Cognitive VANET with Priority Scheme on the Basis of Transmission Range

Navjot Kaur, and Amanpreet Singh Dhanoa

Abstract- In Ad-hoc vehicular scenario the dedicated short size communication frequency. This does not provide sufficient spectrum for reliable exchange of safety and emergency messages to overcome this problem.In some cases if priority is not given then emergency messages do not reach to destination. So in the proposed work, cognitive network architecture is implemented to extend the control channel CCH used by vehicles to transfer safety and emergency massages to achieve this cooperative spectrum sensing scheme through which the network vehicle can optimize the available spectrum resource on that bandwidth. The CCH detect the vacant frequency and use them for transmission of safety and emergency messages. The vacant frequency has been checked by using the various approaches or by sending the one bit messages.

Keywords--- VANET, Priority Scheme, Transmission Range.

I. INTRODUCTION

A (**VANET**) uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns turn participating car into a wireless router or node which allowing cars 100 to 300 meters of each other to connect and create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile network is created. It is estimated that the first systems that will be this technology are police and fire vehicles to communicate with each other for the purpose of security [10].

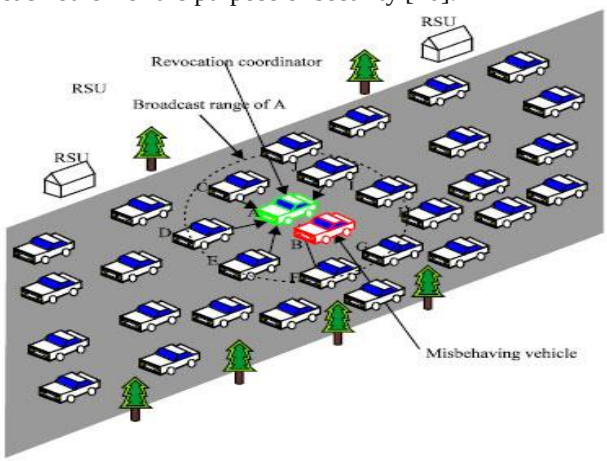

Fig 2: VANET

The connectivity is done among one vehicle to other vehicle and vehicle to road side infrastructure and vehicle or road side infrastructures to the central authority responsible for the network maintenance [8].

The basic tool for message transfer is the short range radios that are being installed in any of the nodes. The short transmission node is used by vehicular node. RSU's are spread sporadically or regularly depending on the deployment of the network in any particular region. In reality spread sporadically [13]. They act as an intermediary node between the Central Authority (CA) and

Vehicular Node (VN). Vanet-Vehicular Ad-Hoc Network is the network in which communication has been done between road side units to cars, car to car in a short range of 100 to 300 m. Existing authentication protocols to secure vehicular ad hoc networks raise challenges like as certificate distribution and revocation, avoidance of computation and communication bottlenecks, and reduction of the strong reliance on tamper proof devices [5]. In a VANET, vehicles will rely on the integrity of received data for deciding when to present alerts to drivers. This data may be used as the basis of control decisions for autonomous vehicles. If this information is corrupted, vehicles may present unnecessary or erroneous warnings to their drivers, and the results of control decisions based on this information could be even more disastrous. Information can be corrupted by two different mechanisms: malice and malfunction. Similarly, vehicles have two defense mechanisms: an internal filter and external reputation information [11].

A) Challenges in Vanet:

- A Speed-based Shortest Path Trip generation has been added. Accordingly, we can customize a threshold between high speed street segments and distance to the destination, which may generate a longer but faster path.
- Street Segments includes a speed limitation attribute. For TIGER files, we generate default values based on the State of California Current regulations, or let the user define them in an external file [12]
- Decoupling the multi-lane feature from the lane changing feature. When multiple lanes are available, each car chooses one lane and keeps it (if available) for the whole trip.
- New Randomized Dijikstra shortest path algorithm. The original Dijkstra's algorithm, given a start and an end point, always selects the same path, even in presence of multiple available paths with same weights. For traffic balancing, cars should be able to select different shortest paths [16].

B) Characteristics of VANET

VANET is an application of MANET but it has its own distinct characteristics which can be summarized as:

- High Mobility: The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy [2]. Rapidly changing

Navjot Kaur is a student of M.Tech (CSE Department). at Rayat & Bahra Institute of Engineering and Bio-Technology, Punjab, INDIA.

