Solutions to Overcome Ipv4/Ipv6 Compatibility Issues In Vehicular Adhoc Networks

R.Jeevitha, N.Sudha Bhuvaneswari

Abstract**:** ***Researchers found that Internet Protocol Version 6 (IPv6) can be considered since it is the important communication protocol for internet access during driving, location privacy in Vehicular Adhoc Networks (VANET). TCP/IP allows devices to interact online. A unique IP address allows each device to communicate with each other over the internet. From the desktop computers to tablets, to PS4s, to mobile phones, to cars, to airplanes, to IP enabled washers and dryers, lot of things will be connected online. It needs a lot more addresses than that are available today. IPv6 was created in the mid-'90s to make the internet grow. It is not backward compatible with IP version 4, but both IPv4 and IPv6 protocols can run simultaneously over the same wires. This requires a transition from IPv4 to IPv6 and vice-versa. The IPv6 layer is a vital issue in the field of Intelligent Transportation System (ITS). The vehicles possess heterogeneous devices like sensors, Global Positioning System (GPS), IPv4 addressing and IPv6 addressing. IPv4 addresses are depleting and IPv6 addressing came into existence. When the Road Side Unit (RSU) communicate with gateway and with vehicular cloud using IPv4 and IPv6 addressing, compatibility issues occur. This paper mainly focuses on the IPv4/IPv6 compatibility issues and the possible solutions to overcome the compatibility issues during the dissemination of data in VANET.***

Keywords: IPv4, IPv6, ITS, VANET

I. INTRODUCTION

The IP network addressing functions on the network layer. The main function of IP protocol is to identify the hosts based on their logical addresses so as to route the packets between them over the network. Due to the deficiency of IPv4, IPv6 came into existence. Address space of IPv4 is exhausted. IPv6 is developed by Internet Engineering Task Force (IETF). Network that use IPv6 supports both IP version 4 and version 6 addresses on their network. IPv6 enhances routing and network auto-configuration of IPv4. IPv6 has 340 trillion trillion trillion of unique addresses. A protocol stack is designed by the Wireless Access in Vehicular Environments (WAVE) for safety-critical communication in VANET. As for WAVE, an extension towards IPv6 primarily base on communication exist, that reuses PHY/MAC layer and network layer functionality from VANET safety-critical communication [3]. IPv6 makes routing easier because of hierarchical addressing mode and simple header format. IP version 6 Provides automatic configuration, mobility with route optimization and end-to-end security [1]. IP Version 6 has new types of service integrations like multicast, QOS, Security and Mobility (MIPv6).

Revised Manuscript Received on November 30, 2019.
* Correspondence Author

R. Jeevitha*, Department of Computer Science, Dr.G.R.Damodaran College of Science, Coimbatore, India.

Dr. N. Sudha Bhuvaneswari, Department of Computer Science, Dr.G.R.Damodaran College of Science, Coimbatore, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

II. IPV4 AND IPV6

This section discusses about the shortcomings of IPv4, advantages of IPv6 over IPv4 and the difference between IPv4 and IPv6.

A. Shortcomings of IPv4

- IPv4 can accommodate about 4 billion hosts.
- No encryption technique is used.
- Packets are not authenticated when they are transmitted.
- Network devices gets overloaded and congested due to broadcasting.
- It is difficult to prioritize the high priority data.
- It is not suitable for VOIP or voice streaming.
- Expiry time for datagram is sent using TTL field in the header. If the time expires, it will be requested again. Delay causes packet loss [4].

B. Advantages of IPv6 over IPv4

- IPv6 has hierarchical network architecture.
- Larger address space.
- Better header format.
- NAT is not required.
- New options, Auto-configuration, plug and play support.
- Allows for extension.
- Supports resource allocation.
- Built-in security and mobility [7].

C. Difference between IPv4 and IPv6

Table- I: IPv4 vs IPv6 [7]

IPv4	**IPv6**
32 bit addressing	128 bit addressing
Broadcasting	Multicasting
IPSec is not compulsory.	IPSec is compulsory.
It must support DHCP or it should be configured manually.	DHCP or manual configuration is not required. Stateless auto configuration is supported.
Header has 12 fields.	Header has 8 fields.
Header is 20-60 bytes. It is based on IP header options.	Header is 40 bytes fixed length. There is no IP header options.

