Multicast and Unicast Communication in Vehicular Network Using IPv6.

Uma Nagaraj[1], Deesha G.Deotale[2], Sumit A.Khandelwal[3]
[1,3]Department Of Computer Engineering, MIT Academy of Engineering, Alandi, Pune India
[2]Department Of Computer Engineering, G.H.R.I.E.T.Wagholi,Pune , India

Abstract**:** *Now a days the research is going on in Vehicular ad-hoc network to make a city as Smart city for the driver and passengers to navigate and to obtain relevant information and avoid the traffic accident. In the proposed system we discuss the different ways of communication for transferring or exchanging the information between the system available in the vehicle and infrastructure. Here we concentrate on the Multicast communication using Internet protocol version 6(IPV6) for faster transferring information to more system as compared with the unicast communication.*

Keywords: *IPv6, Multicast, unicast,OBU,RSU*

I. INTRODUCTION

We see that in current days Vehicle network providing connectivity among vehicle travelling along the road. Internet has created new ways for personal communication and offer and worldwide access to relevant information. Now a day people used the internet mainly in office, home or anywhere and after some years with the deployment of new wireless network technology and new terminals, the internet will “go mobile”. The convergence of cellular network and internet make information instantly available anytime and anywhere. Internet based personal wireless communication to/from cars would greatly enhance the driving. So that driver and passenger to navigate and to obtain relevant information. The goal is to improve safety and traffic efficiency in the city. Thus the government, car manufacturers and telecommunication players are working together towards the definition of new communication standard that enables driver it take advantages from the improved capabilities.

The most commonly considering application are related to increasing traffic yields and safety spatially collision warning system and intelligent vehicle navigation. In the proposed system we discuss the how IPv6 used in vehicular network and how to convert currently use of IPv4 to IPv6. The communication is done through vehicular network with the internet and provides the global connectivity inside the vehicle so that it provides classical and new internet application. Means internet based wireless communication and ad-hoc network would greatly enhance driving. The example is that to offer the service for driver to include relevant traffic and parking information, which are combined with route guidance. To provide classical and new internet application increase the adoption of vehicle communication system by the user because they will see and added value from the installation of such devices inside their vehicle.

II. BASIC CONCEPT OF IP ADRESS

The current version of the Internet Protocol is IP version 4. All devices in the IPv4 network are identified by 32-bit IP addresses, giving an address space of 2^{32} addresses. However, parts of the address space are reserved for special use, which reduces the size of the usable address space. The size of the address space limits the number of devices that can be connected to Internet. The remaining IPv4 address space is decreasing at a fast pace. One of the reasons for starting the development effort was the projected shortage of IPv4 addresses. The new version of the protocol, Internet Protocol version 6 (IPv6), provides a significantly larger address space of 2^{128} addresses [4,24].

However, the differences between IPv4 and IPv6 make them incompatible with each other. Direct communication between IPv6 and IPv4 devices is not possible, if the IPv6 device is not also connected to the IPv4 network. The issue causes the existing IPv4 services to be unavailable in an IPv6-only network. Communication between two devices, connected only to IPv6 and IPv4 networks respectively, is not possible without an intermediary, which does the required translation between the protocols. The indicated lack of IP addresses has thus been the main motivation for the introduction of a new Internet Protocol, namely IPv6 [4], besides its expanded addressing capabilities, IPv6 also supports:

- addressing flexibility (e.g., multiple addresses on one port, addresses are leased),
- Simplified structure of IP packet (e.g., improvements in the IP header: no checksum; extension headers),
- Auto configuration mechanisms,

- Mobility support (Mobile IP),
- Security capabilities (IPSec),
- Quality of service for real {time applications, and
- Utilization of multicast instead of broadcast.