Amanpreet Singh Dhanoa is Assistant Professor of CSE Department at Rayat &Bahra Institute of Engineering and Bio-Technology, Punjab, INDIA.

- Network topology: Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.
- Unbounded network size: VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.
- Frequent exchange of information: The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent [12].
- Wireless Communication: VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication. Time Critical: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly [13].
- Sufficient Energy: The VANET nodes have no issue of energy and computation resources. This allows VANET usage of demanding techniques such as RSA, ECDSA implementation and also provides unlimited transmission power. Better Physical
- Protection: The VANET nodes are physically better protected. Thus, VANET nodes are more difficult to compromise physically and reduce the effect of infrastructure attack [16].

C) Security Requirements For VANETt

- **Authentication:** Authentication is a major requirement in VANET as it ensures that the messages are sent by the actual nodes and hence attacks done by the greedy drivers or the other adversaries can be reduced to a greater extent [3]. Authentication, however, raises privacy concerns, as a basic authentication scheme of attaching the identity of the sender with the message would allow tracking of vehicles. It, therefore, is absolutely essential to authenticate that a sending vehicle has a certain property which provides authentication as per the application. For example, in location based services this property could be that a vehicle is in a particular location from where it claims to be [5].
- **Message Integrity:** This is very much requires as this ensures the message is not changes in transit that the messages the driver receives are not false.
- **Message Non-Repudiation:** In this security based system a sender cannot deny the fact having sent the message. But that doesn't mean that everyone can identify the sender only specific authorities should be allowed to identify a vehicle from the authenticated messages it sends [4].
- **Entity authentication:** It ensures that the sender who has generated the message is still inside the network and that the driver can be assured that the sender has send the message within a very short period.
- **Message confidentiality:** It is a system which is required when certain nodes wants to communicate in private. But anybody cannot do that. This can only be done by the law enforcement authority vehicles to communicate with each other to convey private information. An example would be, to find the location of a criminal or a terrorist [4].
- **Privacy:** This system is used to ensure that the information is not leaked to the unauthorized people who are not allowed to view the information Third parties should also not be able to track vehicle movements as it is a violation of personal privacy. Therefore, a certain degree of anonymity should be available for messages and transactions of vehicles. However, in liability related cases, specified authorities should be able to trace user identities to determine responsibilities. Location privacy is also important so that no one should be able to learn the past or future locations of vehicles [16].
- **Real time guarantees:** It is essential in a VANET, as many safety related applications depend on strict time guarantees. This can be built into protocols to ensure that the time sensitivity of safety related applications such as collision avoidance is met [13].

D) Cognitive Radio

A cognitive radio is an intelligent radio that can be programmed and configured dynamically. Its transceiver is designed to use the best wireless channels in its vicinity. Such a radio automatically detects available channels in wireless spectrum, then accordingly changes its transmission or reception parameters to allow more concurrent wireless communications in a given spectrum band at one location. This process is a form of dynamic spectrum management [14]. In response to the operator's commands, the cognitive engine is capable of configuring radio-system parameters. These parameters include "waveform, protocol, operating frequency, and networking". This functions as an autonomous unit in the communications environment, exchanging information about the environment with the networks it accesses and other cognitive radios (CRs). A CR "monitors its own performance continuously", in addition to "reading the radio's outputs"; it then uses this information to "determine the RF environment, channel conditions, link performance, etc.", and adjusts the "radio's settings to deliver the required quality of service subject to an appropriate combination of user requirements, operational limitations, and regulatory constraints"[17].

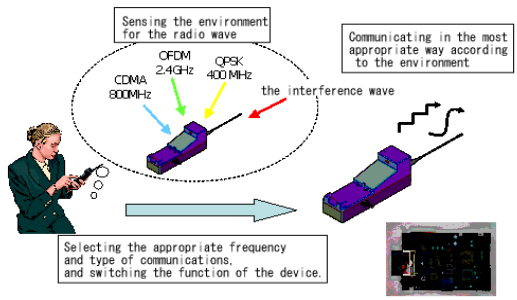

Fig 3 Cognitive Radios

Some "smart radio" proposals combine wireless mesh network—dynamically changing the path messages take between two given nodes using cooperative diversity; cognitive radio—dynamically changing the frequency band used by messages between two consecutive nodes on the path;

and software-defined radio—dynamically changing the protocol used by message between two consecutive nodes [8].

