International Journal of Engineering Applied Sciences and Technology, **2016**
Vol. 1, Issue 4, ISSN No. 2455-2143, Pages 69-74
Published Online January-February 2016 in IJEAST (http://www.ijeast.com)

GREEN MARKETING: AN INITIATIVE TAKEN BY BUSINESS ORGANIZATIONS (OPPORTUNITIES & PROBLEMS)

Dr. A. Meiappane
Associate Professor
Manakula Vinayagar Institute of Technology,
Puducherry

V. Nivetha
PG Student
Manakula Vinayagar Institute of Technology,
Puducherry

***Abstract*— In this modern world, VANET (Vehicular Ad hoc Network) is based on the significant of human security by GPS and navigation method. We propose a prioritized routing protocol for prioritize the emergency message to reach the destination by using On Board Unit (OBU) and Road Side Unit (RSU). Here we using the Broadcast routing protocol with priority and to enhance the user location to provide fully distributed multicast routing protocol, use different form of QoS (Quality of Services) for the different kinds of information, and distance per hop distribute maximum messages. This propose system will configure the vehicle settings by using VANET, design the topology for vehicle to set in particular location and estimate the RSU and OBU unit.**

Key Words: Prioritized based Routing Protocol (PRP), VANET, RSU, OBU, QoS

I. INTRODUCTION

In the old days, the drivers generally refer to a hard copy of the map. But still finding a route is common event for all drivers. After introducing the Global Positioning System (GPS), by receiving the signal driver can be decide the current location and also find the shortest route to reach the destination based on local map. Even though searching the route is based on local map and real time road condition is not taken into an account. By studying the real time road condition [3], a drivers will convert the message to the another system termed as Traffic Message Channel (TMC), which traffic message channel broadcast the traffic information from the Radio FM Data System (RDS).

The purpose of VANET is to permit wireless communication between vehicles on the road covers the roadside wireless sensors, enabling the transfer of information to guard driving safety and planning for dynamic routing. In figure 1, A vehicle can communicate with another vehicle really known to be Vehicle to Vehicle (V2V) communication, or a vehicle able to communicate with an infrastructure such as a Road Side Unit (RSU), well-known as Vehicle-to-Infrastructure (V2I).

Some of the key applications of VANET can be summarised as follows [9]:
Road Traffic Safety- Effort on falling the number of grievances on the roads by alerting the driver about dangers in advance.
Traffic engineering or Efficiency- Increasing the overall performance of the transport systems by sinking, travelling time and congestion.
Comfort and Quality of Road Travel - grant console applications for travellers like 'superior traveller messages systems', 'electronic payment service, 'variable message signs' and 'electronic toll collection' etc.

The purpose of VANET is to allow wireless communication between vehicles on the road including the roadside wireless sensors, enabling the transfer of information to ensure driving safety and planning for dynamic routing, allowing mobile sensing as well as providing in-car entertainment [6]. As VANETs have unique features which contain dynamic topology, frequent disconnection of the networks, and varying environments for communication, the routing protocols for conventional MANET such as Ad hoc On-demand Distance Vector (AODV) (Perkins and Royer, 1999) are not directly usable for VANETs.
In order to achieve further advancement in the technology of mobile communication, research in the vehicular industry has been done with special emphasis in the areas of routing and routing management, information security, and enabling communication between vehicle-to-vehicle and vehicle-to-infrastructure, as well as technological deployments. In the area of routing, however, real-life urban environments cannot be properly reflected by the currently implemented routing protocols for VANETs. Therefore, this study is done in order to solve the problems regarding roads with intersections by addressing the issues which arise from packet transfers on the road and at intersections. The study focuses on improving

International Journal of Engineering Applied Sciences and Technology, **2016**
Vol. 1, Issue 4, ISSN No. 2455-2143, Pages 69-74
Published Online January-February 2016 in IJEAST (http://www.ijeast.com)

VANETs in terms of routing and data forwarding where the characteristics of VANETs are incorporated into the design of a protocol for urban environments.

