A survey on routing protocol and gateway discovery in Vehicular Adhoc NETwork(VANET)

Thamarai selvi SB **Gokulakrishnan P**
Computer science and engineering PSNA College of Engineering and Technology Dindigul,India

Abstract
Vehicular Adhoc NETwork is the subcategory of MANET which has vehicle to vehicle and vehicle to infrastructure communication environment.VANET enable vehicle to communicate with each other but it require an efficient and robust routing protocol for their success. Several gateway selection schemes have been selected the gateway nodes based on some parameters. To improve the network performance, it is essential to select the routing protocol. In this paper, the survey of gateway discovery, gateway selection and comparison of algorithm to choose the routing protocol has been discussed.

Keywords
VANET, Gateway discovery, parameter, Routing protocol

1. Introduction

Vehicular Adhoc NETworks are emerging novel technology to integrate the capabilities of new generation wireless networks to vehicles. The two main type of communication in vanet are vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communication. Communication in V2V and V2I are adhoc in nature. Gateway is the infrastructure for communication between the vehicles for sharing and information from various vehicle. Proactive Gateway is the Gateway that broadcasts a Gateway Advertisement message after each interval. Vehicular nodes in the gateway's transmission range receive the advertisement and those without the route to the gateway, builds a route entry for it in their routing tables. Reactive Gateway is the gateway by performing expanding ring search, the node ready to communicate with the network will contact it within the ad hoc network. A new route is determine towards the Internet, when there is no reply after the search. Hybrid Gateway is the gateway that TTL-limited messages are flooded by the gateways which will be sending only up to few hops away from the gateway. Proactive approach has been accomplish by the sources within its area and outside that it acts as reactive.

II Communication environment

a.Vehicle to Vehicle:

The inter-vehicle communication layout (Fig. 1) uses multi-hop multicast or broadcast to transmit traffic related information over multiple hops to a group of receivers. Vehicles need only be concerned with activity on the road ahead and not behind. There are two types of message forwarding in inter vehicle communications: naive broadcasting and intelligent broadcasting. In naive broadcasting, vehicles forwards broadcast messages periodically and at regular intervals. The vehicle avoids the message if it has come from a vehicle behind it. If the message comes from a vehicle in front, the receiving vehicle forward its own broadcast message to vehicles behind it. This ensures that all enabled vehicles moving in the forward direction get all broadcast messages.

Fig. 1Vehivle-Vehicle communication

The obstacle of the naive broadcasting method is that large numbers of broadcast messages are generated, therefore, hike the risk of message collision resulting in lower message delivery rates and increased delivery times. Intelligent broadcasting with indirect acknowledgement addresses the problems inherent in naive broadcasting by limiting the number of messages broadcast for a provided event. If the event-detecting vehicle receives the same message from beyond, it presumes that at least one vehicle in the back has received it and ceases broadcasting.

b.Vehicle to infrastructure communication:

Manuscript received November 5, 2016
Manuscript revised November 20, 2016

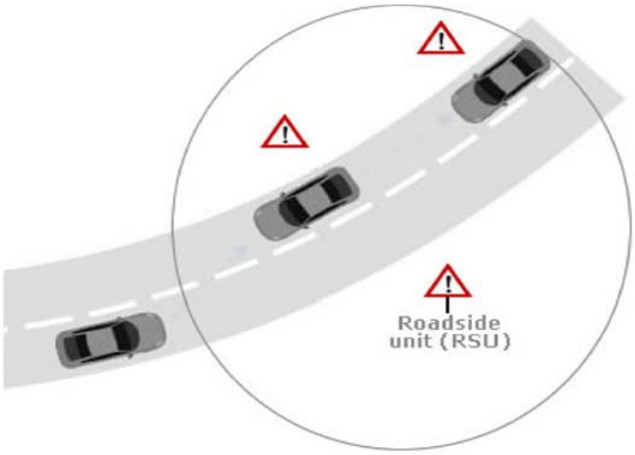

Fig. 2 Vehicle-to-Infrastructure communication

Vehicle to Infrastructure given solution to longer-range vehicular networks. It makes use of preexisting network infrastructure such as wireless access points (gateway or RSUs). Communications between vehicles and gateway are supported by Vehicle to Infrastructure (V2I) protocol. The Road side infrastructure involves additional installation costs.