E) Spectrum Sensing

The important requirement of cognitive radio network is to sense the spectrum hole. Cognitive radio has an important property that it detects the unused spectrum and shares it without harmful interference to other users. It determines which portion of the spectrum is available and detects the presence of licensed users when a user operates in licensed band. The spectrum sensing enables the cognitive radio to detect the spectrum holes. Spectrum sensing techniques can be classified as frequency domain approach and time domain approach. In frequency domain method estimation is carried out directly from signal so this is also known as direct method. In time domain approach, estimation is performed using autocorrelation of the signal [9].

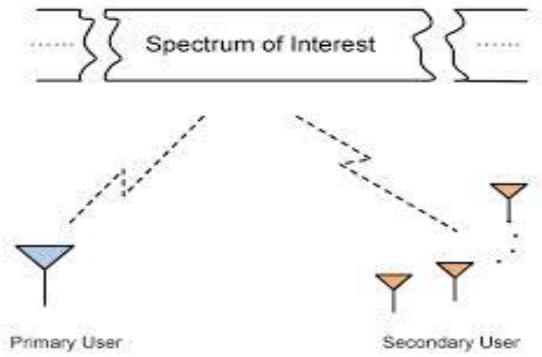

Fig 4 spectrum sensing

Another way of categorizing the spectrum sensing and estimation methods is by making group into model based parametric method and period gram based nonparametric method .Another way of classification depends on the need of spectrum sensing as stated below.

a) Spectrum Sensing For Spectrum Opportunities

- Primary transmitter detection: In this approach, detection of a signal from a primary transmitter is based on the received signal at CR users whether it is present or not. It is also known as non-cooperative detection. This method includes matched filter based detection, energy based detection, cyclo stationary based detection, and radio identification based detection [4].
- Cooperative or collaborative detection: It refers to spectrum sensing methods where information from multiple Cognitive radio users is incorporated for primary user detection. This approach includes either centralized access to the spectrum coordinated by a spectrum server or distributed approach. Spectrum sensing for interference detection [10]
- Interference temperature detection: In this method the secondary users are allowed to transmit with lower power then the primary users and restricted by interference temperature level so that there is no interference. Cognitive radio works in the ultra wide band (UWB) technology.

Primary receiver detection: In this method, the interference and/or spectrum opportunities are detected based on primary receiver's local oscillator leakage power.

II. Related Work

This work will be done by using network simulator NS2. This work will be completed in three phases which are given below.

- In first phase ad-hoc network will be created by initializing number of nodes and then cognitive network will be implemented in which spectrum sensing is done. Spectrum sensing is done to know about the free bands so that they can be utilizing to send emergency messages.
- In second phase bandwidth of channel will be increased so as to avoid congestion and avoid loss of important data. In this phase transmission range to nodes will also be calculated.
- In third phase priority will be given to vehicles. High priority will be given to those vehicles which will be close to their destination or can be said that which will be in transmission range.