III. IPV4 AND IPV6 HEADERS

Transition to IPv6 is hindered by restricted compatibility both forward i.e. the existing IP version 4 devices trying to communicate with IPv6 devices and backward as IPv6 devices communicating with IPv6 devices. The reason is IPv4 and IPv6 use different header formats. The simplified IPv6 packet header format will handle the packets more efficiently [2].

A. IPv4 Packet Header Format

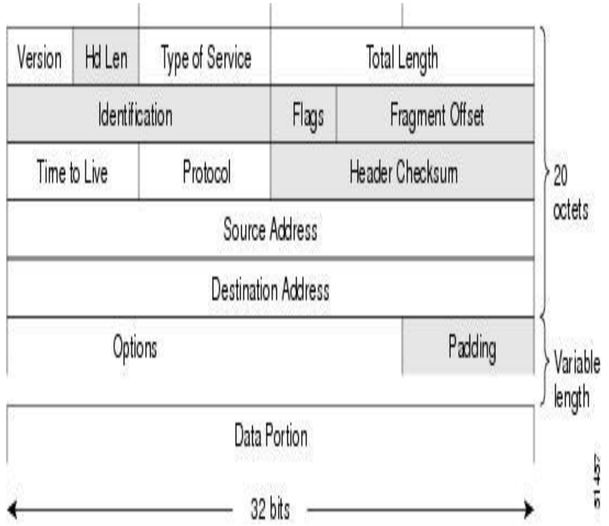


Fig. 1. IPv4 Packet Header [6]

The following are the descriptions for each field on the IPv4 packet header.

Version: First header field which represents the IP protocol version (4 bits). For IPv4, the version is 4.

Hd Len: Header length is 4 bits. It is the second field, which is 32 bit words in the IP header. The minimum value is 5 i.e. length of 5×32 = 160 bits. The maximum length is 15 words i.e. 480 bits.

Type of service: This field (8 bits) carries information to provide Quality Of Service (QOS) metrics such as Low End-to-End Delay and High Throughput.

Total Length: Total header Length and Data (16 bits), minimum value is 20 bytes (20-byte header + 0 bytes data) and the maximum value is 65,535 bytes.

Identification: Unique Packet Id (16 bits) used to identify unique fragments of one IP datagram.

Flags: 3 flags of 1 bit each.

Fragment Offset: 8 bytes. The maximum value of $(2^{13} – 1) \times 8$ = 65,528 bytes. It represents the number of Data Bytes ahead of the particular fragment in the particular Datagram.

Time to live: Lifetime of Datagram (8 bits), maximum time the datagram is allowed to remain in internet system.

Protocol: 8 bits field which specifies the name of the protocol to which the data is to be sent.

Header Checksum: 16 bits header field to check the errors in the datagram header.

Source address: IP address of the source node (32 bits).

Destination address: 32 bits IP address of the receiver node.

Options: It includes optional information like source route to reach destination and record the route. But these are not often used.

Data: It is not included in the packet checksum.

