IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, February 2021
Impact Factor: 4.819

The Convergent Routing Scheme for Graph-Based Mechanism in Vehicular Ad Hoc Networks

Chinnadurai S and Abinaya R
Dhanalakshmi Srinivasan Engineering College (Autonomous), Perambalur, Tamil Nadu

Abstract: *Vehicular ad hoc networks (VANETs) are a special form of wireless networks made by vehicles communicating among themselves on roads. The conventional routing protocols proposed for mobile ad hoc networks (MANETs) work poorly in VANETs. As communication links break more frequently in VANETs than in MANETs, the routing reliability of such highly dynamic networks needs to be paid special attention. To date, very little research has focused on the routing reliability of VANETs on highways. In this paper, we use the evolving graph theory to model the VANET communication graph on a highway. The extended evolving graph helps capture the evolving characteristics of the vehicular network topology and determines the reliable routes preemptively. This paper is the first to propose an evolving graph-based reliable routing scheme for VANETs to facilitate quality-of-service (QoS) support in the routing process. A new algorithm is developed to find the most reliable route in the VANET evolving graph from the source to the destination. We demonstrate, through the simulation results, that our proposed scheme significantly outperforms the related protocols in the literature.*

Keywords: QoS, Vehicular Ad hoc Networks, VANET, MANET, Vehicular network topology.

I. INTRODUCTION

A VANET is effectively a subset of MANETs. Vehicular Ad-Hoc Networks consist of collections of vehicles equipped with wireless communication capabilities. Vehicles cooperate to deliver data messages through multihop paths, without the need of centralized administration. In VANETs (Vehicular Ad-Hoc Networks) RSUs (Road Side Units) and vehicles disseminate safety and non safety messages. The aim of VANETs is to enable dissemination of traffic information and road conditions as detected by independently moving vehicles. It is important to disseminate data from an information source vehicle to many destination vehicles on the road. Dissemination of data in VANETs is used to improve the quality of driving in terms of time, distance, and safety.

The proposed protocol gives the vehicle in the most dangerous situation the highest priority. The superiority of the proposed protocol over existing protocols is highlighted conceptually and with simulations.

1.1 Vehicular Ad-Hoc Networks

The majority of the data transmitted in the vehicular ad hoc network (VANET) supporting traffic safety applications will be broadcasted (one-to-many communication) and no acknowledgements (ACK) will be sent in response if messages are received successfully. Many ITS stations are typically interested in receiving the broadcasted messages and if everyone sent an ACK the communication channel would be flooded. In the VANET using 802.11p (with no central coordination), there will be a set of predetermined frequency channels for communication, and the only way to state the presence of an ITS station is to broadcast CAM/BSM on one these channels.

The network establishment has been removed in 802.11p, i.e., a station is allowed to communicate outside the context of a basic service set (the smallest building block of an 802.11 network). This implies that whenever a station has a message to send it can transmit directly under the condition that the MAC protocol allows it. Ad hoc topologies without prior network establishment has advantages such that a lower average delay can be achieved and no coverage by base stations is necessary – if there is someone to communicate with information exchange can take place. On the other hand, the ad hoc structure entails specific requirements for the communication protocols operating

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, February 2021
Impact Factor: 4.819

in this scenario. Specifically, the MAC protocol used in a VANET must be decentralized. It must cope with few stations as well as many stations without collapsing. Further, it should minimize simultaneous transmissions in an attempt to keep the interference at an acceptable level for receiving stations. The MAC protocol is a key component in cooperative systems because if channel access is not granted in a timely fashion, cooperation cannot be achieved.

1.2 Medium Access Control

The MAC method decides when a station has the right to access the shared communication channel. The regulation is made by scheduling transmissions in time, frequency, space or by using unique codes, constellations or interleaves to distinguish different stations. The type of MAC method to use in a particular communication network
is selected based on network topology and application. Since all communications in a centralized network must traverse the AP/BS, it has knowledge of all nodes within range. A centralized network can therefore use a centralized MAC protocol that distributes available resources (frequencies, time slots or orthogonal codes) among all nodes currently within range. This implies that the AP/BS can use the MAC protocol to optimize performance based on specific requirements. In ad hoc networks it is more difficult find such a resource efficient MAC method, especially since the number of stations can drastically vary from time to time. In a C-ITS operating in a VANET context, the requirements on the MAC method stem from three different parts namely (i) the ad hoc topology, (ii) road traffic safety applications, and (iii) the overall C-ITS

1.3 Vehicular Networks

In recent years, most new vehicles come already equipped with GPS receivers and navigation systems. Car manufacturers such as Ford, GM, and BMW have already announced efforts to include significant computing power inside their cars and Chrysler became the first car manufacturer to include Internet access in a few of its 2009 line of vehicles . This trend is expected to continue and in the near future, the number of vehicles equipped with computing technologies and wireless network interfaces will increase dramatically. These vehicles will be able to run network protocols that will exchange messages for safer, entertainment and more fluid traffic on the roads. Standardization is already underway for communication to and from vehicles. The Federal Communication Commission (FCC) in the United States has allocated a bandwidth of 75MHz around the 5.9GHz band for vehicle to vehicles and vehicles to road side infrastructure communications through the Dedicated Short Range Communications (DSRC) services.

