International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Intelligent Route Discovery through DSP Algorithm in Vehicular Ad-Hoc Networks

Harshal D. Misalkar[Á*] and S. S. Sikchi[Ḃ]

[Á]Information Technology, SGBAU Amravati, Pundlik Baba Colony, Nr Yashoda Nagar, Amravati, Maharashtra, India
[Ḃ]Information Technology, SGBAU Amravati, Khaperde Bagichya, Near Irwin Square, Amravati, Maharashtra, India

Accepted 10 May 2014, Available online 01 June2014, **Vol.4, No.3 (June 2014)**

Abstract

A vehicular ad hoc network is also known as a vehicular sensor network by which driving safety is enhanced through inter-vehicle communications or communications with base station. Vehicular ad-hoc network is different from all other form of ad hoc network because of its hybrid nature and node movement i.e. high mobility of VANET. Design of an efficient routing protocol for VANETs is very crucial. Therefore, in this paper we discuss the routing protocols and implementation of DSP Algorithm in VANET.

Keywords: *VANET, Routing, Mobility, Hybrid.*

1. Introduction

An ad hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use of existing network infra-structure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple network hops may be needed for one node to exchange data with another across the network. In such a network, each mobile node operate not only as a host but also as a router, forwarding packets for other mobile nodes in the network, that may not be within the direct reach wireless transmission range of each other. Each node participates in an ad hoc routing protocol that allows it to discover multi hop paths through the network to any other node. The idea of an ad hoc network is sometimes also called an infrastructure-less networking.

VANET was created in October 2002 by the Federal Communications Commission (FCC). The aim of its creation was to improve safety on the roads. A vehicular ad hoc network is also known as a vehicular sensor network by which driving safety is enhanced through inter-vehicle communications or communications with server. Vehicular communication network is a promising approach to facilitating road safety and traffic management for drivers and passengers. One of the ultimate goals in the design of such networking is to resist various malicious abuses and security attacks.

In ad hoc network the VANET maintain and update information on routing between all nodes of a given network at all times. A Vehicular Ad-Hoc Network, or VANET, is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment (Base Stations) via radio waves. These have similar characteristics as mobile ad hoc networks, often in the form of multi-hop networks. Due to the high mobility of nodes network topology changes occur frequently.

There are three categories of VANET network architecture

i) Wireless Lan/Cellular Network

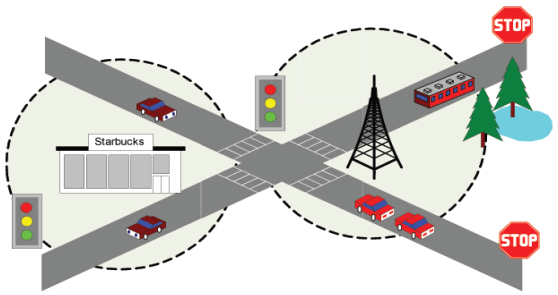

Fig.1 (a) WLAN/Cellular network

ii) Ad hoc Network

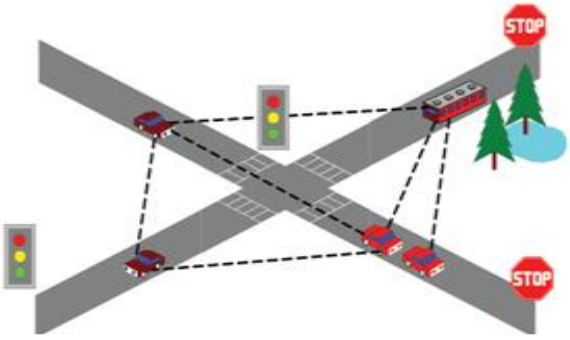

Fig.1 (b) Ad hoc

*Corresponding author: **Harshal D. Misalkar**

iii) Hybrid Network

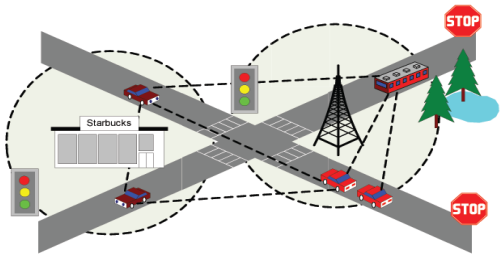

Fig.1(c) Hybrid network

2. Network Architectures and Characteristics

As shown in Figure 1, the architecture of VANETs falls within three categories i.e. pure cellular/WLAN, pure ad hoc, and hybrid.

