International Journal of Networking
ISSN: 2249-278X & E-ISSN: 2249-2798, Volume 2, Issue 1, 2012, pp.-55-59.
Available online at http://www.bioinfo.in/contents.php?id=108

OPTIMIZED AODV ROUTING PROTOCOL FOR VEHICULAR AD HOC NETWORKS

GULHANE S.P., JOSHI A.A. AND CHAVAN K.L.

Department of Electronics & Telecommunication, Final Year, J.D.I.E.T., Yavatmal, India
*Corresponding Author: Email- sanketgulhane@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- A Vehicular Ad-hoc Network (VANET)[4] is a type of Mobile Ad-hoc Network (MANET) that is used to provide communications between nearby vehicles, and between vehicles and fixed infrastructure on the roadside. Though VANET[4] is a type of MANET but the routing protocols of MANET are not feasible with VANET[4] and if they are even feasible then they are not able to provide the optimum throughput required for a fast changing vehicular ad-hoc network. The difference between VANET[4] and MANET is that in VANET[4], the nodes are moving on predefined roads, and node in the network is very fastly movable and this is where the routing protocols have to be modified or changed.The paper presents the Vehicular Ad hoc Networks and the typical routing protocol: the ad hoc on-demand routing protocol (AODV) [5]in mobile ad hoc networks and the optimized protocol AODV_OBD for protocol AODV[6].
Keywords- Vehicular ad hoc networks, Mobility model, AODV, Broadcasting data packet.

Citation: Gulhane S.P., Joshi A.A. and Chavan K.L. (2012) Optimized AODV Routing Protocol for Vehicular Ad hoc Networks. International Journal of Networking, ISSN: 2249-278X & E-ISSN: 2249-2798, Volume 2, Issue 1, pp.-55-59.

Copyright: Copyright©2012 Gulhane S.P., et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Introduction

As a special example of Mobile Ad hoc Networks (MANET), Vehicular Ad hoc Networks (VANET) not only has general characteristics of MANET, but also has many special aspects[2]. Ad hoc Networks is a wireless communication network which comprises a set of mobile nodes with wireless transceiving equipments. It does not rely on preinfrastructure to form temporary networks in which mobile nodes make use of their own transceiving equipments to exchange information so that nodes in networks can share information. When the mutual communication is not in the scope of their own, it can make use of other intermediate nodes to achieve the multi-hop communication. So Ad hoc Networks is a wireless, distributed, multi-hop, self-organization, no-center, mobile networks[3]. Various vehicles in VANET are the mobile nodes in MANET. But some problems for example fast moving nodes, frequent topology change etc. makes a number of technologies (including routing) in MANET difficult to transplant into VANET. Then it is essential to improve technologies in MANET to meet the needs of VANET[4]. Because of fast moving nodes , frequent topology change and slow convergence of routing protocols, a lot of control packets exist on the links to occupy bandwidth; data packets will wait more time for not finding a suitable route, which increases delay and lowers packet delivery rate. When moving speed of nodes and topology changes reach a certain level, the general routing protocols will lose their roles, while flooding can achieve the purpose of passing data packets. For characteristics of mobile nodes in VANET, an improved protocol (AODV_OBD) is proposed to reduce the packet delay.

Routing Protocols

The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. A MANET protocol should function effectively over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks. As fig 1 shows the categorization of these routing protocols.

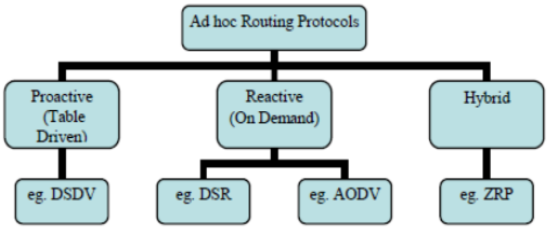


Fig. 1- Hierarchy of Routing Protocols

Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV)[8]. Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR)[7] and Ad Hoc On-Demand Distance Vector (AODV)[6]. Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

Proactive Routing Protocol

In a network utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. On the other hand, routes will always be available on request. Many proactive protocols stem from conventional link state routing, including the Optimized Link State Routing protocol (OLSR).

Reactive Routing Protocol

Reactive routing protocols are on-demand protocols. These protocols do not attempt to maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network. The primary advantage of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be used. While reactive protocols do not have the fixed overhead required by maintaining continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

Hybrid Routing Protocol

Wireless hybrid routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside a group. Both routing table size and update packet size are reduced by including in them only part of the network (instead of the whole); thus, control overhead is reduced. The most popular way of building hierarchy is to group nodes geographically close to each other into explicit clusters. Each cluster has a leading node (cluster head) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be achieved through this flexibility. Since mobile nodes have only a single omnidirectional radio for wireless communications, this type of hierarchical organization will be referred to as logical hierarchy to distinguish it from the physically hierarchical network structure.