B. IPv6 Packet Header Format

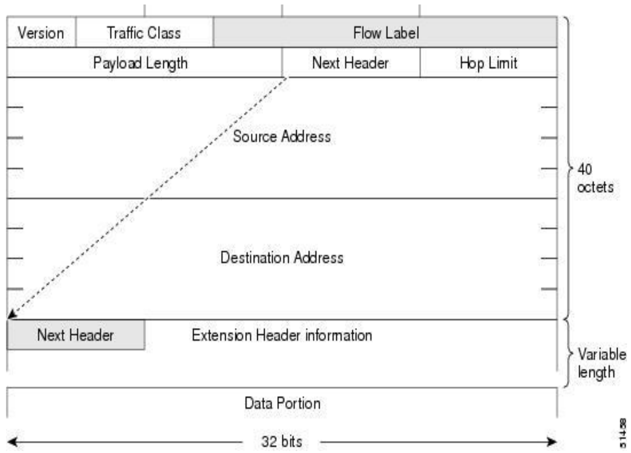


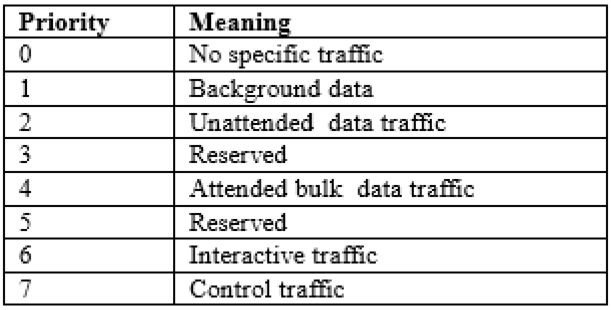
Fig. 2. IPv6 Packet Header [6]

The following are the descriptions for each field on the IPv6 packet header.

Version: this field 4 bits indicates the protocol version and has value 6.

Traffic Class: Traffic class (1 byte) is the priority of IP version 6 packet. It is similar to service field in IPv4 packet. The router handles the traffic according to the priority of the packet. If there is any congestion on the router, then the least priority packets will be discarded. 4 bits are being used [0-7 for congestion controlled traffic and 8-15 for uncontrolled traffic]. Uncontrolled data traffic (Audio/video data) has higher priority. Source node can set the packet priorities but on the way, the routers are capable of modifying the priority.

Table- II: Traffic class priority



Priority	Meaning
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Flow Label: This field is used as a label for the data flow (20 bits).

Payload Length: 16 bit field to indicate the packet data field length.

Next Header: This field points to the type of header immediately following the header (8 bits).

Hop Limit: The hop limit (8 bits) is decremented by one by each node whenever the packet is forwarded. The packet will be discarded, if the hop limit reaches 0.

Source Address: 128 bits. IP address of the sender node.

Destination Address: 128 bits. IP address of the receiver node.

Table- III IPv4 and IPv6 Header Comparison

Header	IPv4	IPv6
Address Length	32 bit	128bits
Header Format	Variable	Fixed
Header Fields	13	8
Header Length	20-60 bytes	40 bytes
Extension header	No	Yes

Header Checksum	Yes	No

C. IPv4 and IPv6 Feature Comparison

IPv6 contains many features which are not available in Ipv4. The table below contrasts the features of IPv4 and IPv6.

Table – IV Feature Comparison chart [5]

Feature	IPv4	IPv6
Security Support	✗	✓
Mobility Support	✗	✓
Anycast address	✗	✓
Multicast scoping	✗	✓
Auto configuration	✗	✓
Router Fragmentation	✓	Source node only
Router Discovery	✗	Neighbor Discovery function

IV. ADDRESSING MODELS IN IPV6

IPv6 has three types of addressing model, namely anycast, unicast, and multicast [5].

IPv6 Unicast: Unicast is a type of IPv6 communication where data is sent from one node to another node. IPv6 Unicast is a one-to-one type of network communication [9].

IPv6 Multicast: IPv6 multicast address delivers the packets to a group of destinations**.** Any packet sent to a IPv6 multicast address, will be delivered to every node that has joined that particular group [9].

IPv6 anycast: IPv6 anycast address is similar to the multicast address. Instead of entire group, the packets are delivered to only one random host [9].

V. APPLICATIONS OF IPV6 IN THE ROAD DOMAIN

IPv6 has the potential to reduce accident rates by enabling the transmission of safety critical information.

A. Internet access

Internet access from the in-vehicle devices is the common service in VANETs. The OBU installed in the vehicle requires internet access. Although IPv4 provides the service using 3G, it suffers a lot of issues because large volume of data need to be exchanged. More than one vehicle wanting to access internet at the same time. It is not the scalable way of accessing internet in the next coming future. In this, the usage of IPv6 technologies can offer good benefits to drivers and passengers. Vehicular Wi-Fi (IEEE 802.11p) can also be used when required and offload the 3G networks [1].