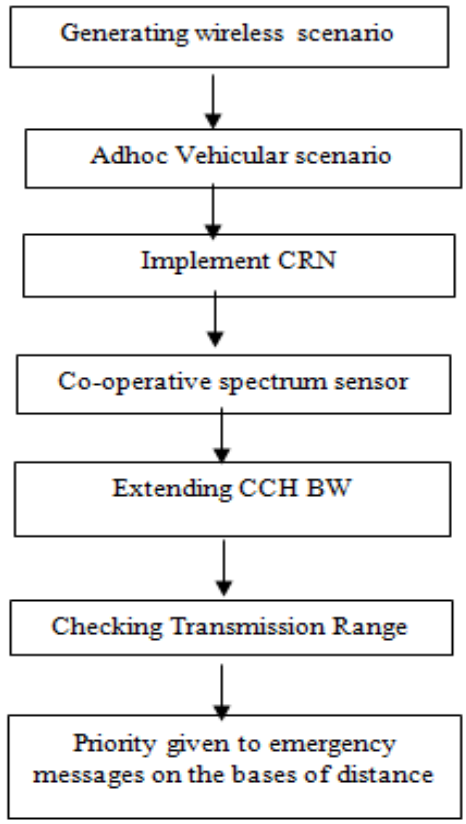

Fig. 5: Flow of Work

III. RESULTS AND DISCUSSION

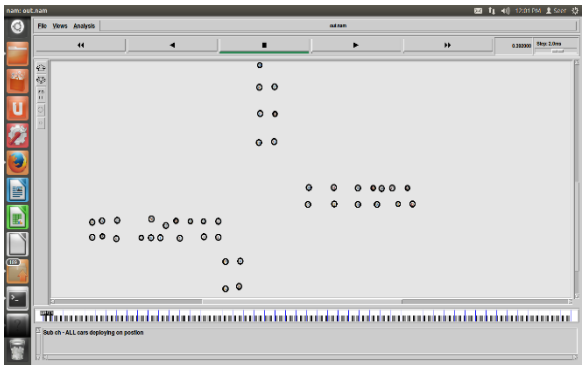

Fig 6. Initialization of nodes

In this figure the nodes are arriving from different locations like up, down, left, right and all are approaching in the center.

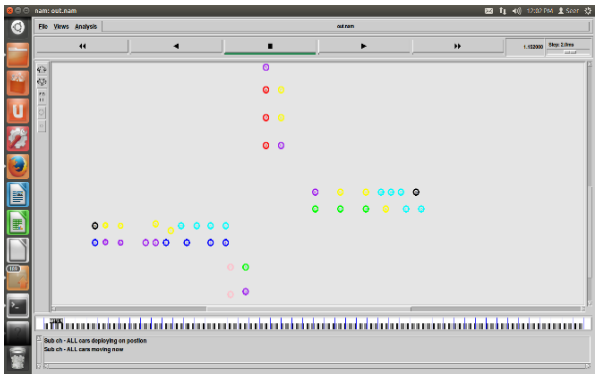

Fig 7. Movement of nodes

In the figure the cars in the lane right and left are moving and upper and lower nodes have to stop because for them the signal is red.

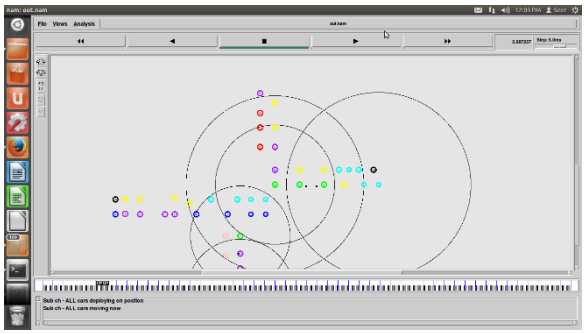

Fig 8 Representing communication between nodes

The figure represents the nodes are communicating with each other.

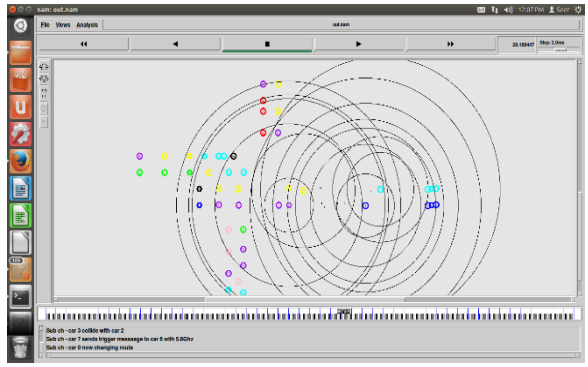

Fig 8 Representing congestion

This figure represents the nodes are moving and at one point the nodes collides and congestion occurs at that point.

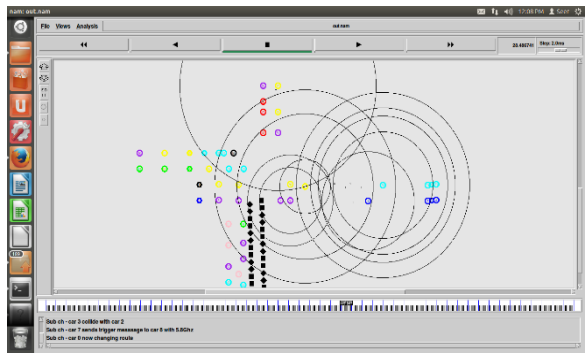

Fig 9 Representing packet drop

This figure represents some cars reach out of range so packet starts dropping at that point.