In this paper we propose VANET based prioritized multicast routing protocol to prioritize the message and also driver to receive this message. Here we used the Priority based Routing Protocol (PRP) to offer the fully circulated routing protocol, the dissimilar quality of services (QoS) for dissimilar message priorities, and peak message distribution distance per hop [8]. PRP is based on broadcast communication; hence the protocols will not require the routing maintenance. Only utmost vehicle will be distributed preferred as a relay vehicle and rebroadcast safety messages. In this exertion, we guess that all vehicles have arranged with Global Positioning System (GPS) to recover their locations and sensors to confirm for defect on vehicles. The vehicles are also implicit to have sufficient storage to store the safety messages for redundancy check.

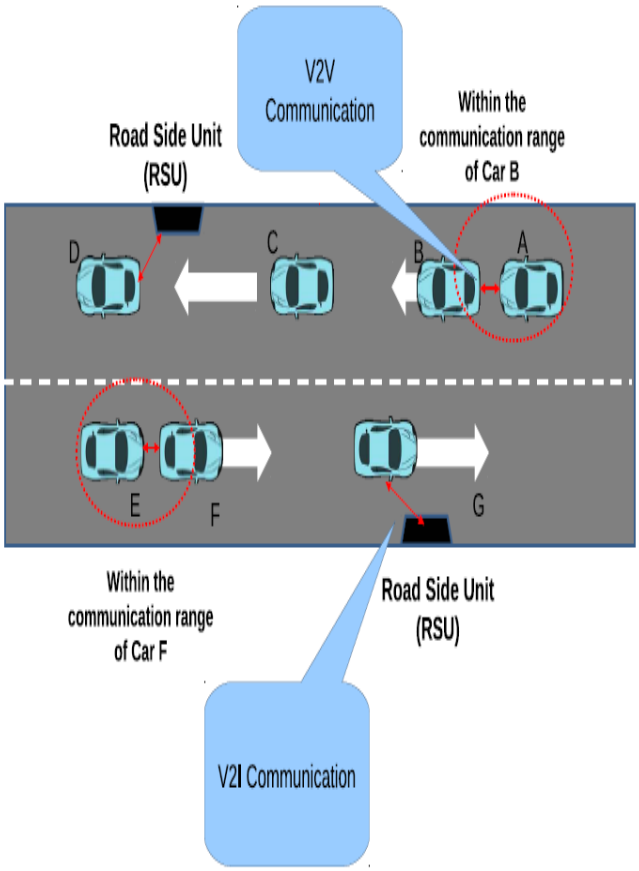


Fig 1: Creating an Ad-hoc Network using Vehicles (VANETs)

II. RELATED WORK

In [1], the author presented a navigation service to develop the road information to guide the drivers to reach the destination. By using VANET, Finding the shortest route and also protect the driver. Here the main monitoring and authority server is handled by single server. If the server fails then the whole application will stop working. VANET has high mobility and authentication is done at every frame by using ECC algorithm. This scheme assumes some security primitives in a significant way to provide a security features such as Vehicles are authenticated by means of pseudo identities, Navigation queries and results are protected from overseer. Besides, with the idea of unsigned permit, no one including TA can link up a vehicle's navigation query and its identity and Information provided by RSUs can be properly authenticated before the route is actually being used. Further satisfying all security and privacy requirements, our result is capable in the wisdom that a vehicle can complete the entire navigation querying process and receive critical announcement in a very short time. VSPN scheme can also apply to the situation where the route searching process is made by a central server, which collects and verifies the data speed and road conditions from RSUs. The authentication process at vehicles can be still simpler because a vehicle only needs to check beside the central server's signature.