1.4 Communications through Cellular Network

The first method connects vehicles to the Internet through cellular data networks using any of the following technologies: EV-DO, 3G, GPRS, etc. This service is already commercially available from car manufacturers and from other third-parties. In most commercially available solutions, the vehicle is transformed into a IEEE 802.11 (WIFI) hotspot and the Internet connection can be shared by many computers in the car. Usually, a limit is set on the amount of data transfer (e.g., 1GB or 5GB maximum per month). The main advantage of this method of connection is that the vehicle will have Internet access wherever cellular coverage is available. The main drawbacks are the dependence on the cellular operator coverage network and the limited available data rates (rates vary around 500Kbps – 800Kbps).

1.5 Vehicle to Highway Infrastructure Communications

The second method uses highway infrastructure. Here, vehicles connect to other vehicles or to the Internet through highway access points positioned along the roads. Two main variants can be found in the literature: the access points could be installed specifically for the purpose of providing Internet access to vehicles or the latter could make use of open 802.11 (Wi-Fi) access points encountered opportunistically along highway. The advantage of this method of connection is that vehicles will be able to connect to the Internet using much higher data rates (e.g., 11Mbps) than through the cellular network. The drawbacks include the cost related to installing access points along the roads to obtain reasonable coverage. Additionally, in the case where open access points are used, the access point's owners' consent would legally be required before such a service is deployed

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, February 2021
Impact Factor: 4.819

1.6 Characteristics of Vehicular Ad Hoc Networks

VANETs are characterized by (a) high node mobility, (b) constrained nodes movements (c)obstacles-heavy deployment fields, and (d) large number of nodes, which all add to the communication challenges. First, vehicles are continually moving along the roads at higher speeds than in a MANET. Thus a VANET will present a continually changing structure, and communication links are expected to be valid for few minutes or seconds. Next, the movements of vehicles are constrained on roads; hence the existing roadmaps put a limit to the topologies available in VANETs, when compared to MANETs. Then, the presence of high- rise buildings and houses between streets impacts the propagation of wireless waves through reflections and refractions. Finally, VANETs have the potential to contain a very large number of nodes as any vehicle can be part of the network. It is assumed that each vehicle is equipped with a Geographical Positioning System (GPS), digital maps or navigation system and an ad hoc wireless communication device.

II. EXISTING METHODOLOGY

- Direction Propagation Protocol (DPP) that elects two gateway nodes in a cluster, one node as a “header” and one node as a “trailer”
- The node farthest from the sender of the packet is selected as relay point. UMB is designed to overcome the interference, packet collision and hidden node problems during message distribution in multi hop broadcast
- Based on the requirements of ITS active safety applications, a mechanism to detect traffic congestion and a method to suppress unnecessary packets for improving the bandwidth utilizations have been introduced
- ABSM automatically adjusts its behavior without keeping track of the degree of mobility sensed by the vehicle to develop an adaptive algorithm which does not depend on any parameter or threshold value to reduce control messages overhead, by eliminating redundant transmissions and to obtain stable routes with the ability to auto-correct.
- AODV is a reactive routing protocol, which operates on hop-by-hop pattern. The Ad-Hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an Ad-Hoc network.

2.1 Drawbacks

- External sources for destination location
- Delay
- Increasing the network congestion
- Flooding in route discovery initial phase

III. PROPOSED METHODOLOGY

Vehicular Ad-Hoc Network (VANET) is a new challenging network environment that pursues the concept of ubiquitous computing for future. VANETs bring lots of possibilities for new range of applications which will not only make the travel safer but fun as well. Reaching to a destination or getting help would be much easier. The concept of VANETs is quite simple: by incorporating the wireless communication and data sharing capabilities, the vehicles can be turned into a network providing similar services like the ones with which are used in offices or homes. Many data dissemination protocols have been proposed to disseminate information about obstacles information, traffic conditions and mishap on the roads. The design of reliable and efficient broadcast protocols is a key enabler for the successful deployment of vehicular communication services. To achieve this, communication protocols must cope with the mobility of vehicles and the dynamics of wireless signals.