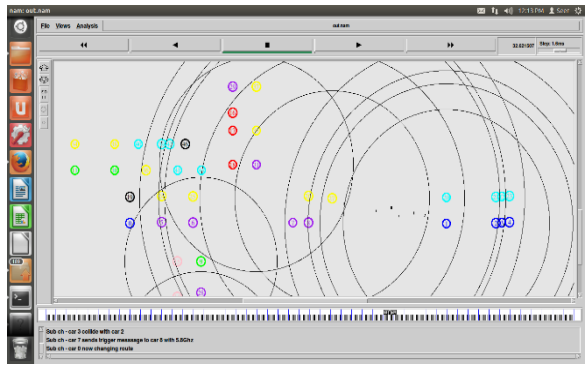

Fig 10 Representing Message passing

This figure represents that the car that got into the range of the collided nodes starts sending alert messages to the nodes coming in the same direction. Here on the basis of distance, highest priority is assigned to the node with least distance.

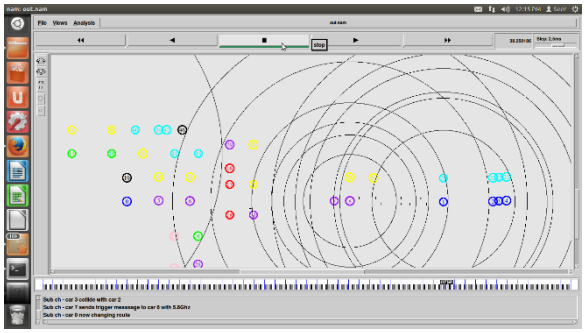

Fig 11.Representing communication on the basis of priority

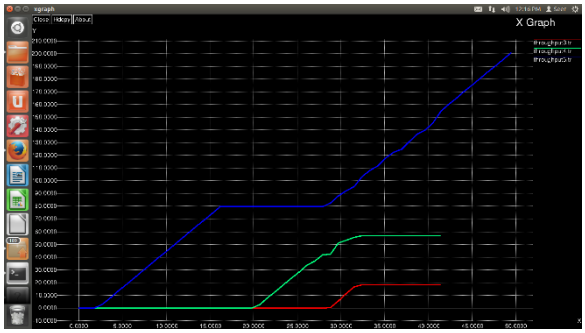

Fig 12 Throughput for 30, 40 and 50 nodes resp.

Throughput is total number of successful bites received. This graph represents throughput.

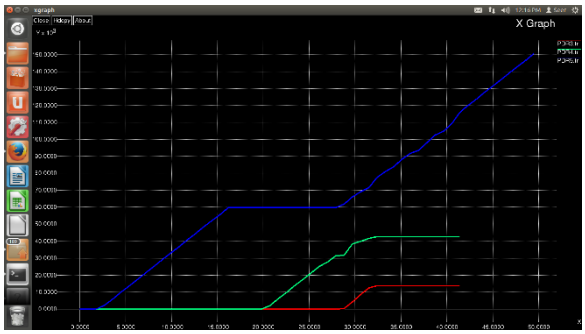

Fig 12 Representing PDR

This figure represents PDR (Packet delivery ratio).

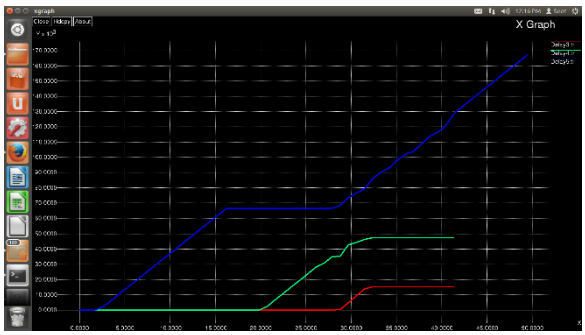

Fig 13 Representing Delay

This figure represents end to end delay of nodes. The red line representing 30 nodes is having the minimum delay so it is better than the other two.