Aodv Routing Protocol and Optimization

On-demand routing protocols[5] are also known as reactive routing protocol. In the ad hoc networks where bandwidth resources are limited and topology frequently changes, it is not necessary to maintain routes to each node. Fast-changing topology shortens effective time of routing and reduces utilization rate of routing information. Therefore, on-demand routing protocols came into being. On-demand routing protocols have two processes including Route Discovery and Route Maintenance. When the source node where there is no routing in the routing table needs to obtain the routing to destination node, the route discovery process will be activated. The node broadcasts routing request packets across the network by flooding. When a route request packet reaches the destination node, the destination node will send a route response packet to the source node. Thus, the two-way activated path will be set up between the source node and the destination node. As the topology changes, the route maintenance process is started when certain link on the activated path breaks [1].

AODV Routing Protocol

AODV is a relative of the Bellmann-Ford distant vector algorithm, but is adapted to work in a mobile environment. AODV determines a route to a destination only when a node wants to send a packet to that destination. Routes are maintained as long as they are needed by the source. Sequence numbers ensure the freshness of routes and guarantee the loop-free routing [5].

Routing tables

Each routing table entry contains the following information:

- Destination
- Next hop
- Number of hops
- Destination sequence number
- Active neighbours for this route
- 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. If active route timeout is big enough route repairs will maintain routes. RFC 3561 defines it to 3 seconds.

Control messages

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

source address	request ID	source sequence No.	destination address	destination sequence No.	hop count

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 route, the RREQ will be rebroadcasted with incremented hop count.

•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. There is an optimization of AODV using an expanding ring (ESR) technique when flooding RREQ messages . Every RREQ carries a time to live (TTL) value that specifies the number of times this message should be re-broadcasted. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Historically such floodings used a TTL large enough - larger than the diameter of the network - to reach all nodes in the network, and so to guarantee successful route discovery in only one round of flooding. However, this low delay time approach causes high overhead and unnecessary broadcast messages. Later, it was shown that the minimal cost flooding search problem can be solved via a sequence of floodings with an optimally chosen set of TTLs.

Routing reply

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.

source address	destination address	destination sequence No.	hop count	life-time

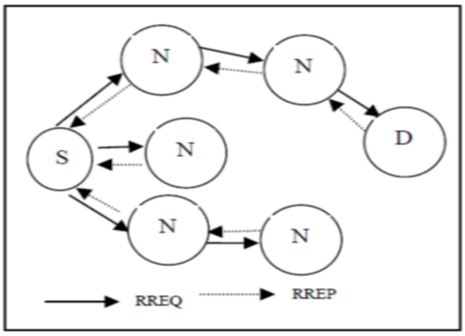
The reason one can unicast RREP back is that every node forwarding a RREQ message caches a route back to the source node .

Route error

All nodes monitor their own neighbourhood. 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.

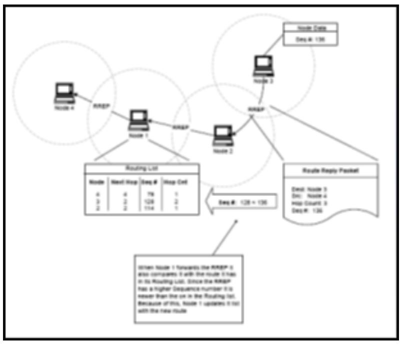
HELLO messages

Each node can get to know its neighbourhood by using local broadcasts, so-called HELLO messages. Nodes neighbours 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 neighbours 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.



Sequence numbers

Sequence numbers serve as time stamps. They allow nodes to compare how "fresh" their information on other nodes is. Every time a node sends out any type of message it increase its own Sequence number. Each node records the Sequence number of all the other nodes it talks to. A higher Sequence numbers signifies a fresher route. This it is possible for other nodes to figure out which one has more accurate information. In the example, Node 1 is forwarding a RREP to Node 4. It notices that the route in the RREP has a better Sequence number than the route in it's Routing List. Node 1 then replaces the route it currently has with the route in the Route Reply.



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 update its routing entries if and only if the RREP has a greater sequence number, i.e. fresh information.

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 neighbour records the address of this neighbour.

