ACTA TECHNICA JAURINENSIS
Vol. 16, No. 2, pp. 42-61, 2023
10.14513/actatechjaur.00693

Review

A survey on efforts to apply IPv6 in V2X communication networks

Hassan Farran[1,*], László Bokor[1]

[1]Department of Networked Systems and Services, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics
Műegyetem rkp. 3., H-1111 Budapest, Hungary
*e-mail: hfarran@hit.bme.hu

Submitted: 25/04/2023 Accepted: 26/05/2023 Published online: 31/05/2023

Abstract: This survey focuses on the application possibilities of using Internet Protocol (version 6) in Vehicle-to-Everything (V2X) networking architectures by analyzing existing standards and related papers in this field. The article explains the terminology used in IP-based V2X networks, introduces the considered use cases, and gives an overview of the three standardized options applying IPv6 in vehicular environments: IEEE WAVE provides networking services to applications in vehicular networks through IPv6, IPv6 over 802.11-OCB can be implemented in Wi-Fi-based ad hoc vehicular networks for both V2V and V2I, and the Geo Networking IPv6 adaption sub-layer (GN6ASL) for IPv6 support in the ETSI ITS protocol family. The paper also highlights non-standardized solutions and available techniques designed for IPv6-based V2X infrastructures, summarizes wireless connection requirements, and mobility management needs, together with the newest research efforts aiming at the applications of IPv6 in V2X communications.

Keywords: Vehicle-to-Everything (V2X); Internet Protocol version 6 (IPv6); vehicular ad-hoc networks (VANETs); IEEE 802.11-OCB; WAVE; GN6ASL

I. INTRODUCTION

V2X is a networking concept for exchanging messages that contain status data and vehicle attribute information in the cooperative and legacy Intelligent Transport Systems (ITS/C-ITS) domain. It allows a vehicle to connect with every transportation participant, such as in the context of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle to Network (V2N), and even introducing pedestrians (V2P) or smart power grids (V2G) [1] into this system. V2X networks have two primary, currently available communication techniques. The first and initial one is the Dedicated Short Range Communications (DSRC) standard (known as ITS-G5 in Europe) which is based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 Wireless-LAN-based (WLAN) standard family. The second is the mobile cellular communications-based solution (Cellular V2X) which relies on the standardization results of the 3rd Generation Partnership Project (3GPP) [2].

DSRC is classified as the Wi-Fi-based V2X technique, using the IEEE 802.11p specifications under IEEE 802.11-2016 (the standard specifying physical (PHY) and MAC layers for wireless communication between moved or fixed stations (STAs) within a local region). IEEE 802.11p or IEEE 802.11-OCB (Outside the Context of Basic Service Set) was designed for ad hoc Wi-Fi networking and to assist in the various vehicular scenarios needed for V2X system operations [3].

However, IEEE 802.11p is an officially accepted amendment to the well-known IEEE 802.11 standard, which is widely recognized as Wi-Fi. Its primary focus is on fulfilling the requirements of vehicular communication systems by introducing protocol improvements that ensure swift and dependable communication in situations involving high-speed mobility. Through modifications to the existing 802.11 standards, 802.11p enables efficient communication among vehicles in V2X scenarios, encompassing both V2V and V2I interactions [4]. Furthermore, IEEE 802.11p is the cornerstone of the IEEE 1609 family of standards [5] created for road safety systems unified by Wireless Access in Vehicular Environments (WAVE) specifications. On the one hand, IEEE 1609 specifies a vehicular communications protocol stack for both safety and non-safety purposes. On the other hand, WAVE standards describe an architecture as well as a complementary, consistent range of services that allow stable V2V and V2I wireless communications. These standards, when combined, pave the way for a wide variety of transportation technologies, including driver safety, electronic tolling, improved navigation, and traffic control [6]. A package of IEEE 1609 standards was adopted for trial use in 2006 and 2007 [3]. IEEE 1609.0 standard defines the WAVE architecture and the facilities required for multi-channel DSRC/WAVE systems, while IEEE 1609.1 describes resource manager specifications. IEEE 1609.2 is the standard for vehicular security, IEEE 1609.3 specifies network layer services and transport layer services, and IEEE 1609.4 defines multi-channel extensions to the IEEE 802.11-2012 Medium Access Control (MAC) layer [7].

In current 802.11p-based systems, Internet Protocol (IP) is not applied: although standards support the application of IP in the networking layer, non-IP solutions have become widespread in practice. The issue with IP is that it requires more bandwidth which is why they are not utilizing it right now. IP, with its transport layer (TCP and UDP), is not a lightweight protocol; the stack implements extensive headers because it is a more general purpose, not concentrating on the issue that we want to address in the ITS domain. Besides the overhead of sub-optimized header structures, tackling latency requirements could also be a problem for IP in the case of real-time safety V2X applications and services.

Cellular V2X (C-V2X) transmits and receives signals via 3GPP fourth-generation (4G) or fifth-generation (5G) and beyond communication. It employs two distinct transmission modes. The first is direct contact between cars, utilities, and pedestrians on the road. Cellular V2X can operate independently of a cellular network in this mode. For correspondence, it employs a PC5 interface. In contrast, the second mode is cellular network communications. C-V2X uses a traditional mobile network to provide information about road and traffic conditions in the field to cars. For correspondence, it employs the Uu interface, the Uu interface utilizes LTE's and 5G NR's uplink and downlink capabilities to establish vehicle-to-vehicle communication. On the other hand, the PC5 interface, also known as sidelink communication in cellular terminology, employs a similar method to DSRC to enable direct connections between vehicles [8]. IP is applied in the Uu interface, but in PC5, it is only an option currently that is rarely considered in actual implementations. Figure 1 summarizes where IP is used in V2X infrastructures nowadays.

The role of vehicular networks within the ITS/C-ITS research area considers new and existing vehicular services, such as fleet management and road pricing. These intelligent environments include services related to transportation and traffic management modes, allowing people to be more aware and use transportation infrastructure. These provide sophisticated telematics using hybrid networks, such as (IP-based) communications and non-IP ad-hoc direct contact between vehicles and infrastructures employed at the same time [9]. Although IP has numerous promising features for V2X applications (e.g., works as a unification layer, provides interoperability, ensures portability and wider deployment) and several efforts are calling for IP to be used in PC5 and DSRC, until these days, those efforts remained sporadic. This article aims to raise awareness of the potential benefits of IP-based V2X solutions.

The current version of the Internet Protocol IPv4 is becoming outdated due to its small address space, lack of required functionality, and insufficient built-in security features. The Internet Protocol version 6 (IPv6) [10] was standardized and intended to replace IPv4 because it suffers from a depleting 32 bits-long address space, affecting Internet continuity's growth, and is no longer scalable for future use. IPv6 offers many benefits that meet the critical needs of cooperative vehicular connectivity, such as the enormously broad address space provided by the enhanced 128 bits long addressing and the built-in and secure Mobile IPv6 protocol family for efficient IP-level mobility management [11].

However, in novel Internet use cases and networking environments, such as V2X, it is intended to rely solely on IPv6-based technologies. Of course, it is a tremendous benefit of IPv6 that it has an enormous address space which is useful when designing ever-growing V2X networks, their technologies, and services. The IPv6 protocol is generally regarded as a widely accepted, standardized protocol that will be predominant for future communication [12].

Currently, there are three major standardized options to apply IPv6 in vehicular networks. IEEE WAVE provides networking services to applications in vehicular networks through IPv6 as an optional networking layer, IPv6 over 802.11-OCB, which can be implemented in IP-based vehicular networks for V2V and V2I for 802.11p-based infrastructures, and the GeoNetworking IPv6 adaption sub-layer (GN6ASL) that provides IPv6 communication capabilities over non-IP Geonetworking mechanisms.

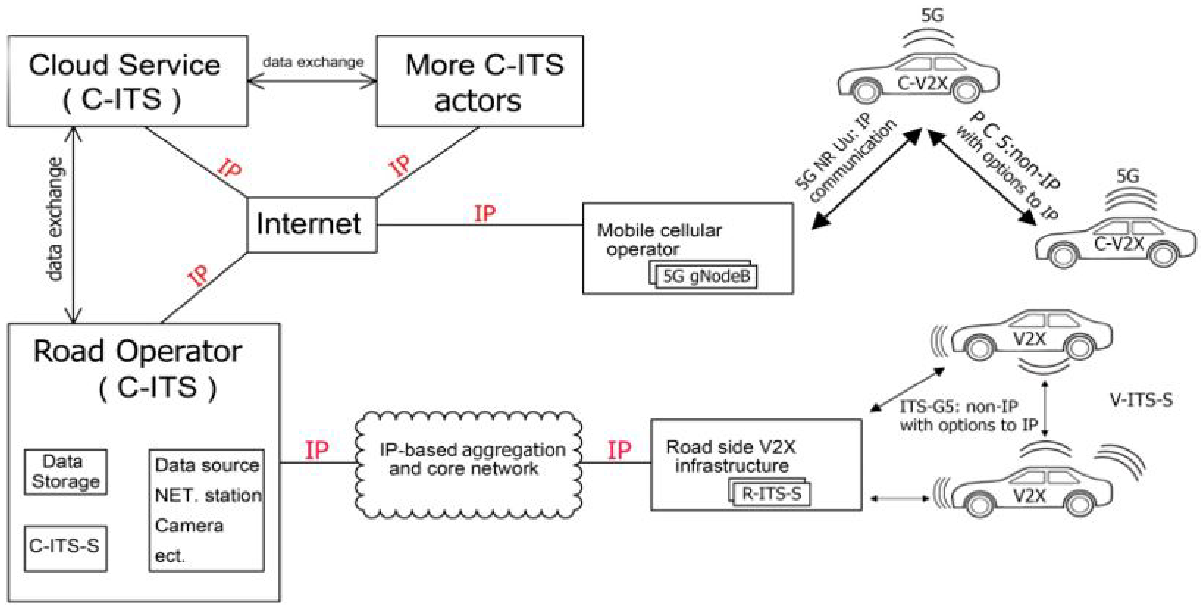

Figure 1. *IP in current V2X infrastructure*

This paper is divided as follows. Section 2 summarizes the motivations and use cases of IP in V2X. Section 3 briefly describes the currently available, most significant standards. Section 4 introduces existing surveys from the domain and presents recent IPv6-based V2X solutions or IPv6 extensions designed for V2X support from the literature. Finally, Section 5 contains our final remarks and conclusion of the paper.