In [2], the author provide different routing protocol used to perform well in both crowded and meager traffic conditions either in town or freeways effortlessly. Both unicast and broadcast protocols finding the position in safety related applications. Although flooding is a procedure appropriate for such applications, blind flooding guides to broadcast-storm problem and results in fragmentation in network. Multicast and Geocast protocols [12] are chosen over flooding techniques in order to guarantee end-to-end quality of service. Proactive approaches for routing have the overhead of maintaining the routing table containing the information of all the vehicles in the network and sharing it among the vehicles, which reduces the usable bandwidth. On the contrary, reactive approaches discover the routes between the vehicles that are communicating on-demand and hence less overhead of route maintenance. Position based routing methods endure from finding the exact location of the vehicles due to the intrinsic incorrectness of the GPS location. Delay tolerant network technique uses a store and forward method to store the data in database or forward the information to drivers. Cluster based routing protocols are suitable for district services and enlarge the different services by means of inter-cluster and intra-cluster communication. Adaptive routing in universal follows two approaches [11] namely methods based on context-awareness and methods encouraged by natural occurrence such as ant activities. Context-aware routing protocols try to integrate the external sources of information such as digital atlas, positioning systems, location services or even schedule of unrestricted transport to develop the performance. Swarm intelligence based protocols aspire to build self-organizing networks based on the collective intelligence of groups of simple agents, i.e. network vehicles.

International Journal of Engineering Applied Sciences and Technology, **2016**
Vol. 1, Issue 4, ISSN No. 2455-2143, Pages 69-74
Published Online January-February 2016 in IJEAST (http://www.ijeast.com)

In [7], The author existing a multi-cast routing approach for transmit the warning information in CCWSs. Dissimilar prior broadcast schemes, the proposed multicast schemes incorporate the model of adaptive transmission range and utilize the vehicle communication graph to spot the receiver vehicles. Using this scheme, the wireless channel efficiency can be enhanced by sinking the number of sent messages and by reducing the radio transmission range. Simultaneously, the receivers can be prioritized based on their decisive interval to frustrate collision, guarantying in-time delivery of the warning messages. We have publicized that the concept can be formulated as an interruption guarded minimum Steiner tree (D-CMST) problem, which is a famous NP problem. Future work includes a performance evaluation and comparison with other broadcast protocols that will be based on researches performed in a network simulator. Advance research is required to enlarge a complete communication protocol based on this multicast scheme. This protocol should consider various characteristics such as consistency, message encoding, numerous sender, transmission scheduling, and multi-channel operation. Also examines superior D-CMST algorithms that can take advantage of the context information such as position, and can be competently implemented in a distributed computing environment.

III. PROBLEM STATEMENT

3.1 OVERVIEWS ASSUMPTION

In this world the drivers face the difficult tasks to find the route to reach the destination. But in the old days, the drivers usually refer the hard copy of map to reach the destination [10]. After that GPS (Geographical Positioning System) was introduced to become more popular. For example, install the GPS device to the vehicle. Using the GPS signal, the device will identify the current location and transmit to local map. In this VANET, TMC (Traffic Message Channel) is used to broadcast the traffic information from Radio FM Data System (RDS).

3.2 SECURITY REQUIREMENT

Security is a significant concern for ad hoc networks, mainly for security awake applications [4]. To secure an ad hoc network, we require considering the following aspect as criteria to evaluate security which incorporates availability, confidentiality, integrity, authentication and non-repudiation, authorization, real time constraints, data consistency, privacy, anonymity.

A. Availability

The availability deal with involve the bandwidth and connectivity of all vehicles by using network services. By using group signature scheme has introduce to guarantee the availability issues, prevention and detection method. This scheme is fully focus on availability of switching the messages between vehicles and RSUs. When the attackers origins the network unavailability, and the proposed techniques still persist due to interconnection using public and private keys between RSUs and vehicles.

B. Confidentiality

Confidentiality assurances that secrete message in the network can never release to anonymous entities. It also avoids unauthorized access to secret information such as driver's name, shield number and location. The most admired technique, sobriquets are used to conserved privacy in vehicular networks. For encryption, each vehicle will have multiple key pairs. Messages are encrypted or signed using different pseudo id and this pseudo id has not related to the vehicle but appropriate authority has access to it. Vehicle requires gaining new pseudo id from RSUs earlier than the past pseudo id terminate.