3.1 Advantages

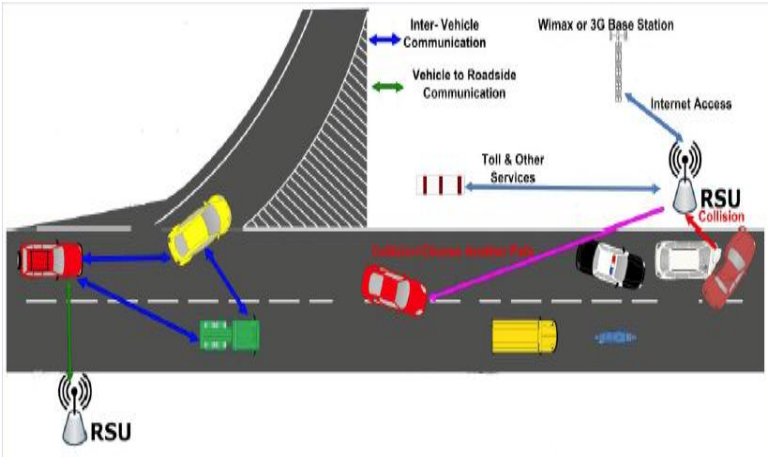
- Inter-vehicular communication services such as intersection collision warning, local danger warning, and the de-central dissemination of real-time traffic flow information.

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, February 2021
Impact Factor: 4.819

- The mobile terminals not only provide a function for information transmission and reception but also provide a function for information relay i.e. provides the function of router.
- Ad-hoc network provides anytime, anywhere access environment.

IV. Related Work

The research on vehicular networks has been growing rapidly in recent years. The security issue is very important for VANETs. A **comparative** study has to be done with the previously existing protocols and the improvements can be made to efficiently disseminate information in vehicular ad hoc networks. There are several directions that could be investigated in order to make protocol more secure. Proposed protocol need to be analyzed mainly in the following aspects: authentication and key management, privacy, and secure positioning. Proposed protocols need to be analyzed in real test bed in order to assess its performance in real scenarios. Such test bed experiments will enhance the protocol.



V. Methodologies

- The simulation work has been done with The Network Simulator (NS-2), Version 2.29. In the simulation 50 nodes are randomly distributed within the network field of size 400mx2400m.
- The RDSM protocol allows any node in the network to discover and verify the position of its communication neighbors participating in the protocol message exchange.
- RDSM does not aim at building a consistent map of verified nodes, as every verifier autonomously tags its neighbors as verified, faulty or unverifiable.
- To selects the neighbor to broadcast the packets in the network. Neighbor selection will be done from the broadcasting of beacon messages in the network.
- It selects the route to broadcast the packets in their network. Route selection will be done through calculating the distance between the nodes. It chooses the route, which has the shortest distance.
- Finally in this module data is disseminated in case of emergency event. Vehicular Ad-Hoc Networks (VANETs) consist of collections of vehicles equipped with wireless communication capabilities.

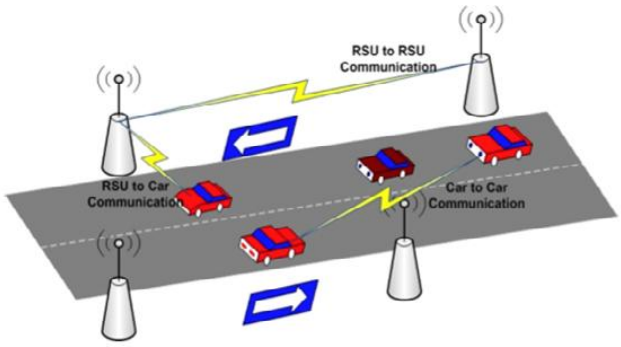
5.1 VANET

- Vehicular ad-hoc networks (VANETs)

5.2 Structure

- Vehicle-to-roadside
- Inter-vehicle

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, February 2021
Impact Factor: 4.819



5.3 Technologies Used

- Sensor technologies(Infra-red sensing/Video and Camera Image Perception/RADAR/gyro sensor/inertial sensor), process data through mathematical algorithms to come up with a virtual understanding of the vehicle environment
- In-vehicle digital maps and positioning technologies(GPS/WiFi/WiMax) as sensing systems to accurately identify the vehicle position and interpret the environment
- If there is a gridlock/high traffic density detected by a roadside infrastructure then the roadside system can broadcast the information to all its nodes/vehicles
- In turn using the DTN capabilities of VANETs, the information can be transmitted to other vehicles heading towards this junction.
- Likewise, it can convey to the incoming vehicles other paths, depending on a centralized system co-ordination of finding non-traffic routes at that point of time.