II. Motivations and use cases of IP in V2X

As we all realize, today's communications environment is exceptionally intricate, but it will be kept together and given coherence by the IP, which serves as the global language that underpins and connects all the elements of this ecosystem. Even though IP does not play an essential role nowadays in V2X deployments, the technological advancements of IP communications have substantially enhanced available solutions and allowed the V2X networks to move toward integrating systems. The main reason is that IP provides a unified layer for underlying technologies and higher-layer applications.

The IP-based communication APIs and the widespread infrastructure support ensure interoperability, such as a vehicle or a router when linked to the Internet; they enable any other local area network or radio network to attain a certain level of smooth cooperation. The utilization of IP is not confined to a specific domain. Instead, it can be applied across a wide range of industries, including but not limited to the World Wide Web, healthcare, government, education, and even V2X communication.

Most new vehicles have embedded built-in or connected brought-in Internet access, or a combination of the two. Vehicles with embedded connections have a built-in radiosystem that receives mobile cellular data directly using the 4G and 5G Uu interface. At the same time, some with connected connectivity use the driver's smartphone data to access the Internet for many reasons (e.g., video streaming, web browsing, and peer-to-peer). Moreover, interoperability is the capacity of systems, applications, or networks from various gateway to work together in a coordinated manner without the intervention of an end user. Interoperability enables unlimited data and resource sharing between systems through local and wide area networks, and this strategy allows the IP to ensure portability.

IP technology allows for the wider implementations and use of OTS (off-the-shelf) applications and services. On the one hand, IP networking is more affordable and accessible, allowing for rapid and cost-effective expansion of network endpoints. On the other hand, IP-based products can be easily updated to fix security issues or add new features.

Although non-IP became essential for early adopters due to its latency power, focused functionality, and well-scoped, safety-centric application areas, IP-based vehicle data transmission via wireless networks as a critical vehicle data application domain has also become significant in the scientific community. Due to IP's flexibility, multiple application areas have been broadly described in automotive research and department activities in recent years. Vehicles lacked suitable, cost-effective wiring technology, so IP introduced a new approach. According to an integration required to maintain an ever-increasing level of security, IP provides performance and maximum security to V2X [18]. There will be a significant benefit to connecting the IP and the vehicles and a large number of function applications based on this linking basis. Through the unique IP address, we can conduct remote access to specific automotive data, perform online operations, and perform remote defect diagnostics [13].

However, the IP's general portability and well-defined APIs are the primary motivation for its use in V2X. IP is a standardized communication protocol that enables long-term and sustainable use because of its widespread deployment in many industrial fields [14]. Moreover, the standardized network technology would simplify communication that would alleviate the usage of IP in the vehicle while also simplifying the vehicle's design. In addition, IP-based technologies entail a large body of knowledge already available, allowing for improved development, maintenance, and testing. Widespread use of IP, standardization, and openness, as well as an ample supply of high-quality chips on the market, leads to low product development and manufacturing costs. Also, IP could potentially pave the way in V2X for improved navigation, location-based services, and remote diagnostics [15].

In the automotive use cases of the 5G and beyond mobile cellular ecosystem, edge computing technology will provide an end-to-end architecture for distributing computing operations over localized networks. Using edge computing and improved network architecture increases the capacity to accommodate extensive automotive data exchange between vehicles and the cloud in a sensible manner [16]. Edge computing technology implementations nowadays mainly focus on IP since the access relies on the Uu interface, where IP is initially implemented, to support a generic platform where IP-based communication enables easy application development and deployment. Of course, PC5-based ad hoc V2X communication could benefit from IP compatibility similarly.

V2X Public-key Infrastructure (PKI) is a system that uses digital certificates to secure communication in vehicular networks. These digital certificates are used to verify the identity of the communicating devices, such as vehicles and roadside units, ensuring that only authorized devices can communicate with each other. The digital certificates used in V2X PKI contain information such as the device's identity, its public key, and the certificate authority's digital signature, which is used to verify the authenticity of the certificate. These certificates establish trust between the communicating devices and ensure that only authorized devices can participate in the communication.

Even non-IP V2X (current DSRC or PC5 implementations) cannot work without having a mobile cellular IP data connection because PKI mechanisms require Internet access. Since the security mechanisms rely on the IP link for the certificate communication, PKI needs to communicate with the infrastructure on the IP part of the architecture, which requires IP data exchange [17].

IP is a critical technology for 5G and beyond V2X/C-ITS deployments that support Uu communication and the Internet of Things (IoT) paradigm evolving towards the vehicular Internet. It also makes it easier to apply and use IP-enabled applications in vehicular communications [18]. For that, there are many benefits of IP in V2X; we can state some of them, such as large address space, which impacts the expansion of Internet continuity. Improved end-to-end connectivity, security service, and mobility. Furthermore, the inclusion of node auto-configuration mechanisms to aid in configuring connected vehicles, among other things. Also, it has a standard communication API and common addressing design. In addition, it is inter-domain communication without gateways, and finally, the transmission is independent of the physical network technology [14].

Pedestrians, and other Vulnerable Road Users (VRUs), such as bicyclists, may utilize their smartphones in various ways; For example, a pedestrian can acquire unique information that will be valuable for attracting attention throughout the activity. Aiming that, VRU protection through Vehicle-to-Infrastructure-to-Pedestrian (V2I2P) networking, such as safety aware navigation services, form another primary motivation and application area for IP in V2X; a vehicle and pedestrian using a smartphone connected with a network device for wireless communication with an RSU can avoid collisions. Moreover, vehicles and pedestrians can connect through an RSU, which provides wireless communication scheduling information [19].

In addition, a Tele-operated Driving (ToD) service can also become a significant advanced V2X use case driving V2N spectrum demand, and spectrum regulators must consider this to facilitate connection and automated mobility applications [20]. Furthermore, a remote driver runs a host vehicle in this use scenario. The host vehicle can accomplish this by providing video and sensor data to the remote driving through the uplink and receiving driving directions via the downlink [21], presumably over IP-based communication.

Internet Protocol appeared in practical V2X deployments to provide efficient, secure, and scalable communication between vehicles and other road users. A good example is Tiempo Secure, a company that is taking a leading role in promoting the use of IP in V2X communications [22]. They have invested over 13 years in developing unparalleled security IP, expertise, and secure software libraries allowing their clients to achieve the highest levels of security for their semiconductor products. Tiempo Secure has stated that IP integration is crucial for V2X communication, and their extensive experience and resources in IP-based security make them a valuable partner for organizations looking to implement V2X solutions. Another example is YOGOKO, a company that is taking the lead in end-to-end connectivity between vehicles and other road users, also advanced internet connectivity such as IPv6, which are utilized to provide expanded connectivity independent of existing access methods and accessible to users, services and applications [23].

III. Current major standards for IPv6-based V2X networking

3.1 The IEEE WAVE networking service

IEEE WAVE is divided into architecture, security services for application and management messages, and networking services (see Figure 2 for details). In this portion, we will discuss the networking service component of IEEE WAVE. Network services are a list of management plane and data plane functions defined in the specification at the network and transport layers that support WAVE communications. Furthermore, it specifies Wave Short Messages (WSM), which provide a WAVE-specific counterpart to IPv6 that applications can explicitly support. This standard also includes a Management Information Base (MIB) for the WAVE networking protocol stack [24].

WAVE networking services are part of the open system interconnect (ISO) communication stack's layers three (networking) and four (transport). [25]. WAVE Short Messages Protocol (WSMP) is a protocol used by DSRC networks to communicate safety information between vehicles and the roadside or just between cars [26].

The IEEE 1609.3 standard, by its practical feature, facilitates IPv6 address autoconfiguration without using the IPv6 Network Discovery (ND). The WAVE service advertising (WSA) for accessible service information transmitted by a WSMP message provides this functionality [7].

This specification aims to include addressing and routing facilities within a WAVE structure, allowing multiple stacks of upper layers above WAVE Networking Service and several lower layers below WAVE communication networks [25]. The Networking Services management functions monitor the transmit parameters (such as data rate and power levels for sending management frames defined in IEEE 1609.4) of data plane traffic [25].

On one hand, the IEEE 1609.3 Management plane facilities are referred to as the WAVE Management Entity (WME), and they provide Registration of an Application as one of the six practical tasks which are [24]:

- Registration of an Application
- Administration of WAVE Basic Service Sets (WBSS)
- Monitoring of channel use
- Configuration of IPv6
- Control of the received channel power indicator (RCPI)
- MIB maintenance

On the other hand, the IEEE 1609.3 Data plane facilities, which are designed for air interface performance and low latency in favor of vehicular applications, consist of the following [25]:

- Logical Link Control (LLC)
- WSMP
- IPv6
- Transmission Control Protocol (TCP) and other transport layer protocols User Datagram Protocol (UDP)

The TCP/IP stack in the network protocol stack follows IPv6 rather than IPv4 to take advantage of IPv6's immense address space and multiple mechanisms for auto-configuration. This IP stack accepts TCP and UDP as transport layer protocols and routes payloads for IP based on the transport layer protocol's port numbers [7].

3.1.1 Wave Short Message Protocol (WSMP)

WSMP protocol for the WAVE network layer allows for high-priority and time-critical connectivity [27]. The propagation of WSMP packets is a significant addition to WAVE networks. However, the WAVE standards require transmitting each WSMP packet using: a specified in-packet data rate, a defined in-packet channel number, and a defined in-packet transmission capacity [26].

3.1.2 Internet Protocol version 6 (IPv6) support

The WAVE standards workgroup adopted Internet Protocol version 6 (IPv6) as the network layer protocol. This decision reflects the WG's commitment to embracing modern and future-proof technologies within the WAVE standard framework. By selecting IPv6, the workgroup acknowledges the need for an advanced, scalable, and robust network layer protocol to support the diverse requirements of vehicular communication systems [26].

In addition to IPv6, the WAVE standard also supports the UDP (User Datagram Protocol), and

TCP (Transmission Control Protocol), protocol suites. This protocols are crucial in facilitating reliable and efficient data transmission within WAVE networks. The LLC sublayer is where IP traffic is sent and received [27].