III. CONNECTION VANETS TO THE INTERNET

To connect VANETs to the Internet, vehicles have to be provided with a full Internet Protocol (IP) stack, as IP is the basic building block for Internet communications. We can identify three main functionalities required to bring IP into the vehicular networks: (a) the capability of vehicles to auto configure an IP address, (b) IP mobility mechanisms suited for vehicular scenarios, and (c) mechanisms for an efficient transmission and forwarding of IP datagram's within the vehicular network. The auto-configuration of IP addresses by nodes of a VANET. IPv6 provides some standardized mechanisms of IP address auto-configuration, both stateless [20, 21] and stateful [22] that cannot–or at the very least are hard to–be applied without any modification in vehicular environments [23].

IV. COVERSION OF IP ADDRESS

In the IPv6 concept used in proposed system because in the world wide or city have no of vehicles and they communicate to each other, it required unique identification ID (IP address) for finding out the Vehicle(s). so the address capability of the IPv4 is not good(i.e. limited address capacity) Vehicular network , so that we used the concept IPv6 next version of IPv4, it's have 2^{128} address space this is good for vehicle network to allocate the unique address to vehicle. But the now we used the IP address version 4 i.e. IPv4 address so simply to convert this IPv4 address to new Version IPv6 as well as solve the some problems like in the proposed system address space and time.

There are two different techniques to convert the IPv4 address to IPv6 address. Firstly represent Decimal number IPv4 address to Binary representation then convert it into IPv6 address and another one is using directly the decimal num of IPv4 address to convert it into IPv6 address. We see both conversion step by step representation of IPv6 Address. The two methods of IPv4 address to IPv6 conversion as shown in fig (1)). In the proposed system used the one of the method of conversion.

- Example of first method:

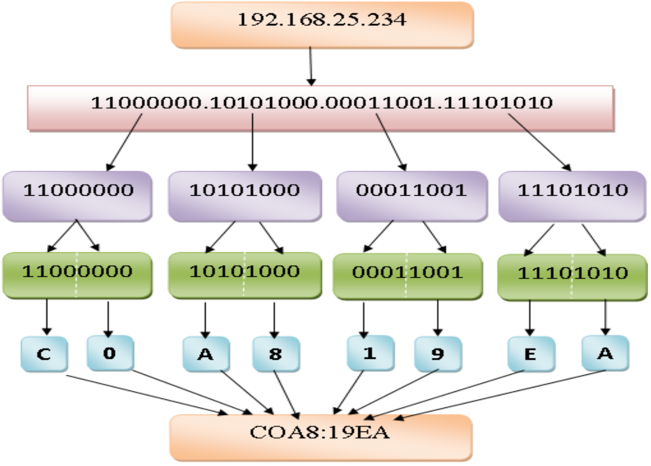


Fig 1- IPv4 to IPv6 Conversion Method1

In this method firstly to convert the Decimal IPv4 address in to Binary representation, then divide this Binary representation into four groups each group have the 8 bit binary number divide this binary number in two parts i.e 4 bits then convert this 4 bit into hexadecimal number representation . we get hexadecimal number i.e. 8 hexadecimal number then group in to two parts i.e. 4 hexadecimal in in one groupi.e 16 bit binary number in the one group in IPv6 address. So we get two group out of 8 group of IPv6 address with the help of IPv4 address. This method used in the proposed system .

- **Example of Second Method:**

In the second method how to convert the IPv4 address into IPv6, we see in details as follows: Firstly IPv4 address in the decimal form in 4 group separate all the octets of IPv4 address then divide this by 16 to each octets.ing after dividing save quotient and remainder of the divide number. First write the quotient and reminder then convert this number into hexadecimal number so after conversion we get the 8 hexadecimal number then merge them into IPv6 address form i.e. getting two group out of 8 group of IPv6 address and each group have 4 hexadecimal numbers

V. COMMUICATION PATTERN

Two devices on an IP network communicate with each other using Unicast. Unicast communication is one-to-one communication. In Unicast communication there is a single sender and receiver for each packet. Each packet is received by a single host in the network. Unicasting the same data to several devices in the network requires sending the data to each receiver separately. Consequently, as the number of receivers increases, more packets have to be sent to reach all the receivers. Sending the same data multiple times increases also the load on the sending machine. Sending data to a large number of receivers at the same time might not be possible due to insufficient transmission capacity in the network. Multicasting alleviates the aforementioned problems by transmitting the same data to a group of devices in the network. Multicasting provides a one-to-many sending method. The sender has to send the data only once. For each packet there can be an unlimited number of receivers.