As shown in Figure 1(a) VANETs can combine both cellular network and WLAN to form the networks so that a WLAN is used where an access point is available. Stationary or fixed gateways around the sides of roads could provide connectivity to mobile nodes (vehicles) but is eventually unfeasible considering the infrastructure costs involved. In such a scenario, all vehicles and roadside wireless devices can form a mobile ad hoc network.

As shown in Figure 1(b) Ad hoc network is used for to perform vehicle-to-vehicle communications and achieves certain goals, such as blind crossing (a crossing without light control).

As shown in Figure 1(c) A hybrid architecture of combining cellular, WLAN and ad hoc networks together has also been a possible solution for VANETs. Hybrid architecture which uses some vehicles with both WLAN and cellular capabilities as the gateways and mobile network routers so that vehicles with only WLAN capability can communicate with them through multi-hop links to remain connected to the world.

Similar to mobile ad hoc networks (MANETs), nodes in VANETs self-organize and self-manage information in a distributed fashion without a centralized authority or a server dictating the communication. In this type of network, nodes engage themselves as servers and/or clients, thereby exchanging and sharing information like peers.

Moreover, nodes are mobile, thus making data transmission less reliable and suboptimal. Apart from these characteristics, VANETs possess a few distinguishing characteristics, presenting itself a particular challenging class of MANETs. Apart from these characteristics, VANETs possess a few distinguishing characteristics are-

- Highly dynamic topology
- Frequently disconnected network
- Patterned Mobility
- Propagation Model
- Unlimited Battery Power and Storage
- On-board Sensors
- Geographical type of communication

3. Routing protocols in VANETs

Routing tasks in VANETs are very challenging due to the high speed of vehicles making topology of the network highly dynamic and causing frequent links disconnections. Routing protocols in VANETs are classified into following categories considering the routing technique aspects. Topology-based, Position-based, Cluster-based, Geocast-based, Broadcast-based.

1) **Topology- based routing protocol:-** In case of topology based routing protocol, selection of route from one point to another i.e. source to destination is based on links information previously collected by the vehicle or sought when needed on-demand. Here, the step of searching or maintaining a route from source to destination is required by rule before sending data packets.

2) **Position-based routing protocols:-** Geographic routing also called position-based routing. It is a principle that relies on geographic position information. It is mainly proposed for wireless networks and based on the idea that the source sends a message to the geographic location of the destination instead of using the network address. This class uses vehicles geographical information in the relay selection process assuming that each vehicle has the mean to know its geographical position. Here, the knowledge of the whole route is unnecessary to deliver the data packets.

3) **Cluster-based routing protocols: -** In cluster-based routing, a virtual network infrastructure must be created through the clustering of nodes in order to provide scalability. Vehicles sharing similar characteristics, such as performing in the same direction with more or less the same velocity, can form a group and elect a cluster-head which manages the clump and is in charge of inter-cluster communication. It is note that intra-cluster communications are cluster-head free and perform using direct links.

4) **Geocast-based routing protocols: -** Geocast routing is basically a location-based multicast routing. The objective of a geocast routing is to deliver the packet from a source node to all other nodes with a specified geographical region. It follows the principle of routing data packets from a single source vehicle to all vehicles belonging to the destination area called zone of relevance ZOR. However, to override the simple flooding of the geocast message from the source to the ZOR, a forwarding area called zone of forwarding. ZOF is used to confine the message forwarding until it reaches the ZOR

5) Broadcasting based routing protocols:- Broadcasting refers to transmitting a packet that will be received by every device on the network. It refers to a method of transferring a message to all recipients simultaneously. Broadcast is a frequently used routing method in VANETs, such as sharing traffic, weather, emergency, road condition among vehicles, and delivering advertisements and announcements. IT is also used in unicast routing protocols (routing discovery phase) to find

an efficient route to the destination. When the message needs to be disseminated to the vehicles beyond the transmission range, multi-hop is used.