3.1.3 Logical Link Control (LLC)

The LLC sublayer is used in Networking Services for both IPv6 and WSMP traffic. Moreover, the header of the LLC sublayer is just 2-octet long and includes an Ethertype that defines the higher layer protocol [25]. With a MAC frame field called Ethertype in the LLC header, the LLC sublayer identifies whether a WAVE MAC frame is meant for the safety application protocol stack or the non-safety application protocol stack [7].

3.1.4 Registration of an Application

To use WAVE networking facilities, all programs must first enroll with the WME. Each program is assigned a distinct provider service identifier (PSID). The registration data is stored in three tables, which are as follows: table of Provider Service Info, User Services Information Table, and Status of Applications Table [24].

3.1.5 WAVE Management Entity (WME)

It is a set of managerial functions that are needed to provide WAVE Networking Services [25]. Moreover, it performs WAVE Networking Management Services tasks such as handling services requests for higher layers, assigning channels, tracking WAVE Service Announcements, configuring IPv6 using data obtained from other WAVE devices, and maintaining MIB [27].

3.1.6 Maintenance of the Management Information Base (MIB)

The WME in a controlled WAVE system must keep a MIB containing configuration and status information. Higher Layers can navigate the MIB using WME-Get and WME-Set. Furthermore, the system can support additional MIBs linked to Networking Service (such as MIBs relevant to IPv6) [25].

3.1.7 WAVE Basic Service State (WBSS)

A BSS category includes a group of stations collaborating by operating in WAVE mode and communicating through a common Basic Service Set Identifier (BSSID). Moreover, WBSS is initiated when the radio in WAVE mode transmits a WAVE beacon containing all the data required for a receiver to enter [4].

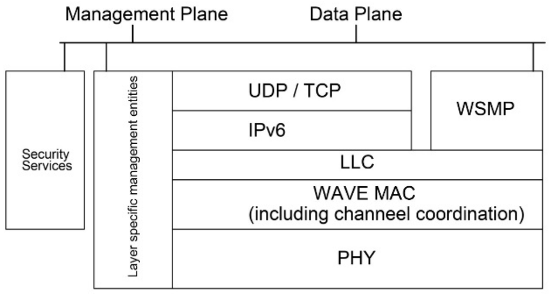

Figure 2. *The standardized protocol layer structure of WAVE*

3.2 IPv6 support in 802.11-OCB based ad hoc networks

The term OCB refers to a mode of service in 802.11-2016 networks, where a station (STA) is not part of the Basic Service Set (BSS) and does not use IEEE 802.11 authentication, affiliation, or data protection [28]. The IEEE 802.11-OCB mode is the ground base of the DSRC system (also known as ITS-G5 in Europe), making it simple for vehicles to connect [29]. The following are the significant characteristics of OCB mode: no IEEE 802.11 Beacon frames sent, no authentication is needed, and no affiliation is required [30].

Furthermore, WAVE also uses IEEE 802.11-OCB networks for vehicular communications.

Two stations (STAs) are connected through IEEE 802.11-OCB following in the considered link model. STAs in vehicular networks may be IP Road Side Units (RSUs) or IP On-Board Units (OBUs). Both connections are peer-to-peer, and several links may exist on the same radio interface. Although the IEEE 802.11-OCB standard is well-defined, and a legacy IPv6 stack will run on those connections, vehicular communications use opens up new possibilities [31].

The IPv6 protocol enables connectivity between nodes in close proximity through a single IEEE 802.11-OCB connection with minor modifications to the current protocol stack and just a few restrictions [28]. Moreover, allowing vehicles to link to the Internet through IEEE 802.11-OCB has received little attention, especially in the sense of IPv6 [29]. The IPv6 network layer works precisely the same way on 802.11-OCB as it does on Ethernet with the following variations: 1) Expectations owing to the difference in the process of the IPv6 network layer on IEEE 802.11 versus Ethernet; 2) Expectations attributable to the OCB existence of 802.11-OCB versus IEEE 802.11 [31]. In addition, Figure 3 depicts a more theoretical and extensive perspective of connections between IPv6 and 802.11-OCB layers [31]. In contrast, EPD is an Ethertype Protocol Discrimination that is runs on the top of the IP layer, and Link Layer Control Service Access Point (LLC_SAP) is the connection between IPv6 and EDP.

We introduce the essential characteristics of using the IPv6 protocol in IEEE 802.11-OCB-based V2X networks in the following sub-sections.

3.2.1 Maximum transmission unit (MTU)

On 802.11-OCB, the default MTU for IP packets is 1500 octets; however, any Internet connection must have a minimum MTU of 1280 and comply with all the other guidelines, including those concerning fragmentation [31]. In today's networks, a value of 1500 octets is considered the de facto standard [28].

3.2.2 Frame structure

IP packets must be sent as Quality of Services (QoS) data frames over 802.11-OCB. An 802.11-OCB packet is directly followed by an LLC header and an 802.11 header. In compliance with Ethertype Protocol Discrimination (EPD), 0x86DD must be set for the Type field in the LLC header. To give priority to traffic that is safety-critical and time-sensitive, it is advised to designate a priority value of 1 for the 802.11 data service mapping. By assigning a higher priority value, the system guarantees that this particular type of traffic is prioritized above other forms of data, enabling the prompt and dependable transmission of vital information [31].

3.2.3 Link-Local Address

If an Extended Unique Identifier (EUI-64) is used to form IPv6 link-local address, the procedure for doing so is the same as creating an IPv6 link-local address on Ethernet connections [31]. EUI-64 is an IPv6 link-local address created by mixing 16-bit 0xFFFE with a 48-bit MAC address. A collection of vehicles can construct a network structure out of 802.11-OCB interfaces, and the network must utilize an IPv6 link local prefix. The interfaces must also be allocated link-local IPv6 addresses [7].

3.2.4 Interface ID generation

According to the IPv6 Link-Local address development principles, the Interface ID (IID) is obtained from a physical (MAC) address in the standard way, using the EUI-64 protocol, and it has a length of 64 bits [28]. A predetermined prefix and the Interface ID are used to generate a link-local address. Furthermore, as a part of IPv6 Neighbor Discovery (ND), IPv6 employs Duplicate Address Detection (DAD) to ensure the distinction of an autoconfigured IPv6 address [7].

3.2.5 Address mapping

The guidelines for creating and mapping unicast and multicast addresses are the same as for IPv6 protocol service over IEEE 802.3 (Ethernet) and IEEE 802.11 (Wi-Fi) networks [28]. For unicast address it is a single interface's identification; when a packet is transmitted to a unicast address, it is sent to the interface specified by the address. While for multicast addresses, it is an identification for a collection of interfaces when multicast packets are transmitted to all interfaces designated by that address [32].

3.2.6 Subnet structures

When V2X network nodes are in close proximity, a subnet structure can be created [28]. IPv6 Neighbor Discovery (ND) is an essential component of the IPv6 suit. It is intended for transit and point-to-point connections (e.g., Ethernet). Moreover, IPv6 ND is assumed that the link layer can have adequate and secure multicast support for a variety of network operations, such as MAC Address Resolution (AR) and Duplicate Address Detection (DAD) [33].

IPv6 ND protocol necessitates reflexive properties (bidirectional connectivity), usually in P2P OCB connections. As a result, mapping an IPv6 subnet on an OCB network is only possible if all network nodes share a common physical broadcast domain. Furthermore, IPv6 ND necessitates nodes' continuous connectivity in the subnet to protect their addresses [31].

Finally, in P2P connections over IEEE 802.11-OCB, the baseline ND protocol must be supported since the IPv6 ND protocol for Ethernet was developed [28]. The general assumption of a stable multicast is not guaranteed, nor is the function of ND, DAD, and AR. Multicast communications over wireless networks are inefficient and disruptive to unicast traffic [12].

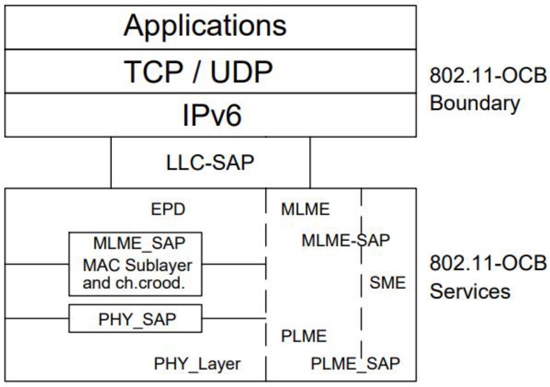

Figure 3. *The paradigm of IPv6 protocol utilization on an IEEE 802.11-OCB link*

3.3 GN6ASL: an adaption layer for IPv6 in V2X networks

3.3.1 ETSI ITS Architecture

The ETSI TC ITS has standardized the GeoNetworking (GN) protocol for routing packets via VANET (Vehicular Ad-Hoc Network) in its system architecture. The GN protocol employs the spatial routing theory, which routes packets depending on the geographical position of network nodes and the packet's destination [34].

The ETSI EN 302 636-6-1 standard [35], defines IPv6 packet transfer over the GeoNetworking (GN) Protocol. The GN protocol is a geographical addressing and routing scheme. With the prevalence of GPS systems, it is known that all nodes are aware of their own geographical location. Furthermore, they discover the location of their immediate neighbors [34]. An adaption sub-layer is specified for IPv6 transmission and is known as the GeoNetworking IPv6 adaption Sub-Layer (GN6ASL), which avoids changes to the standard IPv6 protocol [34]. The GN6ASL is responsible for connecting the IPv6 layer to the GN layer, allowing the GN layer acts as a sub-IP layer in IPv6. IPv6 datagrams are received by the GN layer, which encapsulates them into GN packets, adds a GN header, and sends them [34]. However, the GN protocol supports both point-to-point and point-to-multipoint communications and geographically scoped addressing techniques such as Geo-Anycast and Geo-Broadcast [35].

GN6ASL is a Geo-Networking adaption sub-layer that allows IPv6 packets to be transmitted over the network. The IPv6 layer is introduced to GN6ASL as a link-layer protocol that is based on Geo-Networking [35]. The GN6ASL standard distinguishes three types of virtual connections. The first virtual connection is reachable through symmetric links, using IPv6 ND with Stateless Address Autoconfiguration (SLAAC). In contrast, the other two are in a domain that can be transmitted, which are IPv6 link-local multicast packet distribution and IPv6 packet transmission across geographic boundaries [7]. SLAAC can be used in multi-hope vehicular ad hoc networks by leveraging the vehicle's geographical position recognition capability. The definition of IPv6 connection is applied in SLAAC to a well-defined geographical region connected with a connection point to an infrastructure-based network that serves as the IPv6 Access Router (AR) [36]. Furthermore, AR connects an ad hoc network to the Internet. The Geo ad-hoc router implements both the Geo Networking protocol and the GN6ASL. The Geo Ad-hoc and access router are logical network components that operate independently [35].