III Gateway Discovery:

The gateway discovery can be classified into three major catagories. They are

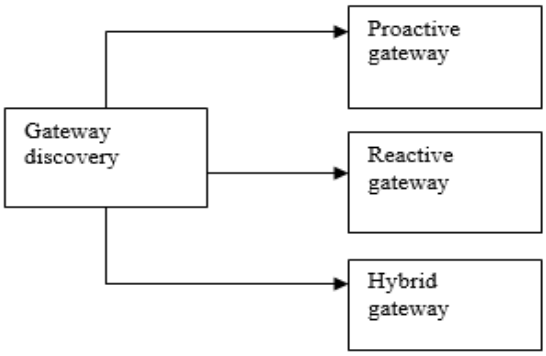

Fig 3: Gateway discovery classification

Proactive gateway discovery
Gateways are periodically broadcasts its advertisement message With TTL and request ID. Client Vehicle sends a Request to Connect message to its related gateway according to previously received advertisement. Gateway replies either a positive or a negative response by sending a Response to Connect message. The connection from the client vehicle through the gateway is thus built.

Reactive gateway discovery
The client vehicle broadcasts a Solicitation message. The gateway receiving the Solicitation message sends back to its own Advertisement message to the client vehicle which is requested. The client vehicle sends a Request to Connect message to the gateway based on the received advertisement. Gateway replies either a positive or a negative response by sending a Response to Connect message. The connection from the client vehicle through the gateway is to built.

Hybrid gateway
Hybrid gateway discovery is the merging of proactive and reactive approaches. In hybrid gateway approach the gateway broadcasts the advertisement message in regular interval. The TTL is set to advertisement zone so that the advertisement message could be forward upto this minimum number of hops through the ad hoc network. The nodes within this receive this message and set based upon the proactive approach. The node outside this region discovers the default routes to the gateways using the reactive approach.

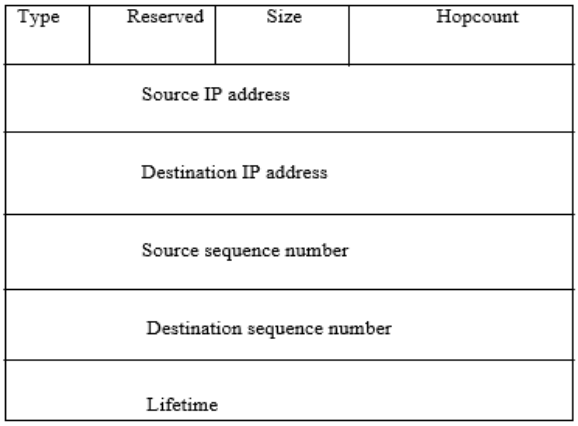

Fig 4: Gateway discovery framework

IV Parameters for Gateway Selection:

Hop count parameter:
Hop count is an essential metric.VANET routing protocol used this metric for routing in multi hop communication for gateway selection. However, the gateway can become a bottleneck when the traffic load is heavy there is a probability of increasing route error because of the intermediate nodes mobility while the gateway selection does not considering.the following figure shows the bottleneck node.the bottleneck node is defined as that it does not able to continue its progress with their neighbour node. The advantage of hop count is that it can reach its destination by using multi hop when the path is not available.

