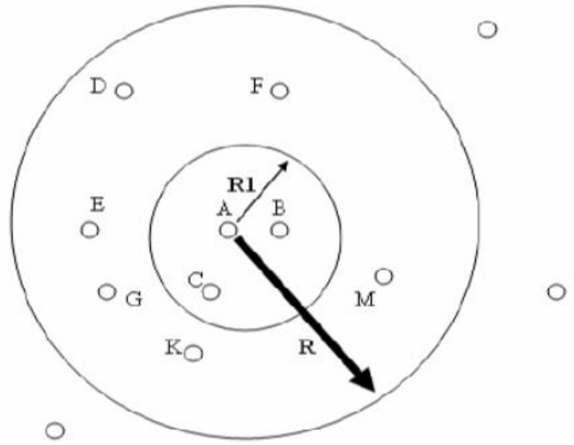

Fig. 4: Prior and overhead neighbors[3]

between overhead zone and transmission range of node A. Overhead neighbors of node A are B and C and prior neighbors of node A are D, E, F, G, K and M.

Suppose that node A wants a route to another node,first it must broadcast RREQ packets to its neighbors. B is also a neighbor of A but, as mentioned before, B is overhead neighbor of A and as depicted in figure, neighbors of A and B are identical. Therefore, B also broadcasts RREQ packets to its neighbors, which had received RREQ packet from A. so, sending RREQ packet to node B only increases routing overheads.

ACKNOWLEDGMENT

I am very grateful and would like to thank my guide and teacher Prof. Nisha V. Shah (HOD) for her advice and continued support without which it would not have done it and the entire Information Technology Department, faculty and staff, for helping me in every possible manner during my course of study for this subject.

V. CONCLUSION

VANET routing is very difficult compare to the MANET. AODV is basically algoritham of the MANET but it gives the better performance than the other algoritham,the final conclusion is that by clustering and grouping the VANET we can get better result throught the AODV.

REFERENCES

[1] Venkatesh, Indra. A and Murali. R, “Vehicular Ad hoc Networks (VANETs): Issues and Applications”, Journal of Analysis and computation, Vol. 8, No. 1, 2012, pp.31-46.

[2] Andrei Furda et al, “Enabling Safe autonomous driving in real-world city traffic using multiple criteria decision making”, IEEE Intelligent Transportation System Magazine, SPRING 2011, pp. 4-17.

[3] 2009 29th IEEE Omid Abedi “ Improving route stability and overhead of the AODV routing protocol and making” it usable for VANETs

[4] Ian D. Chakeres, Elizabeth M. Belding-Royer AODV Routing Protocol Implementation Design.

[5] Y. Saleh, et al., "Vehicular ad hoc networks (VANETs): Challenges and perspectives", in Proc. 6th Int. Conf. on ITS Telecommunication 2006, pp. 761-766.

[6] Fan Li and Yu Wang, “Routing in Vehicular Ad hoc Networks: A Survey”, IEEE Vehicular Technology Magazine,Vol. 2 June 2007, pp. 12-22.

[7] Hasnaa Moustafa, et al, “Adaptive Path Energy Conserving Routing in MANETs”, Ad Hoc and Sensor Wireless Networks, Similar Publications 2005.

[8] Ajay Guleria, et al, “Request Analysis and Dynamic Queuing System for VANETs”, International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.

[9] Qing Yang, “Connectivity Aware Routing in Vehicular Networks”, IEEE Communications and networking conference, April 2008

[10] Hannes Hartenstein, Kenneth P. Laberteaux, “A Tutorial Survey on Vehicular Ad Hoc Networks”, IEEE Communications Magazine, June 2008

[11] Kevin C Lee, Uichin Lee, Mario Gerla, “Survey of routing protocols in vehicular Ad hoc networks”, Advance in Vehicular Ad-hoc networks: Development and Challenges

[12] Gerla M, Hong X, and Pei G, “Routing Protocols in Wireless Ad Hoc Networks–A Simulation Study”, Lulea University of Technology Stockholm 1998.

[13] Yun-Wei Lin et al, “Routing Protocols in Vehicular ad hoc networks: A survey and future perspectives”, Journal of information Science and engineering, 2010, pp.913-932.

[14] Bernsen J and Manivannan D, “Unicast Routing Protocols for Vehicular Ad hoc Networks: A Critical Comparison and Classification “,

[15] S. Jaap, et al., "Evaluation of routing protocols for vehicular ad hoc networks in city traffic scenarios," in Proc. 5th Int. Conf. On Intell. Transprtn. Systems Telecommun. (ITST), Brest, France, June, 2005.