The Multicasting is the ability of communication network to accept a single message from an application and to deliver copies of the message to multiple recipients at different location. Two important concepts in multicasting:

- Multicast routing Algorithm
- Multicast routing protocol

Communication network can be classified into two categories local area networks and Wide area networks. A local area network spans a small geographical area, while wide area network span a large geographical area.

VI. MULTICAST GROUP ADRESSING

Both IPv4 and IPv6 differentiate multicast group addresses from Unicast addresses by their prefix. Using the Classless Inter-domain Routing (CIDR) prefix notation [28], IPv4 uses addresses in 224.0.0.0/4 prefix as multicast group addresses [6]. Similarly, IPv6 addresses in FF00:: /8 prefix are reserved for multicast [8]. However, not all multicast addresses are used in a similar way. The addresses are used in either

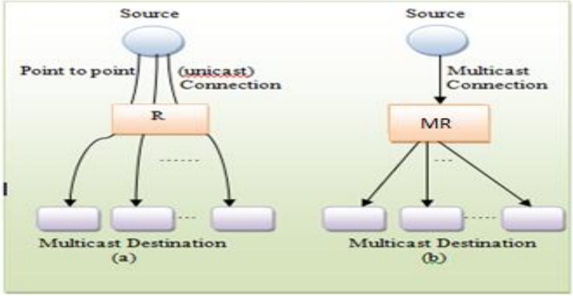


Fig (2) – (a) Any-source multicast (ASM), (b) Source-specific multicast (SSM).

Any-source multicast (ASM) as the name implies, any host on the network can send packets to the multicast group. Because any host on the network can send to an ASM group, the ASM group address space is shared by all hosts on the network. Any-source multicast (ASM) allows sending IP packets to a group of zero or more hosts. The group of hosts is identified by a multicast group address, which is used as the destination address in IP packets [5, 6].

Source-specific multicast (SSM) [9] specifies each multicast group as sender-group pair (S, G). The SSM sender-group pair is called a channel to distinguish SSM from ASM. IPv4 multicast addresses in the prefix 232.0.0.0/8 and IPv6 multicast addresses in FF3x :: /96 are reserved for SSM (x = 0...F). Joining an SSM channel requires specifying the source address S, in addition to the multicast group address G. When listening to an SSM channel, the listener receives only packets sent by source S. Thus, only a single host is able to send packets to the channel, putting each sending host in control of its own group address space.

VII. MULTICAST LISTENER DISCOVERY

The Multicast Listener Discovery (MLD) [10] is the IPv6 counterpart to IGMP [13]. The current version of the protocol is MLDv2, which is interoperable with older MLDv1 [15]. MLD used by IPv6 hosts and routers to transmit multicast group membership information. MLD essentially an adaptation of IGMP from IPv4 to IPv6. Despite the similarities, there are, however, some differences between IGMP and MLD.

As opposed to IGMP, MLD is not implemented as a separate protocol on top of IP. MLD is a sub-protocol of ICMPv6 [16]. Additionally, because multicast and MLD are used in IPv6 neighbor discovery [18], MLD support is required in all IPv6 systems.

As IPv6 specifies separate scopes for multicast addresses [12], MLD Membership Reports are not sent for all multicast groups. The Membership Reports are omitted for the node-local scope, since packets sent to those groups cannot appear outside an IPv6 node. Membership reporting is also omitted for the link-scope all-nodes multicast address, FF02::1, to which all IPv6 systems always listen.