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

•Otherwise all later arriving RREPs will be discarded

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. I tried to find the optimal initial TTL value, TTL step, and the TTL threshold value. They found that the use of initial and step TTL values greater than 1 results in reducing overhead and delay time. They found also that initial as well as step values depend of the network topology, but the threshold value does not. Furthermore, other strategies were proposed to make the route discovery more efficient, e.g. using the history of hop-distance to decide which initial TTL value should be chosen.

Link breakage

Because nodes can move link breakages can occurs. If a node does not receive a HELLO message from one of his neighbours for specific amount of time called HELLO interval, then

•the entry for that neighbour in the table will be set as invalid

•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.

Optimized Routing Protocol[1]

From the above analysis we can see, when the link breaks, local repair reestablishes the routing to the destination node by sending a routing request packet and a routing reply packet, and at the same time the data packets have been cached. The sending of data packets after the routing to the destination node being set up not only increases delay, but also leads to invalid routing because of the change of a newly created routing topology. AODV_OBD[1] establishes a routing to the destination node by broadcasting data packets when local repair is going on. That is to say data packets broadcasted is not only the request packets, but also the data packets. When the node detects the link interrupted, it will broadcast a packet which has an increase of packet header rather than send a RREQ. The packet header which is similar to the packet header of RREQ packet has the function of establishing the reverse routing and finding the routing. When the data packets reach the intermediate nodes instead of the destination node, they will record the reverse routing and then re-broadcast this data packets; when the data packets reach the destination node, it will send a RREP and at the same time receive the data packets. This will not only set up the routing but also reduce the delay. And in the paper the hop count of the RREQ is limited, so when the RREQ can not find the destination node, it can only go through very small hop count. This is implemented by setting a parameter to point out the hop count. When the RREQ reach a node, the hop count decreases if the node is not the destination node. What's more, there is a new method is used by replying a reply packet which can tell the node that the next node can be active. When the next node is the node that the data packet or the RREQ wants to arrive, it reply a RREP and if not, the node cannot reply the RREP. According to whether the node get a RREP, the node takes measures accordingly.

Conclusion

In this paper, we have studied AODV routing protocol which belongs to on-demand routing protocols as well as its improved protocol AODV_OBD[1], and analyzed the packet delivery rate and packet delay. The analyzed results showed that the delay of AODV protocol is larger than that of AODV_OBD protocol. In summary, AODV_OBD protocol reduces the packet delay to some extent and reaches the expected purpose. However, because there is no full consideration of packet delivery rate, the packet delivery rate curve of AODV_OBD protocol is not ideal.

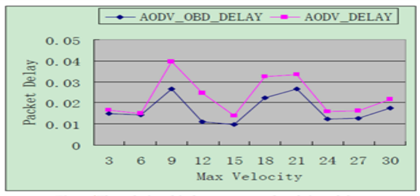


Fig. 4 The relationship between speed and time delay.

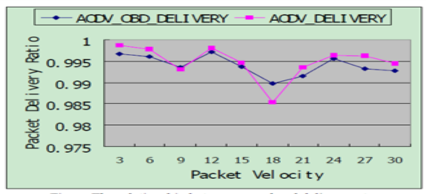


Fig. 5 The relationship between speed and delivery rate.

References

[1] Baozhu Li, Yue Liu and Guoxin Chu (2010) *IEEE.*

[2] Cuyu Chang, Yong Xiang and Meilin Shi (2007) *Journal on Communications*, 28, 116-126.

[3] Charles E Perkins and Elizabeth M Royer (1999) *The 2th IEEE Workshop on Mobile Systems and Application*, 90-100.

[4] Deng H., Li W. and Agrawal D.P. (2002) *IEEE Communications Magazine*, 40(10), 70-75.

[5] Imrich Chlamtac, Marco Conti, Jennifer J.N. Liu (2003) *Mobile ad hoc networking: imperatives and challenges*.

[6] Murthy S. and Garcia-Luna_Aceves J.J. (1996) *ACM Mobile Networks and Applications Journal*, 1, 183-197.

[7] Perkins C.E. (2001) *Ad hoc Networking*.

[8] Ruiqin Zhao, Jungang Yang and Zengji Liu (2007) *Computer Science*, 34, 55-62.

[9] Shunliang Zhang, Chengqing Ye and Fangmin Li (2003) *Computer Science*, 30, 27-30.

[10] *http://vanet.eurecom.fr*.

[11] Xi Sun and Xiamiao Li (2008) *Journal of Shanxi University of Science & Technology (Natural Science edition)*, 26, 107- 109.