C. Authentication

Authentication is the confirmation of the identity between vehicles and RSUs and the justification of integrity of the information swap. Moreover, it guarantees that all vehicles are the right vehicle to interact within network. Public or private keys with CA are suggested to initiate connection between vehicles, RSUs and AS. On the contrary, password is used to access to the RSUs and AS authentication method. Signing each message with this, origins an overhead, to reduce this overhead we can use the approach ECC (Elliptic Curve Cryptography), the efficient public key cryptosystem, or we can sign the key just for the significant messages only.

D. Authorization

Authorization is an advanced level implemented by access control which itself is described by network strategies. Authorization defines the task of a vehicle in the network which comprises the kinds of messages a vehicle can translate or note down on the network, actions. it is allowed to receive and usually the protocols that it can execute.

E. Data Consistency

Moreover authenticating the sender, the reliability of messages with related ones concerning time and location must also be measured, because false messages from genuine senders are not unattainable. It is really essential for warning messages to gather the moment and location constraint. A warning information must be exposed to the driver prior to it is also behind to respond and also prior to passing the related geographic position of the warning.

IV. PRORPOSED WORK

Vehicular ad-hoc networks (VANET) are communicated between the moving vehicles in specific surroundings. Here

International Journal of Engineering Applied Sciences and Technology, **2016**
Vol. 1, Issue 4, ISSN No. 2455-2143, Pages 69-74
Published Online January-February 2016 in IJEAST (http://www.ijeast.com)

Vehicle to Vehicle communication will communicate the vehicle with other vehicles directly, or a vehicles can communicate to an infrastructure such as Road Side Unit (RSU), well-known as Vehicle-to-Infrastructure (V2I). The intention of VANET is to permit the wireless communication between vehicles on the road that allows conveying of information to guarantee driving safety.

This paper offers the Routing Protocol for priority based message in VANET. We proposes a prioritized routing protocol for prioritize the disaster message to attain the destination by using On Board Unit (OBU) and Road Side Unit (RSU). Here we apply Broadcast routing protocol [5] with priority and to develop the user location to intend entirely distributed multi-cast routing protocol, use different form of QoS (Quality of Services) for the different sorts of information, and distance per hop distribute maximum messages.

Prioritized based Routing Protocol (PRP) has to outlook based on broadcast communication, so that the protocol does not want routing maintenance. Simply furthest vehicle will be scattered chosen as a convey vehicle and rebroadcast safety messages. Here exertion, we imagine that all vehicles have prepared with Global Positioning System (GPS) to recover their locations and sensors to verify for irregularity on vehicles. The vehicles are also implicit to have sufficient storage to store safety messages for redundancy check.

The proposed system will focus on QOS in routing the packets and propose a multi-cast routing protocol for priority based messages. Multicasting is a group communication. It involves few bandwidths than sending uni-cast messages to every person in a group. Multi-cast services comprise gradually used by different VANET applications like safety, dissemination of news and entertainment [7]. There is a force to extend QoS model with service differentiation for group applications in sorted to develop the network bandwidth assets efficiently. Priorities have been place based on the VANET applications. These propose system classifies the messages into three based on messages related to possibility of accidents, warnings and others. Priority number 1 is locate to be possibility of accident messages, 2 is set for warnings messages and 3 is set for other messages.

The advantage of this Prioritized routing protocol is to present Reactive routing protocols have not required to periodically deluge the network for updating the routing tables like table-driven routing protocols do. Vehicles are able to consume the Route Cache information efficiently to condense the control overhead. The initiator only tries to searching a route if truly no route is known (in cache). Current and bandwidth saving because there is no need for unnecessary message (beacon-less).

ALGORITHM

Priority based Routing Algorithm

In This algorithm the future protocol determined the path of emergency message to be prioritized and send to the priority vehicle from source to destination.