IPv6 Multicast is relied on the group management mechanism over an IPv6 link. This is defined by the MLD protocol. Multicast routing protocols such as PIM rely on a multicast distribution tree for delivering packets from the source to the receivers. To build such a tree, the protocol defines a set of signaling messages and operations between the multicast routers, the RP and the multicast source. The MLD Forwarding Proxy [RFC 4605] is a simplified approach of multicast. It is mainly used to avoid the deployment of multicast routers in the same network domain. Each router is an MLD Forwarding Proxy. Only, the border router is Multicast router connected to the multicast infrastructure. This approach relies on a spanning tree which connects the routers of the same network domain to the border router considered as a root of the tree.

VIII. COOPERATIVE ITS SYSTEM

The Intelligence Transportation System (ITS) information is shared between the applications providing its services in a single ITS station and those running in different ITS stations. Cooperative - ITS have the following features:

- The sharing of information between applications in a single ITS station
- The sharing of information between any ITS station(Vehicle, Roadside, Central and Personal)
- The sharing of resources (communication, positioning, security, ...) by applications in an ITS station
- The support of multiple applications running simultaneously.

Cooperative ITS system generally spread in three categories: Road safety, Traffic efficiency and other application. In road safety include both applications such as emergency braking or lane departure notification which require short range time-critical for immediate actions from the vehicles, and longer-range applications such as road hazard events (black ice, vehicle in the wrong direction, road work which require non time critical communications(short, medium and long range). In traffic efficiency include road itinerary planning, green wave, road diversion and require constant exchange of information between vehicles and roadside infrastructure as well as some traffic information servers. Last to provide a better transportation experience to the road users.

They thus include comfort and infotainment applications. ITS communication architecture suitable for a variety of communication scenarios (vehicle-based, roadside-based and Internet-based) through a diversity of access technologies (802.11p, infra-red, 2G/3G, satellite, ...) and for a variety of application types (road safety, traffic efficiency and comfort / infotainment) deployed in various continents or countries ruled by distinct policies.

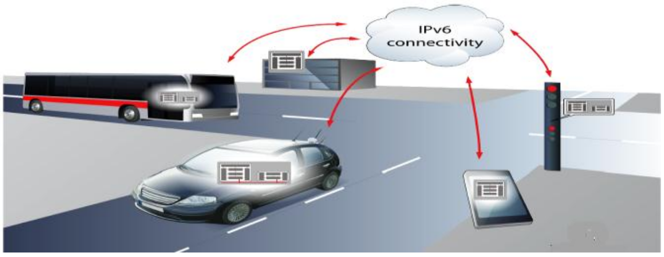


Fig 3- ITS Stations Communicating Using IPv6 Using Various Access Technologies

The time ITS services requiring the use of the public IP addresses appear on the market, there won't be enough public IPv4 address available. The use of this version of IP scales to meet the addressing needs of a growing number of vehicles and connected devices, and provides the added functionality necessary in mobile environments. Relying on IPv6 in their ITS communication architectures, ISO followed by ETSI, Come Safety and the Car-to-Car Communication Consortium have thus taken right decision to guarantee sustainable deployment of C-ITS. IPv6 has potential to decrease accident rates by enabling transmission of safety critical information. Once the safety benefit of IPv6 is acknowledged, there are classical ways of calculating the economic impact of reducing road fatalities.

IX. MULTICAST ALGORITHM

The communication is done between the sender and receiver. Algorithm for both sender and receiver as follows:

Sender:

1. Something happen on the road it *S* generates a packet *P*
2. Then sets the destination geo-area. The distance in the extended header (Distance)is set to the area circle radius

3. The latitude(x) and longitude (y) fields are set to the area center of coordinates.
4. If *Dist(S, D) ≤ R* (i.e. S belongs to the destination geo-area), then *S* sends out the packet in a broadcast mode,else (i.e. S does not belong to the destination geo-area), the packet should be forwarded towards D.