In addition, the Geo-Networking protocol offers a sub-IP multi-hop delivery service to upper layers. The services provided by GN6ASL to IPv6 are distributed by GN6 Service Access Point (SAP), which is built on the service user/provider model. GN SAP refers to a subset of the data SAP supported by Ethernet IEEE 802.3 to ensure backward compatibility with legacy IPv6 protocol implementations [35]. The architecture of GN6ASL in an ITS station is depicted in Figure 4.

The GN6ASL uses the GN geo-broadcasting capabilities to form link-local multicast messages to geographical regions [36].

3.3.2 GeoNetworking Protocol-provided services

GeoNetworking is a geographical routing protocol that distributes packets across the vehicle depending on node location. Nodes are expected to get their own geographical position through a location system. Upper protocol entities are serviced by the GeoNetworking protocol. In addition, the services are delivered through the GN SAP utilizing service primitives of various sorts that hold parameters and the top protocol entity's Protocol Data Unit (PDU). In GeoNetworking, a PDU of transport is designated a Service Data Unit (SDU). The SDU is supplemented with Protocol Control Information (PCI) and sent as a GN PDU to the peer entity. The GeoNetworking protocol uses the ITS Access Layer to deliver packet transport services. The GeoNetworking protocol defines several types of packet delivery services, including single-hop broadcast, Geo-unicast, Geo-broadcast, TSB (Topologically-Scoped Broadcast), and geo-anycast [37]. In Geo-unicast, the packet is sent hop by hop toward the endpoint and transmitted to the particular node. Furthermore, in Geo broadcast, the packet is geo-routed to a particular geographic zone and transmitted to all nodes inside the endpoint area [34].

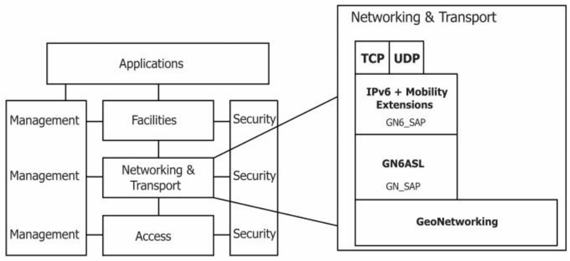

Figure 3. *The architecture of GN6ASL in an ITS station*

IV. IPv6-RELATED PROPOSALS FOR V2X SYSTEMS

As V2X systems progress, there is an increasing demand for reliable and future-proof connectivity solutions. The rise of IoT and the growing presence of connected vehicles and intelligent infrastructures necessitate addressing the limitations of current communication protocols in V2X systems. This advocates for adoption IPv6 as the standard communication protocol for V2X systems.

IPv6 offers numerous advantages compared to its predecessor, IPv4, which currently still even the IP-based V2X deployments. The primary advantage lies in the significantly expanded address space of IPv6, allowing for an almost limitless number of unique IP addresses. Given the expanding number of connected vehicles, infrastructure, and IoT devices, this scalability is crucial to accommodate the expected exponential growth of V2X networks.

4.1 Existing surveys

Available survey papers in the literature already cover some aspects of IP-based vehicular networking. Before highlighting recent research efforts on IPv6-equipped V2X, we introduce these surveys and highlight their main results.

In the article [38], the authors investigate the ITS discussions at the IETF and offer hope for TCP/IP protocols in vehicular communications, as TCP/IP protocol stacks are already present in many vehicles that are linked to the Internet. Furthermore, the authors analyzed the issue statement regarding the usage of IP in vehicle networks, highlighting the benefits of a narrow waist networking layer, including the support for link layers such as 802.11-OCB with a range of modulation methods. In addition, a proposal for an ITS WG was presented to standardize and profile IP protocols for establishing direct and secure communication between moving networks.

In the paper [7], the authors examine IP-based vehicular networking, which is characterized as vehicular networking that is purely based on the IP, and investigate the upcoming smart road vertical Internet of things (IoT) and Multi-access Edge Computing (MEC) applications. This paper focuses mainly on combining intra- and inter-vehicular networks and mobility management within the broader sense of globally protected IP vehicular networking. Furthermore, the authors address the core aspects of IP-based vehicular networking, emphasizing network architecture, IP address autoconfiguration, and accessibility control. In conclusion, this paper discusses the present and future paths of IP-based vehicular networking and solutions for self-driving cars, partly autonomous vehicles, and autonomous vehicles on smart roads.

The article [39], provides an overview of the contemporary internetworking architecture and engineering aspects. The author's objective in writing this survey is to show the deterioration of initial design goals and motives. They intend to develop a new set of rules that might be used to hypothesize architectural concepts for future network architecture. Furthermore, the authors demonstrate that the roots of Internet architecture are solid and well-engineered. Also, the authors of this paper discussed two topics: the design decision that led to the present network architecture and the impacts of this network architecture in terms of inertial effect, which make it hard for the Internet to advance from its current condition. In addition, regarding the V2X scenarios, the platform must be able to collect real-time data from various sources (e.g., road conditions, approaching signals, etc.) in order to make the right decisions about traffic stream and public safety while guaranteeing that the decision is served to an autonomous vehicle instantly, any delay causes knowledge to become outdated and useless. As a conclusion, looking ahead at new applications, the Internet as a single system will be hard to scale; it is easier to grow and embrace in multi-instance contexts.

The study [40], intends to provide both an introduction to vehicular networking for readers with a wide range of technical backgrounds and a comprehensive analysis and categorization of state of the art. The article is organized to guide the reader through the growth of the vehicular networking sector, moving from high-level aims to more granular solutions. In addition, the authors of this study describe the fundamental properties of vehicular networks, as well as an overview of applications and associated needs, obstacles, and possible solutions. Moreover, they have presented an overview of significant ITS initiatives and projects in the US, EU, and Japan, both present and past. Subsequently, the authors of this survey describe mainly concerted initiatives, which include standardization attempts and large projects.

Motivated by the potential of IPv6, ETSI also released a group report focusing on the general questions of IPv6-based vehicular networking [11]. This report collects the ongoing worldwide V2X standardization efforts aiming to introduce IPv6 in V2X communications and contains related applications and services. The document also reports on IPv6 transition strategies for vehicular communications and describes several concrete use cases in which the application of IPv6 could pose significant benefits to the system.

The IETF document [41] presents an up-to-date introduction and analysis of the use of IPv6 in Intelligent Transportation Systems (ITS) for vehicular networking. The main focus of the work is on the communication scenarios of V2V and V2I/I2V. The document first explains the use cases and requirements of C-ITS networking, then conducts a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy) in the context of IPv6-based vehicular networks. The analysis aims to identify the challenges and opportunities for using IPv6 in vehicular networks and the potential benefits for ITS.

Our current study contains the most recent authored papers on V2X systems in which IPv6 is also a key component. Our survey is broad in scope and does not only focus on specific technical concerns or feature areas of IPv6 in V2X. In the following sections, we list and briefly present V2X functional extensions and other proposals relevant to IPv6 communications in the vehicular domain. We classify the relevant articles into focus groups, and review recent works seeking to merge V2X and IPv6. We illustrate the core concepts and benefits of each of the surveyed articles.

4.2 Focus Group #1: IPv6 over IEEE WAVE

The Institute of Electrical and Electronics Engineers (IEEE) family of standards for Wireless Access in Vehicular Environment (WAVE) establishes an architecture and a supplementary standardized collection of services and interfaces that allow for secure V2I and V2V wireless communications. In addition, IEEE WAVE specifies the management structure, communication model security protocols, and architecture in vehicular environments [6]. Moreover, this standard is now regarded as the most promising technology for vehicular networks. Its goal is to promote compatibility and reliable safety communications in the vehicle environment [27].

4.2.1 IPv6 Operation for WAVE-Wireless Access in Vehicular Environments.

In the paper [42], the authors analyze IPv6 operation as defined in the IEEE 1609 family of specifications for WAVE networks and recognize areas where IPv6 procedures for WAVE networks are unclear. Never less, the author proposes a series of additional suggestions to allow optimal IPv6 service in WAVE networks and identifies the problems that have so far been left unresolved in terms of IPv6 function for WAVE. According to the authors, TCP is not often used in VANETs, leaving UDP the only feasible option inside the standard IPv6 stack. There are also technological explanations for why TCP may be a less suitable alternative for the vehicle network.

4.2.2 A Vehicular Mobility Management Scheme for a Shared-Prefix Model Over IEEE WAVE IPv6 Network.

In paper [43], the authors propose a vehicle mobility management technique using IEEE Wireless Access in Vehicular Environment (WAVE) IPv6 networks with a share-prefix architecture. This architecture includes vehicular mobility management neighbor discovery protocol (VMM-NDP) that is utilized for network attachment and handover operations, which manages route changes caused by changing serving Roadside Units (RSUs) within a shared prefix domain. Also, it conceals the IPv6 address change to Correspondent Nodes (CNs) by retaining the prior IPv6 address of the current vehicle is changed owing to the vehicle's relocation into a new shared domain.

Moreover, the authors of this paper noted issues with the present IPWAVE draft [43] of vehicular mobility management and conducted a comparative examination of their architecture to existing mobility architectures. The ns-3 (Network Simulator 3) [71] with its WAVE model library was applied to evaluate the proposed vehicle mobility management method. In conclusion, before the handover, the vehicle gets packets without loss. However, the disjoint scenario has considerable packet loss since RSU coverage does not overlap.

4.3 Focus Group #2: IPv6 over IEEE 802.11-OCB

Since the end of 2012, the Institute of Electrical and Electronics Engineers (IEEE) 802.11p modification has been part of IEEE 802.11 standard. It defines technical properties such as the usage of the 5.9 GHz bandwidth a 10 MHz channel and a novel operating mode to which all 802.11p compatible devices shall be set the Outside Context of Basic Service Set (OCB) mode. Moreover, the OCB mode mentioned in the previous sections, does not require authorization or identification, and the only parameters to configure are the channel bandwidth and central channel frequency [28].