Step 1: Create the message based on priority as Qpri1, Qpri2, Qpri3 and stored in the queue of database.

Create priority Queue Qpri1, Qpri2, Qpri3

Step 2: Priority based message has been assign with the function int priority()

Step 3: Creation of priority message has encrypt the packet and send the encrypted message to RSU.

Void enqueue (packet pkt)

Step 4: Using if condition prioritized message will be set as priority number 1, 2 and 3 has stored in database

If pkt.priority = = 1

Add packet in the queue of priority 1 as Qpri1.append (pkt)

If pkt.priority = = 2

Add packet in the queue of priority 2 as Qpri2.append (pkt)

If pkt.priority = = 3

Add packet in the queue of priority 3 as Qpri3.append (pkt)

Step 5: After encrypte the message in queue, then decrypte the packet in queue

Void dequeue ()

Step 6: Using if condition check whether the packet priority is true or false

```
if  Qpri1.isempty()  = =  false
Then temppkt  =  Qpri1.removepkt ()
else if  Qpri2.isempty()  = =  false
Then temppkt  =  Qpri2.removepkt ()
else if  Qpri3.isempty()  = =  false
Then temppkt  =  Qpri3.removepkt ()
```

Step 7: If the packet priority number receive by OBU is true it send the ACK message to the sender else it sends the packet as send (temppkt)

Step 8: it return the priority to the enqueue database.

V. MODULES INVOLVED

In this fragment, VANET system has present to traffic obstruction in possible route to provide the shortest route. Since vehicle can reach the destination and the statement are control by network simulation. This stimulation will intend the system can be performed by the VANET modulation. The module has different enhancement flow such as Vehicle

International Journal of Engineering Applied Sciences and Technology, **2016**
Vol. 1, Issue 4, ISSN No. 2455-2143, Pages 69-74
Published Online January-February 2016 in IJEAST (http://www.ijeast.com)

Configuration Setting, Topology Design, RSU and OBU unit estimation.

5.1 MODULES DESCRIPTION

Vehicle Configuration Setting

The sensor vehicles are designed and configured enthusiastically, considered to employ across the network, the vehicles are set according to the X, Y, Z dimension, which the vehicles have the direct transmission range to all other vehicles.

Topology Design

This module is developed to Topology design all Vehicle place particular distance. Without using any cables then fully wireless mobile equipment based transmission and received packet data. Vehicle and wireless between calculate sending and receiving packets. The cluster head is at the middle of the round sensing area. Intermediary the sender and receiver of this networking performance on this topology.

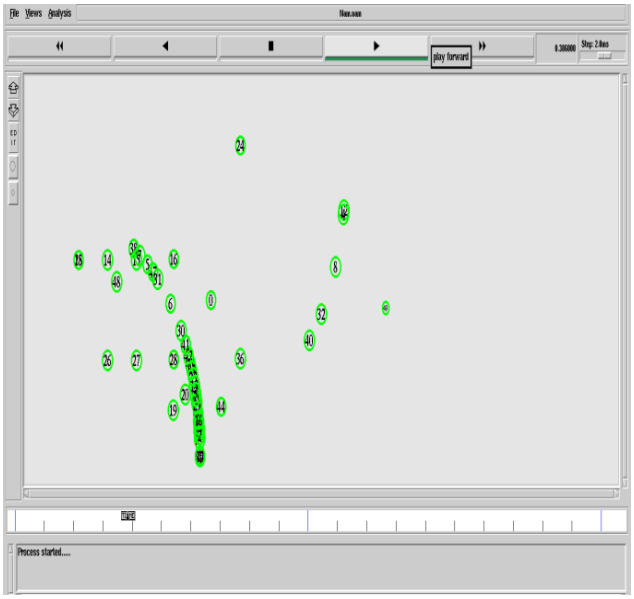
RSU and OBU unit estimation

The RSU (road side unit) is located across on road side, which is used to transfer the data packets to OBU unit. The OBU unit is installed on each vehicle which is act as a receiver medium of messages from road side unit. Both the RSU and OBU units are controlled and authenticated by access point