B. Traffic efficiency services

IPv6 supports traffic efficiency services like congestion detection, management and notification, route planning, variable speed limit or road tolling. When IPv6 networks are used, V2I communication could suffer problems like lack of interoperability. Due to limited 3G coverage, connectivity problems occur in congested road segments. To solve the problem, IPv6 multicasting is used. Novel dissemination strategies can be taken into account by mapping between the geographical position of vehicles and temporarily assigned IPv6 address. NAT 64 can be used during the transition period from IPv4 and IPv6. It can support the access from an IPv6-based vehicular network to IPv4- addressed services [1].

C. Vehicle-to-Vehicle Infotainment

For passing messages, routing information exchange or audio conference requires communication between vehicles. When IPv4 is used, the services must deal with cost and performance issues, NAT issues. As there is no direct IP routes between end devices, it requires a backbone support for allowing Peer to Peer communication. IPv6 solves the above problems because IPv6 has auto configuration which can provide IPv6 global address to each vehicle NAT whenever necessary [1].

D. Safety services

IPv6 supports safety services like road infrastructure alerts, crash notification and vehicle monitoring or emergency calls. By using IPv4, the next limitations are found such as in potential IoT scenarios, IP version 4 addressing will not allow direct access to the vehicles. Depending only on 3G networks could be a problem nowadays of remote locations and mountains. 3G does not warrantee that all vehicles within the geographical areas are aware of safety notifications.IPv6 can solve the problem by improving the communication performance. IPv6 gateways, advanced infrastructure services can be provided to monitor the vehicle status such as oil level and quality, engine operations, etc. [1].

E. Secured services

Using IPv4 does not guarantee about the interoperation. To solve this, IPv6 provides IP security protocol (IPsec) which can provide security tunnels between a pair of IPv6 nodes. This guarantees integrity and confidentiality of the data transmitted [1].

F. Network access

When the nodes enter the vehicular network, there occurs security and business model issue. In future, ITS cooperative services, network authentication and authorization are necessary [1].

VI. IPV6/IPV4 COMPATIBILITY ISSUES

IPv6 is not backward compatible. Compatibility with IPv6 networking can be a software or firmware issue [10]. The compatibility constraint applies to routing protocols also. IPv6 will be used to bypass IPv4 security for attacks like hijacking. The architecture of IPv6 has been designed to permit the prevailing IPv4 users to transition easily to IPv6 while providing services like end-to-end security, QOS and globally unique addresses.IPv6 specification requires 100% compatibility for existing protocols. Compatibility is also required for existing applications during transition. Networks that use IPv6 supports both IPv4 and IPv6 addresses in their network.

A. Transition mechanisms

The elements involved in the transition are basic network infrastructure, Networked infrastructure services, Infrastructure device enablement, middleware and databases. Technologies that ensure smooth transition from IPv4 to IPv6 are as follows:

1. **Dual Stack**

IPv4 and IPv6 runs simultaneously on the devices in the network. Two IP routing tables will place a burden on routers. New IPv6 hosts that require IPv4 compatibility can quickly eat up IPv4 address space [10].

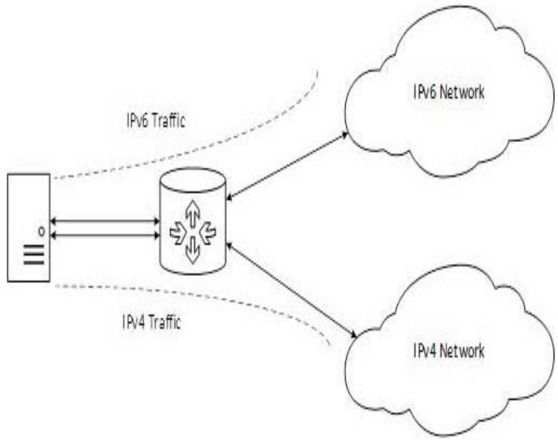


Fig. 3. Dual Stack [12]

In the above Fig.3, a server node consist of IPv4 and IPv6 address configured for it. With the help of Dual Stack Router, it can communicate with all the hosts on both the IPv4 and IPv6 networks. All the nodes are both IPv4 and IPv6 enabled in a dual stack network.

Limitations

It needs a current network infrastructure that's capable of deploying IPv6. IPv6 is not supported on all of the IPv4 devices. IPv6 on existing IPv4 infrastructure can cost more due to hardware changes. The existing network requires to be redesigned, posing business continuity challenges.