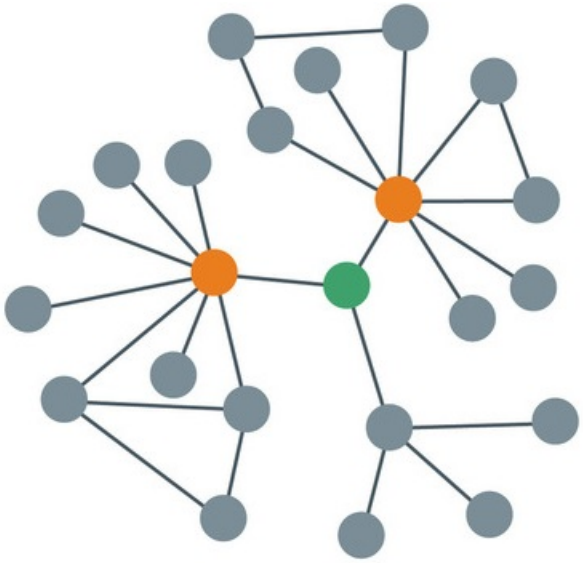

Fig .: bottleneck node

Mobility parameter:
The mobility metric states the speed of each node in the path to the GW. The too fast node can cause topology change that need to reselect the path which will increasing the routing overhead increase the routing overhead. A gateway selection scheme which uses the Tracing-Value as a basic metric to select the gateway.
The Tracing Value value increases if a neighboring node does not receive a broadcasting message before its duration expires. So, the larger value of tracing value means the higher probability of link failure. Therefore, the gateway node on a path with the minimum tracing value is selected.This procedure consumes higher processing power than the hop count. However, considering the speed of the nodes adds additional cost to the selection method which will affect the network's performance.

Qos:

1. Bandwidth:
The total number of information that can be transmitted over a network in a given amount of time.it is usually expressed in bits/sec.

2. Jitter:
The jitter provides the variation in latency

3. Loss:
It shows the percentage of lost data

4. Low throughput:
Network throughput is the rate of successful message delivery over a communication channel.The bit rate that can be provided to a fixed data stream may be too low for real time services if all data streams get the same scheduling priority.

5. Dropped packet:
The routers may fails to deliver some packets if their data is erroneous or they arrive when their buffers are already full.

Maximum Normalized Capacity (MNC):
The Maximum Normalized Capacity is known that the cost of the path represents the amount of wireless network resources consumed by sending a packet. Therefore, each router should select a gateway in so as to limit the hike in path lengths compared with their classical shortest path routing.

Load degree: the number of nodes, which are communicating with this candidate gateway.
Residual energy: the node available energy, supposing that the node may pick up its own residual energy information directly.
Movement rate: the absolute value of nodes movement speed, which is also picked up by the node itself.

V. Routing In VANET:

DSR:
The DSR protocol is consist of two main mechanisms that work together to allow the discovery and maintenance of source routes in the adhoc network:
Route discovery is the mechanism by which a node Src wishing to send a packet to a destination node Dest obtains a source route to D.Route Discovery is used only when S attempts to send a packet to Dest and does not already know a route to Dest.
Route Maintenance is the mechanism by which node Src is able to detect, while using a source route to Dest, if the network topology has changed such that it can no longer use its route to Dest because a link along the route no longer works. When Route Maintenance indicates a source route is broken, Src can attempt to use any other route it happens to know to Dest, or it can invoke Route Discovery again to find a new route for subsequent packets to Dest. Route Maintenance for this route is used only when S is actually sending packets to Dest.

AODV:
The Ad hoc On Demand Distance Vector (AODV) is the routing protocol which is intended for use by nodes in an ad hoc network. It offers quick modification to dynamic link conditions, low processing and memory overhead, low network utilization, and found uni cast routes to sink within the ad hoc network. It uses destination sequence

numbers to ensure loop freedom at all times avoiding problem.
Route request, route reply and route errors are the message types defined by ADOV. these types received via UDP and IP header. It offers quick adaptation to dynamic link condition, low processing, memory overhead, low network utilization and determine unicast destination route.

Destination sequenced distance vector (DSDV):
The Destination sequenced distance vector is the table driven routing protocol. The route is maintained through the routing table. This routing table contains the information about all the nodes in the network i.e. nodes present in network, next node to each sink, metric and the sequence number. The route taken the judgement through the sequence number and metric used in the table. Only the table with very recently updated or modified sequence number is used. This table is updated by a regular interval or when the change in table has happened. The updation of the routing table for regular interval of time makes the utilization of the battery power whether the network remains ideal or populated.