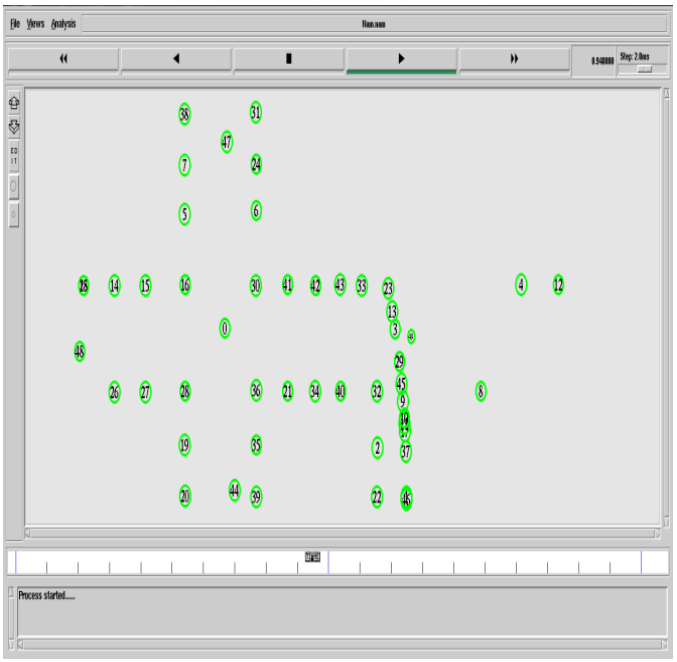
5.2 NETWORK SIMULATION METHOD

The Network Simulation in VANET has shown the out coming result of our project using the software tools. In this proposed work, we use NS-2 (version 2.28) for study the simulator. Network simulator (NS) is an object–oriented, distinct event simulator for networking research. This provides extensible support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The network topology will close to traffic source in each network entity to setup that the event should start or stop transforming the packet in certain region. The driver should setup the simulation by using OTCL script language. Compare to TCL, the OTCL language has more specific involvement. The Network Simulation produce more text based on the output file.

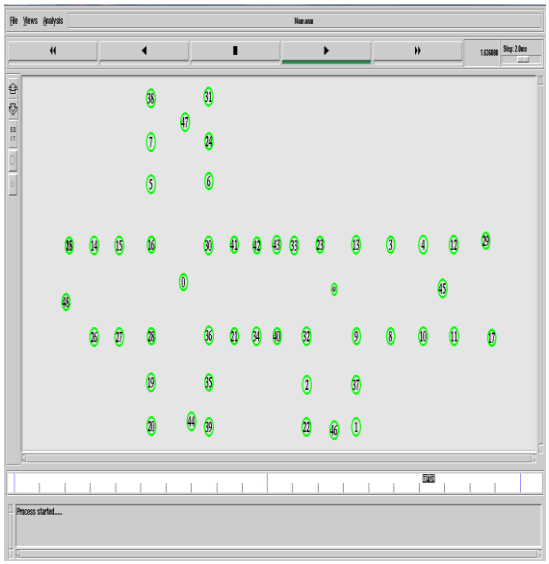
Using NS-2 tool we have to configure the vehicle setting, design the topology in their particular distance, without any wires the mobile equipment will transmit and receive the packet. In this Vehicle Configuration Setting, The sensor vehicles are designed and configured dynamically, designed to use across the network, the vehicles are set according to the X, Y, Z dimension. The vehicles have the direct transmission range to all other vehicles.