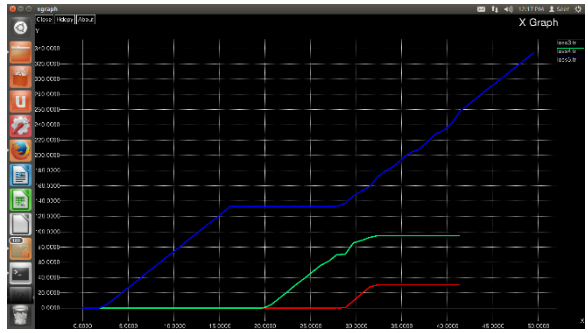

Fig 14 Representing Loss

This figure represents that the results with 50 nodes is having the greatest loss hence, the 30 nodes are considered the nodes giving best results.

IV. Conclusion

A VANET uses cars as mobile nodes in a MANET to create a mobile network. A cognitive radio is an intelligent radio that can be programmed and configured dynamically. In Ad-hoc vehicular scenario the dedicated short size communication frequency. This does not provide sufficient spectrum for reliable exchange of safety and emergency messages to overcome this problem. cognitive network architecture is implemented to extend the control channel CCH used by vehicles to transfer safety and emergency massages to achieve this cooperative spectrum sensing scheme through which the network vehicle can optimize the available spectrum resource on that bandwidth. The CCH detect the vacant frequency and use them for transmission of safety and emergency messages. The vacant frequency has been checked by using the various approaches or by sending the one bit messages

References

[1]. Ali J. Ghandour a, Kassem Fawaz a, Hassan Artail a, Marco Di Felice b, Luciano Bononi "Improving vehicular safety message delivery through the implementation of a cognitive vehicular network", 5643-8425, 123-765, IEEE, 2013

[2]. Srikanth Pagadarai "Characterization of Vacant UHF TV Channels for Vehicular Dynamic Spectrum Access", ISSN 978-1-4244-5685-7, PP 1 – 8, IEEE, 2009.

[3]. Marco Di Felice"Cooperative Spectrum Management in Cognitive",ISSN 978-1-4673-0049-0,PP 47 – 54,IEEE,2011.

[4]. Alexander W"Impact of Mobility on Spectrum Sensing in Cognitive Radio Networks", ISSN 978-1-60558-738-7/09/09,IEEE, 2009.

[5]. Wooseong Kim "Co Route: A New Cognitive Any path Vehicular Routing Protocol", ISSN 978-1-4577-9538-2/11, IEEE, 2011.

[6]. Ali J. Ghandour"Data Delivery Guarantees in congested Vehicular Ad hoc Networks using cognitive networks" ISSN 978-1-4577-9538-2/11, IEEE, 2011.

[7]. Dusit Niyato"Optimal Channel Access Management with QoS Support for Cognitive Vehicular Networks", 573-591, IEEE, 2011.

[8]. Xiao Yu "A Novel Sensing Coordination Framework for CR-VANETs", ISSN 0018-9545/, IEEE 2012.

[9]. Kazuya Tsukamoto "On Spatially-Aware Channel Selection in Dynamic Spectrum Access Multi-hop Inter-Vehicle Communications" ISSN 978-1-4244-2515-0, IEEE, 2009.

[10]. Husheng Li and David K. Irick "Collaborative Spectrum Sensing in Cognitive Radio Vehicular Ad hoc Networks: Belief Propagation on Highway", ISSN 978-1-4244-2519-8, IEEE 2010.
[11]. Qi Chen **"**Overhaul of IEEE 802.11 Modeling and Simulation in NS-2", ISSN 978-1-59593-851, IEEE, 2007.
[12]. Hussain, R. "Rethinking Vehicular Communications: Merging VANET with cloud computing", 978-1-4673-4511-8, IEEE, 2012.
[13]. RoselinMary, S. "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)", 978-1-4673-5786-9, 237 – 240, IEEE, 2013.
[14]. Janech, J. "Comparation of Strategies for Data Replication in VANET Environment", 978-1-4673-0867-0, 575 – 580, IEEE, 2012.
[15]. Ebers, S. "Short paper: Collaboration between VANET applications based on open standards" 14114519, 174 – 177, IEEE, 2013.