This class of routing protocols uses the simple flooding in which each node re-broadcasts messages to all of its neighbors except the one it got this message from. Flooding guarantees the message will eventually reach all nodes in the network. Flooding performs relatively well for a limited small number of nodes and is easy to be implemented.

4. System Architecture

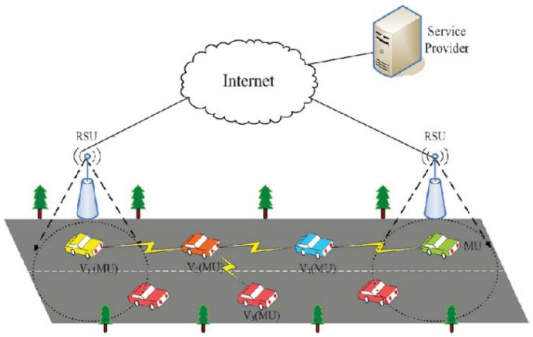

Fig.2 VANET architecture

RSU: The Road Side Units serve as the gateway to connect service provider servers and the Moving Units. Usually, the RSUs are assumed that they may be compromised by attackers, whereas the service provider cannot be compromised since it is in charge of service guarantee and billing. It is also assume that the RSUs could connect to service provider servers by wired links of high bandwidth capacity, low delay, and low bit error rates.

MU*:* In our Idea, the vehicles are moving unit with which mainly communicate with each other for sharing local traffic information to improve safe driving conditions and with RSUs for requesting services. According to the medium used for communications between neighboring MUs and between MUs and RSUs is a 5.9-GHz dedicated short-range communication.

Millions of people around the world die every year in car accidents and many more are injured. Implementations of safety information such as speed limits and road conditions are used in many parts of the world but still more work is required. Vehicular Ad Hoc Networks (VANET) should, upon implementation, collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it.

Vehicular communication networking is a promising approach to facilitating road safety, traffic management, and infotainment dissemination for drivers and passengers. Improving the route discovering process with reducing delay, reduce overhead and localize destination and also improve Communication among road side unit.

Faster data transmission is most important requirement of vehicular ad hoc network. Intelligent route discovery like finding shortest path while transmitting the data from source to destination, so that emergency information about danger will reach on exact destination before actually face by driver and passenger. Hence invention of such technique is important for effective data communication.

5. Dijkstra's Shortest Path Algorithm

Dijkstra's shortest path routing algorithm is link-state-based and iterates on the distance metric. The algorithm uses a "closest nodes "concept and is based on the following principle:

Given a source node, n, the shortest path from n to the next closest note , s, either (a) is a path that directly connects n to s or (b) includes a path containing n and any of the previously found intermediate closest nodes plus a direct link from the last intermediate closest node of this path to s.

Consider the following undirected graph, which depicts a sample network. The vertices A, B, C, D, E, and F may be thought of as routers, and the edges connecting the vertices are communication links.

Edge labels represent an arbitrary cost metric. Our goal is to find the shortest path from A to D based on distance.

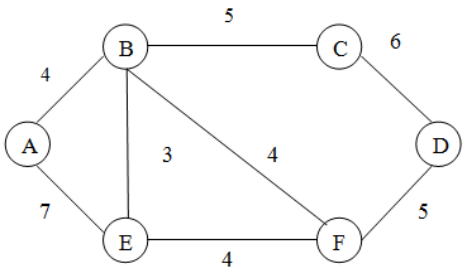

Fig.3 undirected graph with weighted edges

To implement this algorithm, it is helpful to maintain a running record of the successive closest nodes to the source node. Let k represent the nth node. Thus, node A corresponded to k=0. That is, the zero closest node to A is itself. This is the initialization step of the algorithm. We now begin our search for the successive closest nodes to A.

First Closest Node (k=1)

The first closest node to A is either B or E since they are both directly connected to A. Since the AB path has a smaller cost, we select it. Thus, B is the first closest node to A.

K	Node	Path
0	A	-
1	B	AB

Second Closest Node (k=2)

The second closest node to A must either be (a) a direct link from A or (b) via a path that includes the first closest node. The possible paths and related costs are: ABC=9, ABF=8, ABE=7, or AE=7. There are two shortest paths: ABE and AE. THUS, E is the second closest node to A.