4.3.1 Using IPv6 protocol in V2X networks based on IEEE 802.11-OCB mode of operation.

The paper [28], outlines the subject of using the IPv6 protocol on IEEE 802.11-OCB-based wireless networks. Furthermore, the authors discuss wireless network specifics and IP connectivity in V2X networks, emphasizing the layering and chosen IPv6 protocol properties. As a result, the IPv6 protocol, with just a few limitations, enables connectivity between nodes within a domain of each other over a monocular IEEE 802.11-OCB connection with minor modifications to the current protocol stack.

4.3.2 IPv6 Vehicular Communications over IEEE 802.11-OCB Wireless Link.

In this paper [29], the author proposes a possible IPv6 vehicular connectivity implementation using IEEE 802.11-OCB mode. As a result, the author discovered that the IPv6 link-local address was not configured automatically. The IPv6 Network Discovery (ND) protocol was either not operating or running automatically in standard protocol stacks.

4.4 Focus Group #3: IPv6 over GeoNetworking

GeoNetworking, as mentioned above, it is a network layer protocol that enables mobile ad hoc communication using wireless technologies (e.g., ITS-G5). It allows cellular connectivity without the requirement for a coordinating network. Moreover, GeoNetworking is a connectionless and completely dispersed network that operates on ad hoc network ideas with sporadic connectivity [44].

4.4.1 GeoNet: A project Enabling Active Safety and IPv6 Vehicular Applications.

In paper [45], the authors aim to introduce a reference specification for a geographic addressing and routing protocol with IPv6 compatibility that allows sending safety signals between vehicles and between vehicles and roadside facilities within a given destination location, which is called Geographic addressing and routing for vehicular communications (GeoNet). Thus, GeoNet's purpose was to develop and evaluate a networking framework as a discrete software module that could be integrated into Cooperative Systems. In conclusion, this project helped to establish the ETSI GeoNetworking standards and allowed clear IP communication between a vehicle and the infrastructure, also if distribution must be jumped through multiple vehicles or cached along the way.

4.4.2 IPv6 support for VANET with geographical routing.

In paper [46], the authors introduce a new method for effectively running IPv6 over VANET with geographical routing mechanisms, such as in the case of Car-to-Car Communication Consortium C2C-CC environments (CAR 2 CAR, 2021). Moreover, the authors proposed a scheme that runs IPv6 over VANET, which allows for effective IP setup and IP packet distribution without link-scope multicast. Vehicles can set up an IPv6 address at the global level and use it to connect with peers on and off the VANET. As a result, the solution uses inherent location control capabilities to carry out simple IPv6 protocols, including Neighbour Discovery and Stateless Address Autoconfiguration.

4.4.3 Experimental evaluation of an open-source implementation of IPv6 GeoNetworking in VANETs.

In paper [47], the authors explain CarGeo6, an open-source implementation of the IPv6 Geo Networking capability of the ITS station reference architecture, dependent on the Geo Net European Project output. Furthermore, the authors describe the CarGeo6 validation process and network efficiency assessment and compare these findings with Geo Net results. The authors attempted to analyze certain deployment efficiency factors, such as UDP's latency and packet processing ratio. The review of the findings revealed specific efficiency problems that could be improved by implementing certain extensions, such as the IP Next Hop cache to reduce latency and multi-hop beaconing to increase the efficiency of the multi-hope situation.

4.4.4 Real-vehicle integration of driver support application with IPv6 GeoNetworking.

In this paper [48], the authors design and implement an ITS network comprising two entities: an ITS server core and clients in vehicles that use IPv6 Geo-Networking, a geographical addressing and routing system created as part of the Geo-Net project [49]. Since the author's application promotes practical use case scenarios, he incorporated it into INRIA's vehicular platform. As a result, the system was incorporated into an outdoor field research area and worked successfully in practical cases as the Geo-Net project's final demonstration at INRIA.

4.4.5 Geographical information extension for IPv6: application to VANET.

In paper [50], the authors investigate and evaluate various options for enhancing IPv6 with geographical information. The paper's main challenge is incorporating geographical location into the existing IP architecture. However, to complete this challenge, the author investigated four major solutions: application layer expansion, IPv6 utilizing a sender-oriented protocol, IPv6 using a receiver-oriented routing protocol, and solely geographically based.

4.5 Focus Group #4: IPv6 support using NEMO

RFC 5177 defines Network Mobility (NEMO) [51] Internet standards track protocol. The protocol ensures that every node in a mobile network maintains its session while the network traverses, as a whole unit, changing its point of connection to the Internet and hence its reachability in the topology. NEMO comprises one or more IP subnets linked to the Internet [52].

4.5.1 Securing Vehicular IPv6 Communications.

In the article [53], the authors' work focuses on a particular scenario of vehicle-to-infrastructure connectivity, even though the network model discussed provides a V2V context.

Moreover, the authors' discussion depends on IPv6 technologies such as Internet Key Exchange protocol (IKEv2) and Internet Protocol security (IPsec) to support secure connectivity channels between a mobile router, that connects user and on-board devices and the accessibility, which is situated on the infrastructure side in a connected remote point. The paper's proposed paradigm focuses on maintaining IPv6 continuity for in-vehicle nodes via Network Mobility basic support (NEMO). The findings show that using the security proposal does not trigger a significant network overload. Because of the increased packet transfer times and the extra control details in IPv6 packets, there is just a slight efficiency loss as the traffic volume is boosted to make the most of the network.

4.5.2 Towards seamless inter-technology handovers in vehicular IPv6 communications.

In this paper [54], the author proposes an instantiation of the ISO/ETSI reference architecture for vehicular cooperative systems by implementing a real vehicular network based on IPv6 and NEMO's mobility infrastructure with Multiple Care-of Addresses Registration (MCoA) support. As a result, the tests show that the combination of NEMO/MCoA/802.21 MIH (Media Independence Handovers) system inside a vehicular communication stack can provide continuous connectivities during handovers while drastically reducing the time required for this process.

4.5.3 Continuous IPv6 Communications in a Vehicular Networking Stack for Current and Future ITS Services.

In paper [55], the authors describe a vehicular networking connectivity stack dependent on the well-known IPv6 protocol that adheres to current ISO/ETSI trends toward a popular ITS connectivity architecture while also offering modern extensions for handover and protection support. Furthermore, the primary goal in designing this stack was to provide integrated control of IPv6 mobility; the proposal is built on NEMO to enable future point of connection improvements at the IPv6 level. Still, it also includes an authentication/authorization system to automate access to protect domains and expand functionality from supporting handovers.

4.5.4 Car-to-Car and Car-to-infrastructure communication system based on NEMO and MANET in IPv6.

In paper [56], the authors discuss recent progress made by the IETF and NEMO in supporting IPv6 and its associated protocols. They also emphasize the need for the data exchange between vehicle and infrastructure and between vehicles, to be Internet-based and use IPv6 protocols. Moreover, the authors have examined the essential functional needs of the IPv6 communication system for ITS, and the purpose of the NEMO WG is to provide network mobility support to allow the complete IPv6 network to alter its point of attachment to the Internet topology. Following the presentation of the experimental framework for integrated communications, a test was performed utilizing the 4G access cube, a Linux MIPS Box from 4G Systems, and another test for V2V communications based on ad hoc networking. Furthermore, this project aims to create networks that can self-organize themselves with moving vehicles. In conclusion, IPv6 is the underlying communication protocol that will be used in ITS applications. The IPv6-associated concepts of NEMO, ad-hoc networking, and other technologies match the ITS communication system architecture requirements.

4.6 Focus Group #5: IPv6 Moving Object Networking (ipmon)

The ipmon was an IETF Birds of a Feather (BOF) session in late 2022, an informal conversation regarding a specific issue of interest to the Internet Engineering Task Force community. The BOF was declined, but planned activities proposed there were partly imported into the IPv6 Maintenance (6man) WG.

In case of support, the (ipmon)-defined [57] working group will focus on V2X use cases where IPv6 is well-suited as a networking technology and will build IPv6-based solutions to provide fast and encrypted communication between moving items and stationary systems. The key deliverables of this group will be IETF documents that define the procedures for transmitting IPv6 datagrams over either 3GPP 5G V2X or IEEE 802.11bd V2X. The already available draft documents are introduced in this focus group.

4.6.1 Vehicular Neighbor Discovery for IP-Based Vehicular Networks.

This IETF draft document [58] defines Vehicular Neighbor Discovery (VND) as an IPv6 ND extension for IP-based vehicular networks. To improve operational efficiency and save wireless bandwidth and vehicle energy, the authors propose a multi-hop Duplicate Address Detection (DAD) technique and an improved Address Registration. Furthermore, three additional neighbor discovery options are specified to advertise network prefixes and services within a vehicle.

4.6.2 Vehicular Mobility Management for IP-Based Vehicular Networks.

This document [59] defines a design for Vehicle Mobility Management (VMM) in IP-based vehicular networks. This IETF draft aims to provide an efficient mobility management system to facilitate V2X communications on the road. The VMM uses the mobility information and trajectory of each vehicle registered in the vehicular cloud's Traffic Control Center (TCC). Moreover, it can offer a moving car a proactive and smooth handoff as it moves along its trajectory.

4.6.3 Basic Support for Security and Privacy in IP-Based Vehicular Networks.

When implementing IP-based in self-driving situations, data interchange between self-driving vehicles is crucial to vehicle safety since received data from other vehicles may be utilized as inputs for vehicle operations. For that, this document [60] addresses potential security threats and privacy concerns in IPWAVE. Also, it suggests defenses for such attacks and weaknesses.

4.6.4 Context-Aware Navigation Protocol for IP-Based Vehicular Networks.

This document [61] presents a Context-Aware Navigation Protocol (CNP) for IP-based vehicular networks that would allow vehicles on road infrastructures to navigate cooperatively. The CNP protocol employs an IPv6 Neighbor Discovery (ND) option to send driving information. However, CNP attempts to improve driving safety by utilizing a lightweight method of transmitting driving information.

4.6.5 Service and Neighbor Vehicle Discovery in IPv6-Based Vehicular Networks.

This document [62] demonstrates using Domain Name System (DNS) resolution logic to discover a neighbor vehicle or the appropriate services. In addition, the authors raise two concerns related to IPv6 communication between neighbor vehicles and between vehicles and servers. As a result, a DNS Service Discovery and Multicast DNS (DNS-SD/mDNS)-based solution was provided to solve these issues. Also, IPv6 ND's can be used in ITS in conjunction with DNS-SD/mDNS to send certain needed information.