VI. Routing Algorithm:

Gateway migration algorithm (GMA):
The GMA along with the propagation mechanism of QOS parameters during the gateway discovery process. Analyze gateway selection scheme based on QoS in the gateway migration algorithm, where each node periodically advertises its parameters within a reactive region. Some of the advantages of the gateway migration algorithm is to Improve qos, Improve network throughput, Increase the packet delivery ratio.
ABR Algorithm:
ABR algorithm is a compromise between broadcast and point to point routing, connection-oriented packet forwarding mechanism.

SSR Algorithm:
SSR algorithm is the logical offspring ABR algorithm. Routing nodes along the path is based on signal strength and location stability.
TORA Algorithm:
TORA is a link reversal algorithm which is proper for high density node networks. One advantage of TORA is to maintain multiple routes, that can be a source / destination multiple routes to improve. Advantages of the above algorithm is that it can improve the quality of communication over the network it is used to select feasible path.
Table driven routing algorithm:
Table-driven routing will be used in any case of the path is constantly using each other to share information between nodes to maintain routing table.

Table 1: Comparison of table driven and source driven routing

	SOURCE DRIVEN	TABLE DRIVEN
Routing Protocol	Dsdv	Aodv,Ssr,Dsr,Tora
Delay	Low	High
Load	High	Low
Power Consumption	High	Low
Bandwidth Cost	High	Low

Table 2: Routing protocol comparison

	ADOV	DSR	SSR	ABR	TORA
Complexity	Medium	Medium	High	High	High
Multipath support	No	Yes	No	No	Yes
Path	Latest shortest path	Shortest path	Shortest path	Shortest path	Shortest path
Loop freedom	Yes	Yes	Yes	Yes	Yes

The above table discuss that the comparison of routing protocol.

VII. ANALYSIS:

1. BCRPV:
Most of the routing protocols have been proposed to determine routes between vehicles and gateways. However, most of these protocols do not use the bandwidth which is a insufficient resource in VANETS. In this paper, Amadou adama ba, abdelhakim hafid, jawad drissi proposed a routing protocol to connect vehicles to Internet through mobile gateways with the objective to make optimized use of the network bandwidth. Indeed, the protocol significantly reduce the communication overhead required to create and maintain the routes relying on the mobility of the gateways. PBR establishes routes preemptively before existing ones rupture using predicted lifetimes of the routes. The basic idea behind PBR is to preempt route failures and made the most of connection existing leading to a smaller network downtime. BCRPV connects vehicles to Internet via gateways using predicted lifetimes of routes [10].

2. EAP
Amit Kumar Gupta, Naveen Kumar Gupta, Rakesh Kumar proposed that the path established with the RSU is secure as the path may includes quite a few malicious nodes or even congested nodes that may drop the packets it receives without forwarding. To overcome the situation and offered a host-to-host security, it is important to select a trusted secure gateway and authenticate it, which can be reached via trusted and traffic less route and trusted node. An efficient secure gateway selection and authentication scheme in MANET has been designed. This scheme

provides secure gateway discovery and efficient trusted route through which secure data are transferred. A secure GW selection scheme that is aimed at selecting the secure efficient GW candidate node that could be reached via secure, trusted and uncongested path and thereafter, provide a host-to-host security in the integrated network.Protocol used here is Extensible Authentication Protocol (EAP).The EAP contain an authentication server that validates the node information[3].

3. MRBDAS

A MANET accessing routing algorithm for internet, based on dynamic gateway adaptive selection. The algorithm employs the methods of multi paths and query localization technique based on old path information to maintain routing adaptively. To provide a better performance of MANET accessing Internet, it is a key problem to select suitable gateways. In MRBDAS, the destination node answers for selecting dynamic gateways, so its behavior will affect accessing performance of entire network [7].