K	Node	Path
0	A	-
1	B	AB
2	E	ABE
		AE

Third Closest Node (k=3)

The third closest node to A must be via path that includes nodes B or E.(There are no more direct link to A.) The possible paths and related costs are: ABC=9, ABF=8, ABEF=11, or AEF=11.The shortest path is ABF. Thus, F is the third closest node to A.

K	Node	Path
0	A	-
1	B	AB
2	E	ABE
		AE
3	F	AEF

Fourth Closest Node (k=4)

The fourth closest node to A via path that includes nodes B, E, or F. The possible paths and related costs are: ABC=9 or ABFD=13. The shortest path is ABC. Thus, C is the fourth closest node to A. Note that neither ABEF nor AEF is considered at this stage of the algorithm because F was previously found to be the third closest node.

K	Node	Path
0	A	-
1	B	AB
2	E	ABE
		AE
3	F	AEF
4	C	ABC

Fifth Closest Node (k=5)
The fifth closest node to A via path that includes nodes B, E, F, or C. The possible paths and related costs are: ABCD=15, ABFD=13, ABEFD=16 and AEFD=16. The shortest path is ABFD. Thus, D is the fifth closest node to A.

K	Node	Path
0	A	-
1	B	AB
2	E	ABE
		AE
3	F	AEF
4	C	ABC
5	D	ABFD

Since D is the destination node, the shortest path from A to D is ABFD.

One of the main reasons for the popularity of Dijkstra's Algorithm is that it is one of the most important and useful algorithms available for generating (exact) optimal solutions to a large class of shortest path algorithm.

6. Network Architecture

The following VANET architecture has been considered here, which is as shown in figure 4. A vehicular ad hoc network is also known as a vehicular sensor network.

In VANET driving safety is enhanced through inter-vehicle communications (V2V) or communications with road side unit i.e. base station (V2R).

Here the communicating devices (Nodes) i.e. RSU are spread through the network randomly. Each node is limited by its transmission range, which limits its capacity to communicate with all the vehicles those are within the range of RSU. Hence a source node should use one or more intermediate nodes to communicate with the intended node. The nodes which lie within the transmission range of a node are said to be neighboring nodes for that particular node. The node, which is in need to communicate with some other node, is termed as source node, with which the source node wants to communicate is termed as destination node.

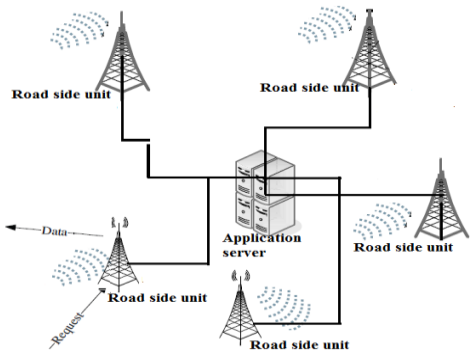

Fig.4 Network Architecture

This Idea has following phases:-

1) Select number of nodes.
2) Giving X and Y co-ordinates of all intermediates nodes.
3) Network management with determination of range.
4) Application Server broadcast information to entire nodes of network.
5) Source and destination node selection.
6) Application Server sending shortest routing path information to requested RSU.
7) Detection of faulty node in case of its availability in shortest routing path provided by server.
8) Alternate route formation for vehicle to move which is stick at particular node because of dense network.
9) Release all resources after receiving data to destination node.

This project focus on detection and elimination of malicious nodes in VANETs using two way handshaking process between server and all the nodes of network based on unique number (ID). For the provision of finding shortest path in a network, at the time of moving from source to destination, DIJKSTRA'S shortest path algorithm is employed for entire network for the faster data transmission.

To find the malicious nodes among the intermediate nodes, all the nodes are continuously monitored with the help of application server. Server will determine the nodes as malicious nodes on the basis of database maintained at server. Database contains information of entire network i.e. of each and every node, which is actually received by the server in the form acknowledgment. Once the intermediate node is determined as the malicious node, the alternate shortest path is employed from current node to the destination. To test the operative effectiveness and performance of the system some of the performance parameters evaluated are, No. of route available, intelligent route discovery, Detection of malicious network.