4.6.6 DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks.

A DNS Name Autoconfiguration (DNSNA) protocol was presented in this document [63] for the global DNS names of Internet of Things (IoT) devices in IP-based vehicular networks. As a result, in wired and wireless networks, the DNS name of an IoT device can be autoconfigured with the device's model information. IoT users on the Internet may quickly determine each device in a network for monitoring and remote-control.

4.7 Focus Group #6: Other IPv6 extensions for VANETs

Several IPv6 extensions have been proposed and implemented for VANETs. These extensions are designed to address the unique challenges of VANETs, such as mobility, low power, scalability, and efficient routing of packets. Moreover, these extensions are also proposed to improve the performance and security of VANETs.

4.7.1 eHealth Service Support in Future IPv6 Vehicular Networks.

In paper [64], the authors propose combining vehicular and eHealth testbeds and a lightweight auto-configuration approach built on a DHCPv6 extension to support IPv6 compatibility with a small number of messages. Moreover, the authors reflect on incorporating eHealth in V2I environments, encouraging Internet usage from vehicle settings to spread health-related data. Experimentation shows that eHealth-specific data can be transmitted over IPv6 from a vehicular environment using an experimental IPv6 implementation over High-Speed Packet Access (HSPA) in the beyond 3G era of mobile communications.

4.7.2 Application of IPv6 multicast to VANET.

In paper [65], the authors investigate and analyze the possibilities for incorporating an IPv6 multicast mechanism in Vehicular Ad hoc Networks (VANET). Moreover, the authors propose encoding GPS coordinates into IPv6 multicast addresses and using digital maps to map multicast addresses to dedicate locations. Consequently, when using their proposed software, appropriate delays are indicated, and streamlined delays are demonstrated when using the static multicast daemon.

4.7.3 A study of IP-based vehicular gateway with IPv6.

In this paper [66], the authors introduce the plan and deployment of an IPv6-based in-vehicle gateway (IVG) for end-to-end connectivity between an IPv6-based controller area network (CAN) unit and an Ethernet-based segment. Furthermore, the following characteristics of this architecture and deployments: 1) different in-vehicle bus nodes will seamlessly link to the IPv6 internet and exchange data through interconnection; 2) each vehicle node is allocated a distinct IPv6 address.

As a result, the terminal monitor will use the unique IPv6 address to reach the in-vehicle CAN node, send instructions, request data, and perform remote diagnostics on IP-based vehicles.

4.7.4 IPv6-based vehicular cloud networking.

In this paper [70], the authors suggest an IPv6-based vehicular cloud network (VCN). Information acquisition is accomplished by IP-based unicast rather than content-centric broadcasting to lower the cost of content acquisition. Moreover, a modern address structure is suggested to connect an IP address and a type of content and use this modern address (the contents can be obtained in a unicast manner from the closest vehicular cloud member). Also, the authors have proposed a specific scheme for this purpose.

Consequently, after the scheme has been tested and assessed, it demonstrates that it efficiently decreases the cost of content acquisition.

4.7.5 Research on IPv6 address configuration for VANET.

In article [67], the authors suggest an IPv6 setup scheme for VANETs. In the system, each Access Point (AP) has its own address space and the authority to delegate an IPv6 address to an On-board Unit (OBU). The address setup task is therefore spread through all APs in a VANET. In addition, the authors suggest an address recovery algorithm in which an AP will restore IPv6 address services published by OBUs in a timely and efficient manner. As a result, the proposed scheme lowers the cost of address configuration, shortens the latency in address configuration, and increases the performance rate of address configuration.

4.7.6 Cellular V2X IPv6 Transaction Support via Global IP Address.

This technical report [68] contains all of the Application Programmable Interfaces (APIs) required for on-board Unit (OBU) and Roadside Unit (RSU) implementations of such IPv6 global sessions. Furthermore, this study explains how to create the WAVE Router Advertisement (WRA) on the RSU and how the OBU must enable general IPv6 internet access via the RSU.

4.7.7 Cross-layered Architecture for Securing IPv6 ITS Communication: Example of Pseudonym Change.

In paper [69], the authors provide an ITS station reference design recently created by ETSI TC ITS and ISO TC204 WG16. In addition, the authors suggest a Service Access Point definition for securing Cooperative ITS communication using IPv6 by developing generic instructions for activating/deactivating IPv6 security services; and by developing generic commands for requesting atomic security operations. Moreover, the authors also illustrate an example of how the suggested generic instructions are utilized in the pseudonym change. Lastly, this study contributes to the ISO/ETSI ITS station reference architectural standardization, and the example in this study serves as a starting point for critically considering the cost of the pseudonym change at the IPv6 layer.

Table 1. Details of the surveyed papers

1st Group		**IPv6 over IEEE WAVE**		
Reference	Topic	Focus of evaluation	Evaluation parameters	Main results
[42]	-Analyzing IPv6 operation defined in the IEEE 1609 family of specifications for WAVE networks.	-Collects areas where IPv6 procedures for WAVE networks are not well investigated, lists issues, and analyses the main challenges of providing IPv6 for WAVE networks.	-IPv6 link model. -IPv6 addressing model. -WAVE interface in Link model. -Neighbor asymmetry.	-The authors have identified the problems that have been left unresolved in terms of the IPv6 function for WAVE.
[43]	-A vehicle mobility management technique with a share-prefix architecture.	-Describes the issue and offers a partial solution based on the specifications.	-Enhances the effectiveness of wireless communication. - Supports pseudonym.	-Before the handover, the vehicle gets packets without any loss. However, there is considerable packet loss in the disjoint scenario.

2nd Group		**IPv6 over IEEE 802.11-OCB**		
Reference	Topic	Focus of evaluation	Evaluation parameters	Main results
[28]	-Outlines the use of the IPv6 protocol on IEEE 802.11-OCB-based wireless networks.	-Terminology description used in V2X networks and the IPv6 protocol properties in greater depth.	-Forming stable Interface ID. -Creating subnet structure in V2X.	-IPv6 protocol enables connectivity between nodes within a domain of each other over a monocular IEEE 802.11-OCB connection with minor modifications to the current protocol stack.
[29],	-Suggestion for a possible IPv6 vehicular connectivity implementation	-The system architecture of IPv6 vehicular communications over IEEE 802.11-OCB mode to aid IPv6 adoption in vehicular communications.	- Implementation alternative for the IPv6 over IEEE 802.11-OCB.	-The author discovered that the IPv6 link-local address wasn't configured automatically, and the IPv6 Network Discovery (ND) protocol was either not operating or running automatically in standard protocol stacks.

3rd Group		**IPv6 over GeoNetworking**		
Reference	Topic	Focus of evaluation	Evaluation parameters	Main results
[45]	-Introduce reference specification for geographic addressing.	-Describe the problem and provide a solution based on requirements.	-Impact of traditional attacks on vehicles operating IPv6 GeoNetworking.	-Establishing the ETSI GeoNetworking standards by allowing clear IP communication.
[46]	-New method for effectively running IPv6 over VANET.	-C2C-CC architecture as a reference frame, using IPv6 operation without relying on link-scope.	-IPv6 using geographical routing mechanisms. -Neighbor Discovery.	-Inherent location management capabilities to carry out basic IPv6 protocols.
[50]	-Evaluation of various options for enhancing IPv6 with geographical info.	-Geographical addressing information extension for IPv6	-Decreasing the dependency. -IPv6 using geographical-based protocol	-Application layer expansion, IPv6 utilizing a sender-oriented protocol, uses a receiver-oriented routing protocol.

[47]	-Implementation of IPv6 Geo Net capability of ITS station.	-Reporting the validation procedure and the network performance evaluation of CarGeo6.	-Evaluating the latency on IPv6 hosts connected to a mobile router (MR).	-Specific efficiency problems that could be improved by implementing certain extensions to reduce latency.
[48]	-Implementing an ITS Network that uses IPv6 Geo-Networking	-Establishing a geographical addressing and routing mechanism in the GeoNet project.	-Testing multi-hop communication in VANET. -Demonstrating the efficiency of incorporating the ITS functionality on top of IPv6 GeoNetworking.	-The system was incorporated into an outdoor field research area and worked successfully in practical cases as the Geo-Net project's final demonstration at INRIA.

4th Group	**IPv6 support using NEMO**			
Reference	Topic	Focus of evaluation	Evaluation parameters	Main results
[53]	-Focusing on the security of IPv6 in the particular case of V2I communications.	-Experimental evaluation of the proposal using networking technology focused on base network efficiency and handover.	-Handover time operation.	-No significant overload in the network is generated by the security proposed in the paper.
[54]	-Suggestion of instantiating the ISO/ETSI reference architecture by implementing a real vehicular network based on IPv6.	-Handover time and characteristics.	-Network efficiency with a particular emphasis on handover time.	-The combination of NEMO/MCoA/802.21 MIH system can provide continuous connectivity during handovers while drastically reducing the time required for this process.
[55]	-Description of a vehicular networking stack based on IPv6 protocol that adheres to current ESO/ETSI trends.	-New extensions for enhancing security and handover assistance and integrating of IETF protocols.	-IPv6 feasibility to minimize handover latency.	-An authentication/authorization system to automate access to protect domains and expand functionality from supporting handovers.
[56]	-Description of the recent work at the IETF and NEMO	-Experimental framework for integrated communications	- Creating networks that can self-organize themselves with moving vehicles	-The IPv6-associated concepts of NEMO, ad-hoc networking, and other technologies match the ITS communication system architecture requirements.

5th Group	**IPv6 Moving Object Networking (ipmon)**			
Reference	Topic	Focus of evaluation	Evaluation parameters	Main results
[58]	-Defining (VND) as an IPv6 ND extension for IP-based vehicular networks.	-Multihop Duplicate Address Detection (DAD) technique and an improved Address Registration are used to improve efficiency.	-Neighbor Discovery -Duplicate address detection	-An efficient mobility management design is also provided to facilitate efficient V2X communications.
[59]	-Defining a design for Vehicle Mobility Management (VMM) in IP-based vehicular networks.	-Provide an efficient mobility management system to facilitate V2X communications on the road.	-Mobility management	-VMM can offer a moving vehicle with a proactive and smooth handoff as it moves along its trajectory.
[60]	-Addressing potential security threats and privacy concerns in IPWAVE.	-Suggests defense for such attacks and weaknesses.	-Security and privacy	
[61]	-Context-Aware Navigation Protocol (CNP) for IP-based vehicular networks.	-The CNP protocol employs an IPv6 Neighbor Discovery (ND) option, which sends driving information.	-Neighbor Discovery	-CNP attempts to improve driving safety by utilizing a lightweight method of transmitting driving information.