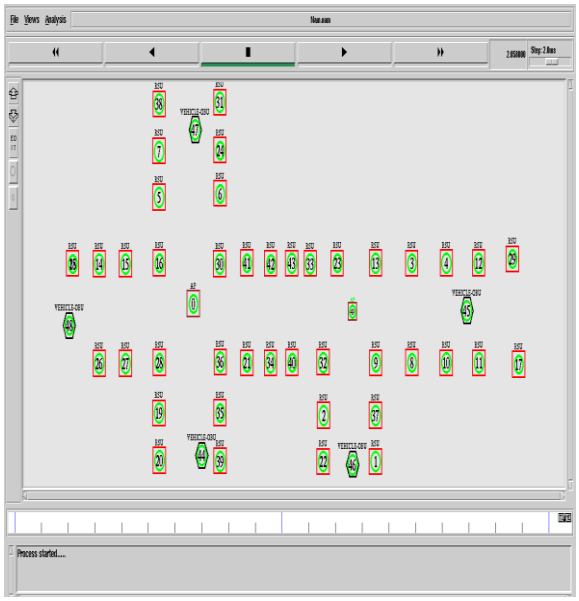
In this topology, design all Vehicle place particular distance. Without using any cable or wires the wireless mobile equipment will transmit and receive the packet data. Vehicle and wireless network also calculate sending and receiving packets.



International Journal of Engineering Applied Sciences and Technology, **2016**
Vol. 1, Issue 4, ISSN No. 2455-2143, Pages 69-74
Published Online January-February 2016 in IJEAST (http://www.ijeast.com)



In This RSU (road side unit) is placed across the road side, which is used to transfer the data packets to OBU unit. The OBU unit is installed on each vehicle is act as a receiver medium of messages from road sides unit. Both the RSU and OBU units are controlled and authenticated by access point.



VI. CONCLUSION AND FUTURE WORK

In this paper, we propose a Priority based Routing Protocol (PRP) for security messaging in VANET. PRP is fully distributed routing protocol. This multicast routing protocol is proposed with different priority based on the type of the messages. The priority messages in our system make a safe vehicular communication among the vehicles in network. Here we configure the vehicle setting and design the vehicle in particular distance and we establish the RSU and OBU. In the future work, we have to create vehicle and message in priority wise. Assigning priority provides a most efficient network communication on emergency condition, the collision, accidents are eliminated through our proposed protocol, and since priority assigning makes a packet collision in queue structure on emergency state. The protocol also achieves maximum message dissemination distance per hop (200- 250 m from 225 m) of communication range. So, the future research is concentrate on avoiding the packet collision in the RSU vehicles.

VII. REFERENCE

1. T.W. Chim, S.M. Yiu, Lucas C.K. Hui, "VSPN: VANET-Based Secure and Privacy-Preserving Navigation", IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 2014.
2. Venkatesh, AIndra, R Murali, "Routing Protocols for Vehicular Adhoc Networks (VANETs)", Journal of Emerging Trends in Computing and Information Sciences Vol. 5, No. 1, January 2014.
3. Rukaiya Y. Shaikh Int. Journal of Engineering Research and Applications Survey on "VSPN: VANET-Based Secure and Privacy-Preserving", Navigation Vol. 4, Issue 10 (Part - 5), pp.01-05, October 2014.
4. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan "Vehicular Ad Hoc Networks (VANETS): Status, Results, and Challenges" 2013.
5. Bharati Mishra, Saroj Kumar Panigrahy, Tarini CharanTripathy, Debasish Jena, and Sanjay Kumar Jena "A Secure and Efficient Message Authentication Protocol for VANETs with Privacy Preservation" World Congress on Information and Communication Technologies, Volume 11 – 14, December 2011.
6. G. Samara, W. Al-Salihy, and R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", Proc. IEEE Fourth Int'l Conf. New Trends in Information Science and Service Science (NISS '10), pp. 393-398, May 2010.
7. Alvin Sebastian, Maolin Tang, Yanming Feng, and Mark Looi "A Multicast Routing Scheme for Efficient Safety Message Dissemination in VANET", IEEE Wireless Communications and Networking Conference, April 2010.
8. M. A. Zayene, N. Tabbane, and R. Elidoudi, "Performance Evaluation of Greedy Perimeter Stateless Routing Protocol in Ad Hoc Networks", International Conference IEEE paper Nov 2009.