   In this situation S proceeds as follows:

   If there are neighbors available around, then for each neighbor.
   - Calculate *Dist (I, D)*, and then send the packet *P* to the neighbor i which corresponds to shortest distance *Dist (i, D)*, where *Dist (i, D) < Dist(S, D).*
   - else put P in the store and forward buffer , Where *Dist (i, D) < Dist (F, D).* The position vector in the common header of *P* is updated with the *j*' position information before retransmitting *P*.

Receiver:

1. Node *j* receives through a forwarder *F* a Geo Broadcast packet *P* which has been initially sent from a source node *S*.
2. The packet P is destined to all nodes located within a geo-area of rectangular shape with *D* as center. *j* proceeds as follows:
   - If security check is failed, then *P* is dropped.
   - *j* checks either the same packet *P* has not been processed previously by checking the matching of Source node ID and Timestamp value. If the packet *P* has been already processed, then it is dropped.
   - *j* updates its location table by updating/adding the two entries that correspond to *S* and *F* respectively.
   - If *j* does not belong to the destination geo-area, it shall drop any packet which comes from a forwarder which is located inside the destination geo-area. So if *Dist (F, D) ≤ R* and *Dist (j, D)>R*, then *P* is dropped.
   - Else, if *Dist (j, D) ≤ R* then *j* is considered as destination. Therefore *j* delivers the payload of *P* to upper layer, and then sends out the packet in a broadcast mode.
   - else, if *Dist(F, D) > R*, the packet should be forwarded towards *D*.

The IPv6 Multicast communication process is representing mathematically in vehicular network. *S = {I, O, P, Vehicle, RSU, Internet Φ}* Where, *S* be the system defined for the vehicle (user) in VANET, System components are vehicle, RSU, Satellite/GPS, Internet. Road Side Unit (RSU) to transmit the data (packets) from the vehicle to another RSU or vehicle or satellite. Internet avail the facilities like Web access, entertainment based services to the users in Vehicle. Inputs are Geographical coordinate of the vehicle & warning message *I={ VP1,VP2,VP3……....∞}* where, *VPi ={Lati , Longi }* longitude and latitude information of vehicle position. The outputs are the different communication Unicasting and multicasting. *O= {GUM1, GBM1}* Where, *GBM=0* on failure *GBM=1* on success, Geo-broadcast message GBM – Geo-Broadcasting message or IPv6 Multicast Message. The Data packet generated between RSU & vehicle or RSU to CU and vice versa. *P ={P1,P2,P3,P4,…………………..∞}* Vehicle (User)→Vehicle equipped with transceiver *V={V1,V2…………Vn}* RSU→ Road Side Unit (RSU) to transmit the data (packets) from the vehicle to another RSU or vehicle or satellite *RSU={RSU1, RSU2,……..RSUn}* Internet = To avail the facilities like Web access, entertainment based services to the users in vehicle *Φ→f(I)=0* Function which map input to desire output.

Transmit (Veh_id, Veh_pos, Msg):-Transmits the details to the nearest RSU or Vnode.
Receive (Veh_id, veh_pos, Msg):- Receive the details from nearby RSU or Vnode.
Request **(***Veh_pos, Request_content):-* Request to the satellite or RSU to get Geographical information. *Response (Veh_pos, resp_result):-* Response to the vehicle which requested the geographic information.