2. Tunneling

Different IP versions (version 4 or 6) exist on intermediate path network. It is generic routing encapsulation [8].

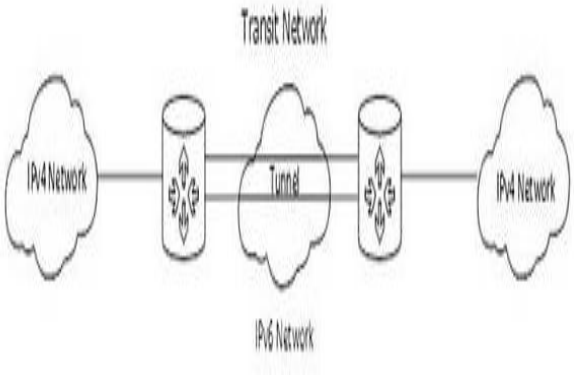


Fig. 4. Tunneling [12]

The above Fig.4 depicts how tunnel is used as a medium for two IPv4 remote networks to communicate as the transit network was on IPv6. Vice versa (IPv6 to IPv4) is possible.

Limitations

Tunneling does not enable users of the new protocol to speak with users of the old protocol without dual-stack hosts that negates interoperability.

3. Translation

Enable IPv4-only devices to speak to IPv6-only devices and vice-versa [8].

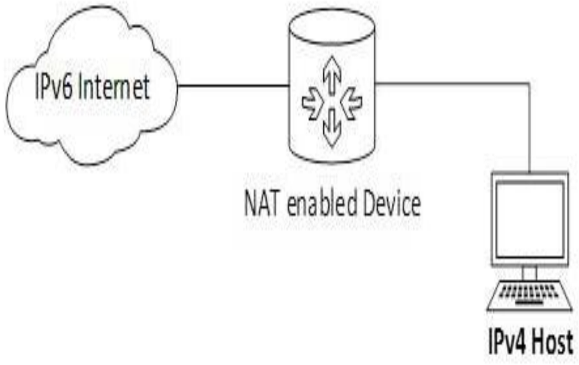


Fig. 5. Translation [12]

In the above fig. 5. An IPv4 host sends a request to an IPv6 enabled server on the internet that does not perceive IPv4 address. The NAT-PT router act as intermediate to make the devices communicate. If the IPv4 host sends a request packet to the IPv6 server, the NAT-PT router strips down the IPv4 packet. The IPv4 header is removed and the IPv6 header is added and passed it through the net. Once a response from the IPv6 server comes for the IPv4 host, the NAT-PT router does vice versa [12].

Limitations

IPv4 and IPv6 are not directly interoperable, session packets have to be translated at-least twice (to and from the server).

VII. POSSIBLE SOLUTIONS FOR IPV6/IPV4 COMPATIBILITY

A. Single Stack Encapsulation

This proposed methodology combines Dual stack and Tunneling mechanism. TCP/IP v6 application should accept the IP version 4 address embedded in the IP version 6 address and then successfully connect to its corresponding server application on other machines.

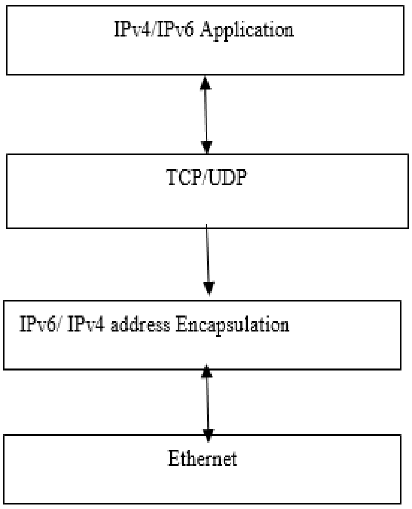


Fig. 6. Single Stack Encapsulation

B. IPv4 compatible Encapsulation

IPv4 addresses are encapsulated inside IPv6 address. As the IPv4 packets are enclosed inside IPv6 packets, the data inside the IPv4 packets can traverse an IPv6 network.