[62]	-Demonstrating how to use Domain Name System (DNS) resolution logic to discover a neighbor vehicle.	-Two concerns were raised related to IPv6 communication between the neighbor vehicle and between the vehicle and server	-Neighbor vehicle -Link layer address	- DNS Service Discovery and Multicast DNS (DNS-SD/mDNS)-based solution was provided to solve these issues. IPv6 ND's can also be used in ITS in conjunction with DNS-SD/mDNS to send information.
[63]	-Presenting a DNS Name Autoconfiguration (DNSNA) protocol.	-An IoT device autoconfiguration strategy based on device configuration and DNS search list.	-Network Discovery -Router Advertisement -Stateless Address Autoconfiguration	-The DNS name of an IoT device can be autoconfigured with the device's model information. IoT users on the Internet may quickly determine each device in a network for monitoring and remote control.

6th Group	Other IPv6 extensions for VANETs			
Reference	Topic	Focus of evaluation	Evaluation parameters	Main results
[65]	-Analyzing the possibilities for incorporating an IPv6 multicast mechanisms	- Encoding GPS coordinates into IPv6 multicast addresses.	- Measuring the delay of multicast.	-Appropriate delays are indicated using easy the proposed software, and the static multicast routing daemon shows streamlined delays.
[67]	-Suggestion of an IPv6 setup scheme for VANET.	-Introducing an address recovery algorithm and testing the proposed scheme's results.	-CAC, HID, and the suggested scheme are tested.	-The scheme lowers the cost of address configuration, shortens the latency in address configuration, and increases the performance rate of address configuration.
[70]	-Suggestion of an IPv6-based vehicular cloud network (VCN) in which information acquisition is accomplished by IP-based unicast.	-New address structure to establish the relationship between an IP address and the contents, which can be acquired in a unicast manner from the nearest vehicular cloud member.	-Assessing the multimedia file-sharing service and matching the expense in this paper's scheme to the cost in another paper's current scheme.	-After the scheme has been tested and assessed, it demonstrates that it efficiently decreases the cost of content acquisition.
[66]	-Deployment of an IPv6-based in-vehicle gateway (IVG) for end-to-end connectivity.	-Evaluating the conversion of IPv4 to IPv6 and developing an address mapping system.	-A unique IPv6 address to reach the in-vehicle CAN node.	-Testing IPv6 address to reach the in-vehicle CAN node, send commands and request information and perform remote diagnostics on IP-based vehicles.
[64]	-Combination of vehicular and eHealth testbeds and a lightweight auto-configuration approach built on a DHCPv6 extension.	-Evaluate the IPv6 vehicular interface that incorporates eHealth sensors and allows for the transmission of collected health-related data.	-Comparing the throughput between IPv6 access point name (APN) with IPv4 APN for eHealth application in V2X.	-Experimentation shows that eHealth-specific data can be transmitted over IPv6 from a vehicular environment using an experimental IPv6 implementation over (HSPA).
[69]	-Suggesting a Service Access Point definition for securing C-ITS communication using IPv6.	-Developing generic instructions for activating/deactivating IPv6 security services.	-Illustrating an example of how the suggested generic instructions are utilized in the pseudonym change	-This study contributes to the ISO/ETSI ITS station reference architectural standardization.

V. CONCLUSION

We examined the current status of IPv6 integration in V2X networks in-depth, focusing on the supported IPv6 features. IPv6 allows IP-enabled technologies, applications, and services to be seamlessly implemented and used in vehicular communications. Moreover, it was also claimed that IPv6 has many benefits that resolve essential needs of collaborative vehicular communication, such as a broad address space due to the depletion of IPv4 address space, affecting internet continuity growth. IPv6 only should be encouraged to be the primary IP-based solution for V2X, with other transitions seen as supplemental [9]. In addition, this paper also presents details on existing standards of V2X-related IPv6 supporting schemes (IEEE WAVE networking layer, IPv6 over IEEE 802.11-OCB, and ETSI GN6ASL). Our survey concluded that we still should consider IPv6 as the primary driver of the global network connectivity in V2X to provide the reachability of Internet resources. Several authors focused on using IPv6 as the primary communication protocol instead of the dedicated protocol developed specifically for each wireless communication system in the cooperative ITS domain. The main proposal is to consider IPv6 a universal protocol even in V2X wireless communications. Available results in the literature proposed multiple modifications, missing features, and protocol improvements to cope with the requirements of V2X. These papers analyzed the existing issues of IPv6 when it is used in V2X, including security. Despite these results, IP(v6) communication is still considered outside of the scope of safety V2X applications but started to gain momentum in other use cases due to the increasing proliferation of 5G technologies and C-V2X.

AUTHOR CONTRIBUTIONS

H. Farran: Conceptualization, Theoretical analysis, Writing.

L. Bokor: Supervision, Review and editing.

DISCLOSURE STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] 5G American (2018) ‘5G Americas White Paper: Cellular V2X Communications Towards 5G’, http://Www.5Gamericas.Org.

[2] Sattiraju, R. *et al.* (2020) ‘Link level performance comparison of C-V2X and ITS-G5 for vehicular channel models’, *arXiv*.

[3] Group, I. 1609 W. (2014) IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture, IEEE Std 1609.0-2013.

[4] Jiang, D. and Delgrossi, L. (2008a) ‘IEEE 802.11p: Towards an international standard for wireless access in vehicular environments’, IEEE Vehicular Technology Conference, pp. 2036–2040. https://doi.org/10.1109/VETECS.2008.458

[5] Gräfling, S., Mähönen, P. and Riihijärvi, J. (2010) ‘Performance evaluation of IEEE 1609 WAVE and IEEE 802.11p for vehicular communications’, ICUFN 2010 - 2nd International Conference on Ubiquitous and Future Networks, pp. 344–348. https://doi.org/10.1109/ICUFN.2010.5547184

[6] ITS Standards Program | Fact Sheets | ITS Standards Fact Sheets (2021). Available at: https://www.standards.its.dot.gov/Factsheets/Factsheet/80 (Accessed: 23 April 2021).

[7] Jeong, J. et al. (2021) ‘A comprehensive survey on vehicular networks for smart roads: A focus on IP-based approaches’, Vehicular Communications. Elsevier Inc., 29, p. 100334. https://doi.org/10.1016/j.vehcom.2021.100334

[8] Miao, L., Virtusio, J. J. and Hua, K. L. (2021) ‘Pc5-based cellular-v2x evolution and deployment’, Sensors (Switzerland), 21(3), pp. 1–14. https://doi.org/10.3390/s21030843

[9] ETSI - Automotive Intelligent Transport | Intelligent Transport Systems (ITS) (2021). Available at: https://www.etsi.org/technologies/automotive-intelligent-transport (Accessed: 24 April 2021).

[10] Lee, L. S. (2011) ‘The New Internet Protocol’, Internet Auditor, 68(11), pp. 21–23.

[11] Report, G. (2020) ‘Etsi gr ip6 030 V.1.1.1 (2020-10)’, 1, pp. 1–30.

[12] Litvik, I. D. and J. (2021) ‘An overview of neighbor discovery issues in vehicular V2X networks’, pp. 80–83.

[13] Yu, H. et al. (2012) ‘Implementation of an IP-based In-Vehicle Gateway, version 6’, World Automation Congress Proceedings, pp. 4–7.

[14] Steffen, R. et al. (2009) ‘Design and Realization of an IP-based In-car Network Architecture’. https://doi.org/10.4108/icst.isvcs2008.3543

[15] Bello, L. lo (2012) ‘The case for Ethernet in automotive communications’.

[16] AECC (2020) ‘General Principle and Vision-White Paper’, pp. 1–15.

[17] Haidar, F., Kaiser, A. and Lonc, B. (2018) ‘On the performance evaluation of vehicular PKI protocol for V2X communications security’, IEEE Vehicular Technology Conference, 2017-Septe, pp. 1–5. https://doi.org/10.1109/VTCFall.2017.8288286

[18] European Commission (2021) ‘5G HarmoniseD Research and TrIals for serVice Evolution between EU and China’, pp. 1–42.

[19] Hwang, T. and Jeong, J. (Paul) (2014) ‘SANA: Safety-aware navigation application for pedestrian protection in vehicular networks’. IEEE, 9502, pp. 127–138. https://doi.org/10.1007/978-3-319-27293-1_12

[20] Linget, T. (2021) ‘5GAA Automotive Association Technical Report Tele-Operated Driving(ToD): System Requirements Analysis and Architecture’. Available at: www.5gaa.org.

[21] 5GAA (2020) ‘5GAA TR S-200137 Study of spectrum needs for safety related intelligent transportation system - day 1 and advanced use cases’, pp. 1–50.

[22] Tiempo Secure (2023). Available at: https://www.tiempo-secure.com (Accessed: 4 January 2023).