4. DYMO

Rajesh Gargi yogesh chaba R.B.patel proposed a hybrid Mobile Ad Hoc Network (MANET) is provided by gateways (GWs), which connect the MANET to the Internet. Hybrid MANETs are weak to more security threats while routing through the gateways. Gateway is classified into two classified into public gateway and protected gateway. Protected gateway can route both public and protected data. On the contrary, public gateway can just route public data. Among multiple gateways, a gateway is elected using multi criteria gateway selection strategy. Transmission of public data through prGW does not require any authentication but transmission of protected data through prGW requires authentication phase. Authentication of prGW with mobile nodes is performed using pre-authentication and utility function. For performing the authentication process, each prGW employs Extensible Authentication Protocol (EAP). The used Protocol is DYMO.DYMO can work as both proactive and reactive routing protocol [11].

5. ECDSA

S.Biswas et al have proposed a safety message authentication scheme for vehicular ad hoc networks using an ID based technique offers a certificate low public key verification while a proxy signature provide flexibility in authenticated message and trust management. In this scheme ID based proxy signature framework with the standard ECDSA for VANET's gateway originated safety application message is incorporated.An ID-based signature allows a verifier to use a publicly well known piece information about the signer for the verification of the digital signature.Based on the context,the public information could be an actual identity of the signer.This scheme has an advantage of ECDSA employs a relatively short encryption key[2].

6. ABAKA

J.L.Huang, et al had proposed a anonymous batch authenticated and key agreement (ABAKA) scheme to authenticate multiple request sent from different vehicles and establish different session key for different key at the same time. ABAKA can efficiently authenticate multiple request by one verification operation and negotiate a session key with each vehicle by one broadcast message. The advantage of the ABAKA system is the message delay and message loss rate are less than that of the existing elliptical curve digital signature algorithm based scheme. It also lowers verification delay and transmission overhead [4].

VIII Conclusion:

Routing is one of the most important parameter in vehicle to vehicle communication (V2V) and vehicles to infrastructure communications (V2I). Thus this survey has presented an overview about the various routing protocols of VANET.The paper also characterizes the advantages and limitations of the protocols by comparing the different parameters and also about the gateway discovery and selection of gateway.

References:

[1] Liu Jie, "Ad Hoc Access Gateway Selection Algorithm",2012 International Conference on Solid State Devices and Materials Science

[2] J.L.Huang , "Routing in Vehicular Ad HocNetworks: Survey" Fan University of North Carolina at Charlotte, ieee vehicular technology june 2007.

[3] Amit Kumar Gupta, Naveen Kumar Gupta, Rakesh Kumar, "An Efficient Secure Gateway Selection and Authentication Scheme in MANET", Volume 4, Issue 2, February 2014 IJARCSSE

[4] Biswas, Hui Liu, Dinesh Rajan, "Optimal Placement and Configuration of Roadside Units in Vehicular Networks", ISSN :1550-2252 Ieee transaction on vehicular technology,2012

[5] D. B. Jagannadha Rao,Karnam Sreenu, Parsi Kalpana "A Study on Dynamic Source Routing Protocol for Wireless Ad Hoc Networks", IJARCCE Vol. 1, Issue 8, October 2012

[6] Madhuri H Badole, T Raju, "Protocol design for an efficient GatewayDiscovery & Dispatching for Vehicular Ad HocNetwork", (IJAIEM),2014

[7] R.Kumar, Performance Evaluation of Gateway Discovery Approaches in the Integrated (MANET)-Internet Scenario",(IJCTEE) Volume 2, Issue 3, June 2012

[8] Safdar Hussain Bouk, Iwao Sasase, Syed Hassan Ahmed, and Nadeem Javaid, "Gateway Discovery Algorithm Based on Multiple QoS Path Parameters Between Mobile Node

and Gateway Node", journal of communications and networks, vol. 14, no. 4, august 2012.
[9] Z Mahmood et al, "Review paper of gateway selection schemes for MANET of NEMO",fifth international conference of mechatronics ,2013
[10] Amadou adama ba, abdelhakim hafid, jawad drissi, "Broadcast Control-Based Routing Protocol for Internet Access in VANETS" IEEE wireless communication and mobile computing conference,july 2011
[11] Rajesh Gargi yogesh chaba R.B.patel, "Performance Improvement of DYMO Routing Protocol using Gateway Authentication Technique" IEEE CECNet international conference on 23 april 2012