After it traverses, the IPv4 packets are unpacked into the native form as shown in figure 7. For example, if the IP version 4 address is 127.0.0.1, it is encapsulated as 0: 0: 0: 0: 0: ffff: 7f00: 1. As soon as the packet arrives the destination, it is decapsulated as 127.0.0.1. 4 over 6 Provider Edge router can be used.

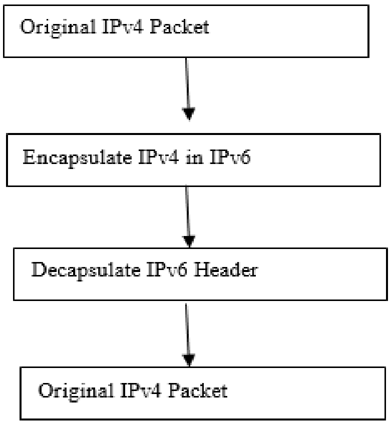


Fig. 7. IPv4 compatible Encapsulation

Step 1: Router will have an encapsulation table with IP version 4 prefix and its corresponding IP version 6 address.

Step 2: Local IPv4 routing table will point to the encapsulation table entry with matching destination IP version 4 prefix.

Step 3: Router encapsulation table has the corresponding IPv6 address for the IPv4 prefix.

Step 4: IP version 4 packet is encapsulated in IPv6 header.

Step 5: As soon as the packet arrives the destination node, IPv6 header can be removed and the original IP version 4 packet is forwarded to the destination node.

The drawback is that, if session time is out, it results in packet loss. So retransmission delay increases.

C. After transition to IPv6

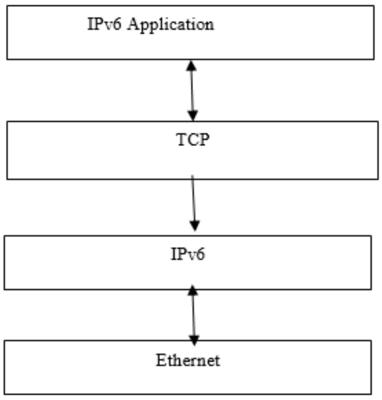


Fig. 8. After transition to IPv6

IPv6 gateway can be provided when necessary. Cloud based gateway is used for traffic and content message dissemination.

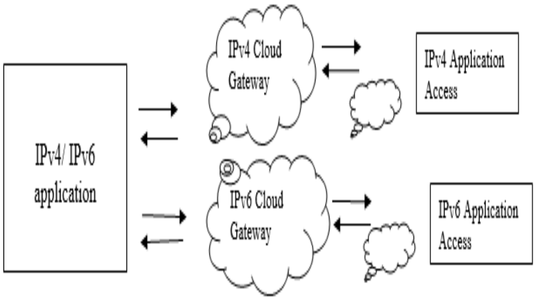


Fig. 9. IPv4/v6 Gateway

Gateway should support both IPv4 devices as well as IPv6 devices. Gateway solution is typically hardware based. Internal router port acts as a gateway for IPv4 addresses and IPv6 addresses separately. External router port will have single stack configuration with IPv6 and IPv4 encapsulated address.

Other solutions include Dual Stack Lite, Light weight 4 over 6 and Hybrid scenario of existing transition methods [11].

D. Address format

IPv4 compatible address formats can be used for representing an IPv6 node. This format in figure 10 will enables us to configure the IPv6 node to use IP version 6 without possessing a real IPv6 address. This type of address format also allows us to experiment with different IPv6 deployments since automatic tunneling can be used to cross IPv4- only routers.