X. IPv6 Contribution in GeoNetwork

Safety and non-safety application vehicles exchange the information with other vehicles and road side infrastructure and avoiding the traffic accidents. Geo Networking is a geographic addressing and routing protocol originally defined by the Car-to-Car Communication Consortium (C2C-CC) and allowing non-IP multi-hop communications between vehicle and roadside ITS stations attached to the same vehicular ad-hoc network. Position-based routing or geographic routing (geo networking) makes a forwarding decision based on the geographic location of communication peers such as source, destination and neighbors. The support of IPv6 (Internet Protocol version 6) in VANETs is necessary. With IP, all types ITS applications can be accommodated and legacy Internet applications can be brought to vehicles. Applications are run transparently over diverse underlying communication medium which can be replaced as technology improves. More importantly, IP enables interoperability of ITS communication systems with other communication systems. The combine both IPv6 and geo-network into a common ITS communication system [19]. Architecture IPv6 Geo-Networking and allows to perform IPv6 communication over a multi-hop network made of forwarding vehicle and roadside ITS stations. It requires the encapsulation of IPv6 packets within Geo Networking packets. an ITS station to broadcast time-critical safety information's to all ITS stations located in a given geographic area, either immediately located around the sending ITS station or located in a remote area defined by geographical coordinates (e.g. a roadside ITS station informing approaching vehicles located at some distance that there is black ice). The combination of IPv6 with Geo-Networking into a single protocol stack has been defined by the GeoNet (IPv6 Geo-Networking) FP7 European Project (2008-2010).The ITS stations are as follows: ITS station located in a vehicle i.e. vehicle ITS Station. ITS station located in the roadside infrastructure i...e. Roadside ITS Station, ITS station located in the central infrastructure i.e. Infrastructure ITS station.

XI. SYSTEM ARCHITECHTURE

A typical road safety use case where IPv6 is applied shown in Fig 4. A Vehicle A detects black ice on the road. As an immediate action, the traffic hazard application running on Vehicle A informs all the vehicles driving immediately behind it about this traffic hazard and the information is broadcasted (Geo Broadcast) from vehicle to vehicle within a limited geographical area. As a result the message reaches Vehicle B which further broadcast the same message to other vehicles and the message reaches vehicle C.

This road hazard information is going to be valid for some time and vehicles not immediately following but heading to the same spot could benefit from this information too. Vehicle A would thus send this information to a traffic control center server located in the Internet, through the Internet access provided by a roadside ITS station (RSU1 on the Fig. 3). IP - thus IPv6 - must be used in such a case. Vehicle A transmits this information using IPv6 Unicast [1] through RSU1, either directly as shown on the figure or through intermediate vehicles in case Vehicle A is not anymore in RSU1's radio range.

In this latter case, the notification would forward from vehicle to vehicle until it reaches a node connected to the Internet. The traffic control center server receives this information and consolidates it with information received from various source.

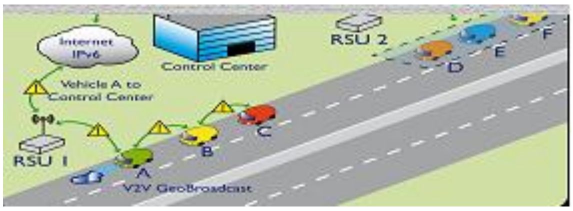


Fig 4 - IPv6 Scenario

If appropriate, it periodically transmits road hazard information to all vehicles in some specific geographic area. The black ice report only concerns vehicles heading to specific point on a specific road. The server

Would thus send an IP packet using IPv6 multicast [1] to a roadside ITS station (RSU2 on the Figure9) known to serve the geographic area where the information should be distributed. Once this information is received, RSU2 would in turn broadcast (Geo - Broadcast) it to all vehicles in the specific geographic area. Vehicle E would get the packet first and would retransmit it to other vehicles (i.e. Vehicles D and F).

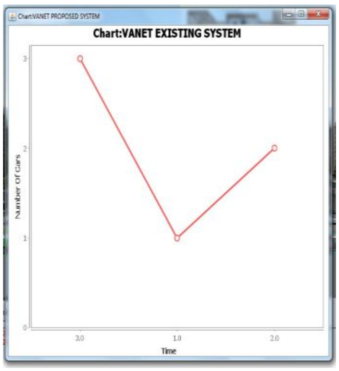
To transferring the information from source to destination each system maintains the information. Road side unit maintain the information like IPv4 address and IPv6 address of Vehicle, location, event message, port number etc. central unit maintain the information in tabular format i.e. IPv6 address of Roadside unit available in the in the area of that city, port number and location .