[23] YoGoKo - Mobility data exchange made simple (no date). Available at: https://www.yogoko.com/ (Accessed: 28 January 2023).
[24] Weil, T. (2009) 'Service management for ITS using WAVE (1609.3) networking', 2009 IEEE Globecom Workshops, Gc Workshops 2009. https://doi.org/10.1109/GLOCOMW.2009.5360714
[25] Transportation, (2010) 1609.3 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)— Networking Services IEEE Vehicular Technology Society.
[26] Morgan, Y. L. (2010) 'Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics', IEEE Communications Surveys and Tutorials, 12(4), pp. 504–518. https://doi.org/10.1109/SURV.2010.033010.00024
[27] Ahmed, S. A. M., Ariffin, S. H. S. and Fisal, N. (2013) 'Overview of wireless access in vehicular environment (wave) protocols and standards', Indian Journal of Science and Technology, 6(7), pp. 4994–5001. https://doi.org/10.17485/ijst/2013/v6i7.18
[28] Dolnak, I., Jantosova, A. and Dado, M. (2020) 'Using IPv6 protocol in V2X networks based on IEEE 802.11-OCB mode of operation', 2nd International Conference on Electrical, Communication and Computer Engineering, ICECCE 2020, (June), pp. 12–13. https://doi.org/10.1109/ICECCE49384.2020.9179202
[29] Mugabarigira, B. A. (2020) 'IPv6 Vehicular Communications over IEEE 802 . 11-OCB Wireless Link', (Mm), pp. 482–483.
[30] Yoshizawa, T. and Preneel, B. (2019) 'Survey of Security Aspect of V2X Standards and Related Issues', 2019 IEEE Conference on Standards for Communications and Networking, CSCN 2019. IEEE, pp. 1–5. https://doi.org/10.1109/CSCN.2019.8931311
[31] RFC 8691: Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11 (no date). Available at: https://www.rfc-editor.org/rfc/rfc8691.html (Accessed: 30 April 2021).
[32] Thomson, S., Narten, T. and Jinmei, T. (2007) 'IPv6 Stateless Address Autoconfiguration Status', Request for Comments, pp. 1–30. Available at: https://tools.ietf.org/html/rfc4862.
[33] IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases (no date). Available at: https://tools.ietf.org/id/draft-ietf-ipwave-vehicular-networking-13.html (Accessed: 30 April 2021).
[34] Victor Sandonis, I. S. and , Maria Calderon, M. U. (2016) 'Vehicle to Internet communications using the ETSI ITS GeoNetworking protocol', Transactions on emerging telecommunications technologies, 25(3), pp. 294–307. https://doi.org/10.1002/ett
[35] ETSI (2013) 'EN 302 636-6-1 - V1.2.1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols', 1, pp. 1–47.
[36] Gramaglia, M. et al. (2012) 'IPv6 address autoconfiguration in geonetworking-enabled VANETs: Characterization and evaluation of the ETSI solution', Eurasip Journal on Wireless Communications and Networking, 2012. https://doi.org/10.1186/1687-1499-2012-19
[37] ETSI (2011) 'Vehicular communications ; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications';, Intelligent Transport Systems, 1, pp. 1–75. Available at: http://www.etsi.org/deliver/etsi_ts/102600_102699/1026360401/01.01.01_60/.
[38] Petrescu, A. et al. (2016) 'Intelligent Transportation Systems and the IETF To cite this version ', 12(1), pp. 11–14.
[39] Makhijani, K. et al. (2018) 'A Survey of Internet Protocol and Architectures in the Context of Emerging Technologies', (c), pp. 14–19.
[40] Karagiannis, G. et al. (2011) 'Vehicular Networking : A Survey and Tutorial on Requirements ', 13(4), pp. 584–616.
[41] IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases (2021). Available at: https://datatracker.ietf.org/doc/draft-ietf-ipwave-vehicular-networking/21/ (Accessed: 30 April 2021).
[42] Baccelli, E. et al. (2011) 'IPv6 Operation for WAVE - Wireless Access in Vehicular Environments To cite this version : HAL Id : hal-00651593 IPv6 Operation for WAVE - Wireless Access in Vehicular Environments'.
[43] Ko, M., Kim, H. and Min, S.-G. (2022) 'A Vehicular Mobility Management Scheme for a Shared-Prefix Model over IEEE WAVE IPv6 Networks', IEEE Access. IEEE, 10(September), pp. 1–1. https://doi.org/10.1109/access.2022.3201520
[44] ETSI (2014) 'ETSI EN 302 636-1 v1.2.1 (2014-04) Intelligent Transport Systems; Vehicular Communications; GeoNetworking; Part 1: Requirements', 1, pp. 1–14. Available at: http://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf.

[45] Mariyasagayam, M. N., Menouar, H. and Lenardi, M. (2008) 'GeoNet: A project enabling active safety and IPv6 vehicular applications', Proceedings of the 2008 IEEE International Conference on Vehicular Electronics and Safety, ICVES 2008, pp. 312–316. https://doi.org/10.1109/ICVES.2008.4640897

[46] Choi, J. H. et al. (2008) 'IPv6 support for VANET with geographical routing', Proceedings - 2008 8th International Conference on Intelligent Transport System Telecommunications, ITST 2008, pp. 222–227. https://doi.org/10.1109/ITST.2008.4740261

[47] Toukabri, T. et al. (2011) 'Experimental evaluation of an open source implementation of IPv6 GeoNetworking in VANETs', 2011 11th International Conference on ITS Telecommunications, ITST 2011, pp. 237–245. https://doi.org/10.1109/ITST.2011.6060060

[48] Noguchi, S. et al. (2011) 'Real-vehicle integration of driver support application with IPv6 GeoNetworking', IEEE Vehicular Technology Conference, pp. 2–6. https://doi.org/10.1109/VETECS.2011.5956756

[49] Geoaddressing and Georouting for vehicular communications | GeoNet Project | FP7 | CORDIS | European Commission (no date). Available at: https://cordis.europa.eu/project/id/216269 (Accessed: 15 May 2021).

[50] Khaled, Y., Tsukada, M. and Ernst, T. (2009) 'Geographical information extension for IPv6: Application to VANET', 2009 9th International Conference on Intelligent Transport Systems Telecommunications, ITST 2009, pp. 304–308. https://doi.org/10.1109/ITST.2009.5399339

[51] RFC 5177: Network Mobility (NEMO) Extensions for Mobile IPv4 (2008). Available at: https://www.rfc-editor.org/rfc/rfc5177.html (Accessed: 4 December 2022).

[52] RFC 4885: Network Mobility Support Terminology (2007). Available at: https://www.rfc-editor.org/rfc/rfc4885 (Accessed: 4 December 2022).

[53] Fernández, P. J. et al. (2016) 'Securing Vehicular IPv6 Communications', IEEE Transactions on Dependable and Secure Computing, 13(1), pp. 46–58. https://doi.org/10.1109/TDSC.2015.2399300

[54] Fernández, P. J. et al. (2017) 'Towards seamless inter-technology handovers in vehicular IPv6 communications', Computer Standards and Interfaces. Elsevier, 52(February), pp. 85–96. https://doi.org/10.1016/j.csi.2017.01.013

[55] Santa, J. et al. (2012) 'Continuous IPv6 Communications in a Vehicular Networking Stack for Current and Future ITS Services', pp. 1–7.

[56] Ernst, T. and De La Fortelle, A. (2006) 'Car-to-car and car-to-infrastructure communication system based on nemo and manet in IPV6', 13th World Congress on Intelligent Transport Systems and Services, (September 2014).

[57] IPv6 Moving Object Networking (ipmon) (2022). Available at: https://datatracker.ietf.org/doc/bofreq-jeong-ipv6-moving-object-networking-ipmon/ (Accessed: 14 November 2022).

[58] Jeong, et al. (2022) draft-jeong-ipwave-vehicular-neighbor-discovery-14 - Vehicular Neighbor Discovery for IP-Based Vehicular Networks. Available at: https://datatracker.ietf.org/doc/draft-jeong-ipwave-vehicular-neighbor-discovery/ (Accessed: 14 November 2022).

[59] Jeong, J. P. (2022) draft-jeong-ipwave-vehicular-mobility-management-08 - Vehicular Mobility Management for IP-Based Vehicular Networks. Available at: https://datatracker.ietf.org/doc/draft-jeong-ipwave-vehicular-mobility-management/ (Accessed: 14 November 2022).

[60] Jeong, Jaehoon (2022) draft-jeong-ipwave-security-privacy-06 - Basic Support for Security and Privacy in IP-Based Vehicular Networks. Available at: https://datatracker.ietf.org/doc/draft-jeong-ipwave-security-privacy/ (Accessed: 15 November 2022).

[61] Jeong, J. (2022) draft-jeong-ipwave-context-aware-navigator-06 - Context-Aware Navigation Protocol for IP-Based Vehicular Networks. Available at: https://datatracker.ietf.org/doc/draft-jeong-ipwave-context-aware-navigator/ (Accessed: 15 November 2022).

[62] CNNIC, Z. Y. (2022) 'Service and Neighbor Vehicle Discovery in IPv6-Based Vehicular Networks draft-yan-ipwave-nd-10.txt'. Available at: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf.

[63] Jaehoon, J. P. (2022) draft-jeong-ipwave-iot-dns-autoconf-13 - DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks. Available at: https://datatracker.ietf.org/doc/draft-jeong-ipwave-iot-dns-autoconf/ (Accessed: 15 November 2022).

[64] Imadali, S. et al. (2013) 'eHealth service support in future IPv6 vehicular networks', Future Internet, 5(3), pp. 317–335. https://doi.org/10.3390/fi5030317

[65] Khaled, Y. et al. (2009) 'Application of IPv6 multicast to VANET', 2009 9th International

Conference on Intelligent Transport Systems Telecommunications, ITST 2009, pp. 198–202. https://doi.org/10.1109/ITST.2009.5399356

[66] Yu, H. et al. (2018) 'A study of IP-based vehicular gateway with IPv6', International Journal of Embedded Systems, 10(2), pp. 168–179. https://doi.org/10.1504/IJES.2018.090573

[67] Wang, X. and Zhong, S. (2013) 'Research on IPv6 address configuration for a VANET', Journal of Parallel and Distributed Computing. Elsevier Inc., 73(6), pp. 757–766. https://doi.org/10.1016/j.jpdc.2013.02.002

[68] Qualcomm (2022) 'C- V2X IPv6 Transaction Support via Global IP Address Revision history'.

[69] Lee, J. H., Ernst, T. and Bonnin, J. M. (2011) 'Cross-layered architecture for securing IPv6 ITS communication: Example of pseudonym change', 2011 3rd International Workshop on Cross Layer Design, IWCLD 2011. IEEE. https://doi.org/10.1109/IWCLD.2011.6123070

[70] Wang, X. (2015) 'IPv6-based vehicular cloud networking', IEEE Communications Letters, 19(6), pp. 933–936. https://doi.org/10.1109/LCOMM.2015.2422703

[71] Riley, G. F. and Henderson, T. R. (2010) 'The ns-3 network simulator', *Modeling and Tools for Network Simulation*. Springer Berlin Heidelberg, pp. 15–34. https://doi.org/10.1007/978-3-642-12331-3_2/COVER

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution NonCommercial (CC BY-NC 4.0) license.