Initially server send data to all nodes and receive acknowledgment from each and every node, in this way communication is maintained between each node towards the server is carried out, this is technique is also known as two way handshaking process. This helps to locate malicious node in our network. If we want to transfer data from source to destination user has to provide definition of source and destination. At the time of data transmission, node is said to be connected with other node when the other node is within the range of first.

Formation of the clusters

A node is said to be connected with other node when the other node is within the range of first node. Let the coordinates of node1 be (x1, y1) and that of node2 be (x2, y2) the distance between them is calculated by using the formula,

$$D = \sqrt{(x1 - x2)^2 + (y1 - y2)^2}$$

If D <= Range, the node is said to be connected otherwise it is disconnected. Based on the communication range and coverage area of the base station the clusters are formed.

Vehicle within the range of RSU, it send request for shortest path from one place to another .Road side unit accept that request and submit to application server. After that, server will process the request and send response to respected RSU. Finally RSU send back to vehicle. One of the most important role played by server All important or safety information's such as traffic jam, accident i.e. dense network are quickly broadcast to all nodes of network. In such scenario server will provide another shortest route, if it is available towards that destination.

To transfer data between two nodes will take some fixed interval of time delay. In this time delay user will see current situation of system. In the mean time if user creates malicious node then server will come to know with the help of handshaking process which is carried out between all nodes and server. In this way server will tracing location of malicious node in our system.

Conclusion

We present a novel approach to Recognize and Eliminate malicious nodes in VANETs using two way handshaking process between server and each node with the help of road stations unique number (ID). The proposed methodology and its results show that by using this, we can easily recognize and eliminate the malicious nodes in the Vehicular Ad Hoc Network. This system evaluates performance parameters evaluates are, Number of paths available, Number of routes involving malicious nodes, Number of malicious nodes.

Use of DIJKSTRA'S shortest path algorithm in this project proves that it is one of the most important and useful algorithms available for generating (exact) optimal solutions to a large class of shortest path algorithm. The proposed methodology shows greedy algorithm that produces an optimal solution. The goal of this project is to develop a vehicular communication system to enable quick and cost efficient distribution of data for the benefit of passenger's safety and comfort also facilitating road safety and traffic management.

References

Prashant Sangulagi, Mallikarjun Sarsamba, Mallikarjun Talwar, Vijay Katg (Mar 2013) "*Detection and Elimination of Malicious Nodes in Vehicular Ad hoc Networks (VANET's)*" Indian Journal of Computer Science and Engineering (IJCSE). Vol. 4 No.1

Fan Li and Yu Wang, University of North Carolina at Charlotte (JUNE 2007) "*Routing in Vehicular Ad Hoc Networks: A Survey*" IEEE Vehicular Technology Magazine.

Xiao lei Dong, Lifei Wei, Haojin Zhu, Zhenfu Cao, and Licheng Wang (FEBRUARY 2011) "*EP2DF An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-Oriented Vehicular Ad Hoc Networks*" IEEE Transactions on Vehicular Technology, Vol

Salim Allal, Saadi Boudjit "*Geocast Routing Protocols for VANETs: Survey and Geometry-Driven Scheme Proposal"* Journal of Internet Services and Information Security (JISIS), volume: 3, number: 1/2, pp. 20-36.

Ejaz Ahmed, Kashan samad, Waqar Mahmood (Aus CERT-2006), "*cluster based intrusion detection architecture for vehicular ad hoc network"* 5thConference, Gold Coast, Australia. pp:48.

M. Johnson, L. De Nardis, and K. Ramchandran, (September 2006.) *"Collaborative Content Distribution for Vehicular Ad Hoc Networks*," Allerton Conf. Communication, Control, and Computing, Monticello, IL,

S. Lo and W. Lu,(Apr. 2009) "*Design of data forwarding strategies inVehicular Adhoc Network*," in Proc. VTC, pp.1-5,

Kevin C. Lee, Uichin Lee , Mario Gerla" *Survey of Routing Protocols in Vehicular Ad Hoc Networks*" Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, book.