XII. COMPARE UNICAST AND MULTICASTCOMMUNICATION

In the proposed system we used both communication patterns for achieving the goal. And performing Communication between a single communication endpoint with another single communication endpoint .Is the Unicast communication means one receiver and one sender message is transfer to behind the vehicle using geographical location of vehicle A. Within the range of vehicle A come another vehicle B it send the message from vehicle A to B then same concept is repeated and stop when no vehicle come within range of vehicle that sending message to next.

The multicast source relies on multicast-enabled routers to forward the packets to all client subnets that have clients listening. There is no direct relationship between the clients and Windows Media Server. The communication is done one too many i.e. single communication endpoint with multiple communication endpoints. Multicast communication is that means one sender and multiple receivers. One copy of message send to all receiver come within geographical area.

The multicasting is better because it takes less time to sending message to group of vehicle but in unicasting it takes large time. In Unicast communication one to one send the packet not to all at the same time. In Multicast Packet delivery ratio is increase in communication as compared to Unicasting and also increases the throughput of multicasting. Multicasting can allow reaching many end users while utilizing only one data stream, decreasing the amount of bandwidth and saving cost compared to Unicast.



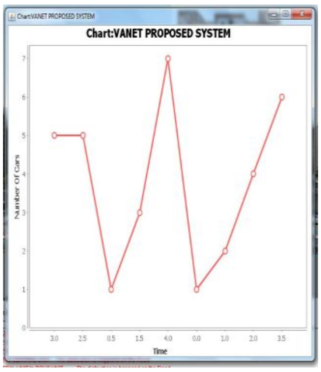


Fig 5- Unicast communication i.e. one to one communication.
Fig 6- Multicast communication using Geoarea.

Multicast only requires one stream to serve many end users. Unicast requires a single stream for every user served, which means much more bandwidth is used. Multicasting utilizes one data stream to serve hundreds or thousands of end user. Unicasting requires more bandwidth for every end user added clogging up a network and increasing the cost, if Unicast used to support group communication then two Unicast communication relationships have to be established between two members in a group. The number of transmissions for a packet delivery linearly increases with group size. Since there is no scalability with respect to group size, Unicast communications not feasible option for large groups. When compared to traditional IP Unicasting and broadcasting, IP multicasting is more efficient and economical, consumes less bandwidth and processing power, scales better, and does not lead to network congestion as the number of clients grows. Multicasting operates over any network technology that can support Transmission Control Protocol/Internet Protocol (TCP/IP), including Ethernet, Asynchronous Transfer Mode (ATM), frame relay, and satellite .When compared to existing i.e. Unicasting system with the proposed system i.e. multicasting, The graph of Unicast communication is shown in Fig 5 & Fig 6 shows less time in delivering the message to number of vehicles.

XIII. CONCLUSION AND FUTURE WORK

IPv6 Multicast communication in vehicular ad-hoc network module take less time to delivered the message to vehicles on a road. The communication is done between vehicle to vehicle, vehicle to fixed equipment placed in road side and vice versa. The developed software was tested the results were comparable with the existing system. The vehicle IP in the old version IPv4 was converted in to new version of IP address IPv6, so that more vehicle get an IPv6 Address in the world that was not possible with old version of IPv4 address.

To analyze the possibility to perform IPv6 multicast for VANET by considering the availability of geographical information and digital maps. One of the main contributions of this paper is the definition of new address format in order to encode geographical and analysis the possibility to integrate the digital maps information into IPv6 address. In addition to IPv6 multicast addressing format, two operational multicast solutions, which could be adapted to VANET are present forwarding proxy and static multicast routing.