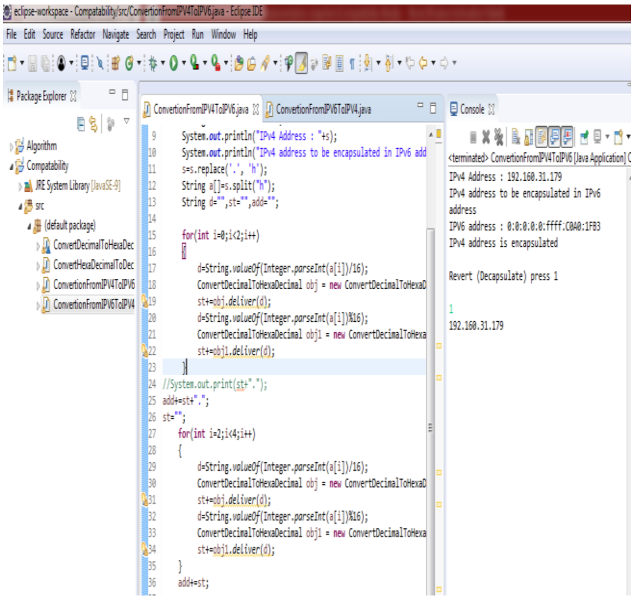
000........000	IPV4 address

Fig. 10. IPv4 compatible address formats

To analyze the IPv6/IPv4 compatibility, IP Address Management tool (IPAM) is used. It can track all IP addresses within your LAN and network. It can handle large volume and length of addresses. It tells how IPv6 fits into existing network, what needs to change, how it will look before and after implementation.

VIII. IMPLEMENTATION AND RESULT

The proposed mechanism is implemented using JAVA.


eclipse-workspace - Compatability/src/ConvertionFromIPV4ToIPV6.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help
Package Explorer
Algorithm
Compatability
JRE System Library [JavaSE-9]
src
(default package)
ConvertDecimalToHexaDec
ConvertHexaDecimalToDec
ConvertionFromIPV4ToIPV6
ConvertionFromIPV6ToIPV4
ConvertionFromIPV4ToIPV6.java
ConvertionFromIPV6ToIPV4.java
Console

```
    System.out.println("IPv4 Address : "+s);
    System.out.println("IPv4 address to be encapsulated in IPv6 add
    s=s.replace('.', 'h');
    String a[]=s.split("h");
    String d="",st="",add="";

    for(int i=0;i<2;i++)
    {
        d=String.valueOf(Integer.parseInt(a[i])/16);
        ConvertDecimalToHexaDecimal obj = new ConvertDecimalToHexaD
        st+=obj.deliver(d);
        d=String.valueOf(Integer.parseInt(a[i])%16);
        ConvertDecimalToHexaDecimal obj1 = new ConvertDecimalToHexa
        st+=obj1.deliver(d);
    }
//System.out.print(st+".");
add+=st+".";
st="";
   for(int i=2;i<4;i++)
   {
        d=String.valueOf(Integer.parseInt(a[i])/16);
        ConvertDecimalToHexaDecimal obj = new ConvertDecimalToHexaD
        st+=obj.deliver(d);
        d=String.valueOf(Integer.parseInt(a[i])%16);
        ConvertDecimalToHexaDecimal obj1 = new ConvertDecimalToHexa
        st+=obj1.deliver(d);
   }
   add+=st;
```

```
<terminated> ConvertionFromIPV4ToIPV6 [Java Application] C
IPv4 Address : 192.160.31.179
IPv4 address to be encapsulated in IPv6
address
IPV6 address : 0:0:0:0:0:ffff:C0A0:1FB3
IPv4 address is encapsulated

Revert (Decapsulate) press 1

1
192.160.31.179
```

Fig. 11. Snapshot of IPv4 Encapsulation and Decapsulation

For instance, IPv4 address is 192.124.93.1. It needs to be encapsulated inside IPv6 since IPv6 is not backward compatible. The address needs to be compressed. When it reaches the destination, the header of the encapsulated packet is removed.

The message is transmitted and the encapsulated address is decapsulated to the original form.

```
IPv4 Address: 192.124.93.1
IPv4 address to be encapsulated in IPv6 address
IPV6 address: 0:0:0:0:0:ffff:C07C:5D01
IPv4 address is encapsulated
Revert (Decapsulate) press 1
1
192.124.93.1
```

IPv4 addresses are encapsulated inside the IPv6 address. The data inside the IPv4 packets can traverse an IPv6 network, as the IPv4 packets are enclosed inside IPv6 packets. After traversal, the IPv4 packets are unpacked into the native form.