5.4 Security in VANETs

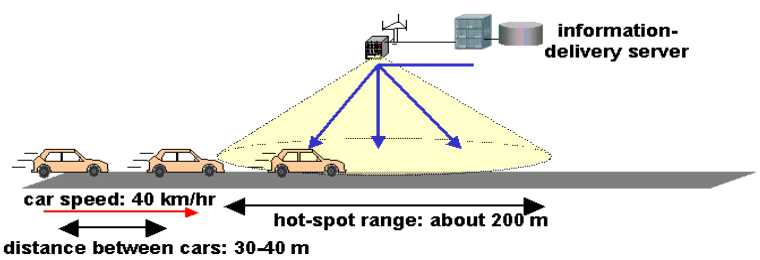
- When data is compromised, the whole system suffers.
- The nature of VANETs could lead to malicious attacks.
  - Predictable movement of nodes.
  - High mobility of victim/attacker.
- Adversaries could break the system.
  - Data sinkholes (black hole).
  - Feed false information.
  - Sybil attacks.
  - Flood the system.
- Security measures must be taken to avoid malicious attacks on the system.

VI. CONCLUSION

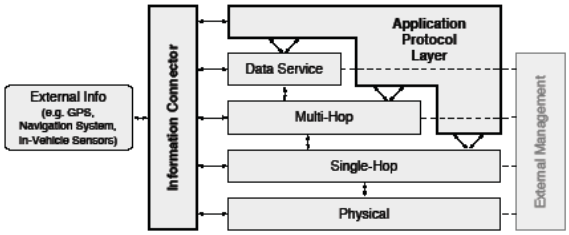
- In VANET, vehicles can communicate with the roadside communication infrastructure and also among each other.
- A vehicle is not only information source or sink, but also information distributor.
- The communication services enable a wide range of applications, ranging from road safety and traffic efficiency, driving comfort and infotainment.
- In Intelligent Vehicular Ad-Hoc network (In VANET), vehicles are enabled to communicate among themselves i.e. V-2-V. It is explained that V-2-V enables communication for small to medium distances and at locations even where roadside access points are not available. Are we assuming that all the vehicles on the road will be equipped with communication/networking capabilities? If not, how realistic is in VANET?

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, February 2021
Impact Factor: 4.819

- Vehicles move at certain speeds. We have roads or highways which have various speed limitations. Does in VANET impose any restriction on the speed of a vehicle for its smooth operation?



- The basic safety message spreading in a vehicular network consists of event warning message. But there are scenarios when message need to be delivered to specific areas for example, to the end of a traffic jam queue so that arriving vehicles have the option of taking another route before getting stuck. How can the vehicular network support the secure routing?
- Any two nodes that wish to communicate securely can simply establish apriority a shared secret, to be used by their routing protocol modules.
- Is the network expandable? How did the cars in the network and the terminals maintain the flow control in the network?



REFERENCES

[1]. L. Zhang, C. Hu, Q. Wu, J. Domingo-Ferrer, and B.Qin, "Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response," IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, Aug. 2016.

[2]. Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," IEEE Transactions on Vehicular Technology, vol. 59, no. 2,pp. 559–573, Feb 2010.

[3]. F. Qu, Z. Wu, F. Y. Wang, and W. Cho, "A security and privacy review of vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996, Dec 2015.

[4]. "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages," IEEEStd 1609.2-2016 (Revision of IEEE Std 1609.2-2013), pp. 1-240, March 2016.

[5]. "L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in vanets," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 3, pp. 516–526, March 2017.

[6]. L. Chen, S. L. Ng, and G. Wang, "Threshold anonymous announcement in vanets," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp.605 -615, March 2011.

[7]. Y. Liu, J. Ling, Q. Wu, and B. Qin, "Scalable privacy-enhanced traffic monitoring in vehicular ad hoc, networks," Soft Computing, vol. 20, no.8, pp.3355-3346, Aug 2016.

[8]. R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward cloud based vehicular networks with efficient resource management," IEEE Network, vol. 27, no. 5, pp. 48–55, September 2013.

IJARSCT
ISSN (Online) 2581-9429
ISSN (Print) 2581-XXXX
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, February 2021
Impact Factor: 4.819

[9]. J. A. Guerrero-ibanez, S. Zeadally, and J. Contreras-Castillo, "Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies," IEEE Wireless Communications, vol. 22, no. 6, pp. 122–128, December 2015.

[10]. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia," A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp.50–58, Apr. 2010002E