REFERENCES

[1] Yacine Khaled, Ines Ben Jemaa, Manabu Tsukada and Thierry Ernst "*Application of IPv6 multicast to VANET*" 2009 IEEE

[2] B. Haberman and D. Thaler. *Unicast-prefix-based ipv6 multicast addresses*. Rfc, IETF, 2002.

[3] T. Hain. An ipv6 geographic global unicast address format. Internet-draft, IETF, 2008.

[4] Stephen E. Deering and Robert M. Hinden. *Internet Protocol, Version 6 (IPv6). Internet RFC 2460*, December 1998.

[5] BHATTACHARYYA, S. *An Overview of Source-Specific Multicast (SSM).* Requestor Comments (RFC) 3569, Internet Engineering Task Force, July 2003.

[6] DEERING, S. *Host Extensions for IP Multicasting. Request for Comments (RFC) 1112*, Internet Engineering Task Force, Aug. 1989.

[7] Easy cast du multi hub: http://unfix.org/projects/ecmh/

[8] HINDEN, R., AND DEERING, S. *IP Version 6 Addressing Architecture. Request for Comments (RFC) 4291*, Internet Engineering Task Force, Feb. 2006.

[9] HOLBROOK, H., AND CAIN, B. *Source-Specific Multicast for IP. Request for Comments(RFC) 4607*, Internet Engineering Task Force, Aug. 2006.

[10] VIDA, R., AND COSTA, L. *Multicast Listener Discovery Version 2 (MLDv2) forIPv6. Request for Comments (RFC) 3810*, Internet Engineering Task Force, June2004.

[11] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami. *Multiple Care-of Addresses Registration, November 2009. RFC 5648*.

[12] HINDEN, R., AND DEERING, S. *IP Version 6 Addressing Architecture. Request for Comments (RFC) 4291*, Internet Engineering Task Force, Feb. 2006

[13] CAIN, B., DEERING, S., KOUVELAS, I., FENNER, B., AND THYAGARAJAN, *A. Internet Group Management Protocol, Version 3. Request for Comments (RFC) 3376*,Internet Engineering Task Force, Oct. 2002.

[14] Car-to-car communication consortium: http://www.car-to-ar.org

[15] DEERING, S., FENNER, W., AND HABERMAN, B. *Multicast Listener Discovery (MLD) for IPv6. Request for Comments (RFC) 2710*, Internet Engineering Taskforce, Oct. 1999.

[16] CONTA, A., DEERING, S., AND GUPTA, M. *Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. Request for Comments(RFC) 4443, Internet Engineering Task Force, Mar. 2006.

[17] Car-to-car communication consortium: http://www.car-to-car.org

[18] NARTEN, T., NORDMARK, E., SIMPSON, W. AND SOLIMAN, H. *Neighbor Discovery for IP version 6 (IPv6). Request for Comments (RFC) 4861*, Internet Engineering Task Force, Sept. 2007.

[19] JinHyeock Choi, Yacine Khaled, Manabu Tsukada and Thierry Ernst *IPv6 support for VANET with geographical routing*, 978-1-4244-2858-8/08©2008 IEEE

[20] T Narten, E Nordmark, W Simpson, H Soliman, *Neighbor Discovery for IPversion 6 (IPv6). RFC 4861*. (September 2007)

[21] S Thomson, T Narten, T Jinmei, *IPv6 Stateless Address Autoconfiguration.RFC 4862*. (September 2007)

[22] R Droms, J Bound, B Volz, T Lemon, C Perkins, M Carney, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315* (July 2003).

[23] Marco Gramaglia1,2*, Carlos J Bernardos2, Ignacio Soto3, Maria Calderon2 and Roberto Baldessari , "*IPv6 address auto configuration in geo networking enabled VANETs: characterization and evaluation of the ETSI solution*", Journal on Wireless Communications and Networking 2012

[24] Uma Nagaraj , Deesha G. Deotale , *"IPv6 Multicast in VANET"* International Journal of Computer Science and Information Security(IJCSIS), Vol. 10, No. 4, April 2012