IX. CONCLUSION

The proposed work is implemented in JAVA. The above proposed mechanism can overcome IPv4/v6 compatibility issues in VANET. IPv6 is much easier to install and implement because of auto configuration and Neighbor Discovery functions. IP spoofing continues to be a potential security concern with IPv6 networks. In future, IPv6 enabled Internet version 2 will exist. Third party vendors like Future Soft have announced products like hosts and routers for IPv6 compatibility. Device manufacturers should plan to offer IPv6 by-default enabled on devices. The IPv6 design should support both IPv6 networking and geographical VANET networking. Location verification data dissemination and video-centric routing issues exist. Geographical information notion is not built-in in IPv6. In future, the geographical information can be incorporated in the IPv6 header.

REFERENCES

1. Anttonio F.Skarmeta, Pedro M.Ruiz, Jose Santa Lozano and Alejandro, "Governments Enabled with IPv6 – GEN6", supported by the European Commission.
2. Babu Ram Dawadi, Shashidhar Ram Joshi, Ananda Raj Khanal, "Service Provider IPv4 to IPv6 Network Migration Strategies", J. *of Emerging Trends in Computing and Info Sci*, Vol. 6, No. 10, 2015, pp. 565-572.
3. C. Campolo, A. Molinaro, R. Scopigno, Eds., "Vehicular ad hoc Networks -Standards, Solutions, and Research", *Springer*, 2015.
4. Henry Chukwuemeka Paul, Kinn Abass Bakon," A study on IPv4 and IPv6: The importance of their co-existence*", Int J. of Info Sys and Eng.*, Vol. 4, No.2, 2016, pp.97-106.
5. Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworkingProtocols, ETSI European Norm 302 636-6-1, Rev. 1.2.1, May 2014.
6. Khan, Rafiqul Zaman, "A Comparative Study on IPv4 and IPv6", *Int J. of Advanced Info Sci and Tech (IJAIST)*, Vol.33, No.33, 2015, pp. 9-16.
7. Olabenjo Babatunde, Omar Al-Debagy," A Comparative Review of Internet Protocol Version4 (IPv4) and Internet Protocol Version 6 (IPv6)", *Int J, of Comp Trends and Tech (IJCTT)*, Vol. 13, No. 1, 2014, pp. 10-13.
8. C. V. Ravi Kumar, Kakumanilakshmi Venkatesh, Marri Vinay Sagar and Kala Praveen Bagadi, "Performance Analysis of IPv4 to IPv6 Transition Methods", *Indian J. of Sci and Tech*, Vol. 9 ,No. 20, 2016, pp. 1-8.
9. Uma Nagaraj, Deesha G.Deotale, "Study of Communication using IPv6 in VANET", *Int J. of Comp. Sci and Commn Net*, Vol 1, No.3, pp. 247-251
10. Xianhui Che, Dylan Lewis," IPv6: Current Deployment and Migration Status", *Int J. of Research and Reviews in Comp Sci*, Vol. 1, No. 2, 2010, pp.22-29.
11. Yong Cui, Wendong Wang, Qi Sun, Lishan Li, Xingwei Wang, "IPv4 Address Sharing and Allocation for IPv6 Transition", *IEEE Internet computing*, 2015, pp.66-71
12. www.tutorialspoint.com

AUTHORS PROFILE

R.Jeevitha, is currently pursuing her Ph.D. in Computer Science in Dr.G.R.Damodaran College of Science, Coimbatore, India. Her area of interests include Network security and VANETs. She has nine publications in International Journals to her credit. She has presented papers in International and National Conferences. She has also received Best Paper Presenter award in the International Conference.

Dr.N.Sudha Bhuvaneswari, is working as Associate Professor Dr.G.R.Damodaran College of Science, Coimbatore, India. She has more than 20 years of teaching experience. She has authored 2 books and 3 Chapters and more than 80 Journal and Conference publications. She is a fellow in Asia Pacific Internet Governance Forum and Asia Pacific Network Information Centre and her Cyber Security Policy is accepted by the United Nations Organization of Internet Governance. She has also received Marquis "Who is who in the World" award for the year 2012.

Retrieval Number: A4382119119/2019©BEIESP
DOI: 10.35940/ijitee.A4382.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication