A Comprehensive Survey on Vehicular Networks for Smart Roads: A Focus on IP-Based Approaches

Jaehoon (Paul) Jeong[a,*], Yiwen (Chris) Shen[b], Tae (Tom) Oh[c], Sandra Céspedes[d,e], Nabil Benamar[f], Michelle Wetterwald[g], and Jérôme Härri[h]

[a]*Department of Computer Science & Engineering, Sungkyunkwan University, Suwon, 16419, Republic of Korea; (Email: pauljeong@skku.edu)*
[b]*Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon, 16419, Republic of Korea; (Email: chrisshen@skku.edu)*
[c]*Department of Information Sciences & Technologies, Rochester Institute of Technology, NY, 14623-5603, USA; (Email: tom.oh@rit.edu)*
[d]*Department of Electrical Engineering, Universidad de Chile, Santiago, Chile; (Email: scespedes@ing.uchile.cl)*
[e]*NIC Chile Research Labs, Santiago, Chile*
[f]*Department of Computer Sciences, Moulay Ismail University of Meknes, Morocco; (Email: n.benamar@est.umi.ac.ma)*
[g]*Netellany, France; (Email: michelle.wetterwald@netellany.fr)*
[h]*Communication Systems Department, EURECOM, France; (Email: jerome.haerri@eurecom.fr)*

Abstract

In vehicular communications, the use of IP-based vehicular networking is expected to enable the deployment of various road applications, namely for vehicle-to-infrastructure (V2I), infrastructure-to-vehicle (I2V), vehicle-to-vehicle (V2V), and vehicle-to-everything (V2X) communications. This paper surveys vehicular networking based solely on the Internet Protocol (IP), which is defined as IP Vehicular Networking, in smart road scenarios. This paper presents a background tutorial on IP-based networking, with an overview of the main technologies enabling IP vehicular networking, vehicular network architecture, vehicular address autoconfiguration, and vehicular mobility management. IP-based vehicular use cases for V2I, V2V, and V2X are presented and are analyzed based on the latest standardization and research activities. The paper highlights several research challenges and open issues that must be addressed by researchers, implementers and designers, and discusses security considerations that should be factored in for a secure and safe vehicular communication. Finally, this paper offers current and future directions of IP-based vehicular networking and applications for human-driving vehicles, partially autonomous vehicles, and autonomous vehicles in smart roads.

Keywords: IP vehicular networking; network architecture; IP address autoconfiguration; mobility management; standardization; security

1. Introduction

Over the past decades, vehicular networking has been gaining more and more attention from both academia and industry along with other emerging technologies such as automated vehicles, Internet of Things (IoT), and artificial intelligence (AI). Recently, the increasing presence of connected and automated vehicles (CAV) technologies has become a new promising pattern that may come to fundamentally change the landscape of smart road networks, also called Intelligent Transportation Systems (ITS). For the purpose of connecting vehicles with wireless communications, the industry has developed IEEE 802.11p-based wireless communication technologies, called Dedicated Short-Range Communications (DSRC) [1] in the US and ITS-G5 [2] in the European Union (EU). Alternatively, the 3rd Generation Partnership Project (3GPP) has completed the first version of Long-Term Evolution (LTE) V2X technology specification [3] in 4G-LTE network, and been investigating new use cases and technology requirements in 5G and beyond networks [4, 5]. For enabling vehicular networking, the US Federal Communications Commission allocated wireless channels in the range of 5.850 $\sim$ 5.925 GHz [1], whereas the EU assigned a radio spectrum in the 5.875 $\sim$ 5.905 GHz band [6]. DSRC/ITS-G5 or LTE/5G V2X technologies provide V2I, I2V, V2V and V2X communications, which is an important building block for future ITS applications. Considering the peculiar dynamics of vehicular mobility, along with the local scope targeted by DSRC, ITS-G5 and LTE/5G V2X for ITS applications (e.g., intersection collision and lane change warning), non-IP protocol stacks have been developed by IEEE Wireless Access in Vehicular Environments (WAVE) [7, 8, 9, 10], ISO Communications Access for Land Mobiles (CALM) [11], and the European Telecommunications Standards Institute (ETSI) ITS [12]. Those standards use different kinds of messages such as the basic safety message (BSM) [10], the cooperative awareness message (CAM) [13], and the decentralized environmental notification message (DENM) [14], respectively.

However, with the currently growing interest of new vertical markets (e.g., IoT and Multi-access Edge Computing (MEC) [15]) in vehicles' on-board sensors and intra-vehicular network, as well as the need for global connectivity in support of future tele-operated or automated driving, IP is again attracting increasing attention, because IP is the most popular network protocol for the Internet. None of the IEEE WAVE, ISO CALM,

*Corresponding author

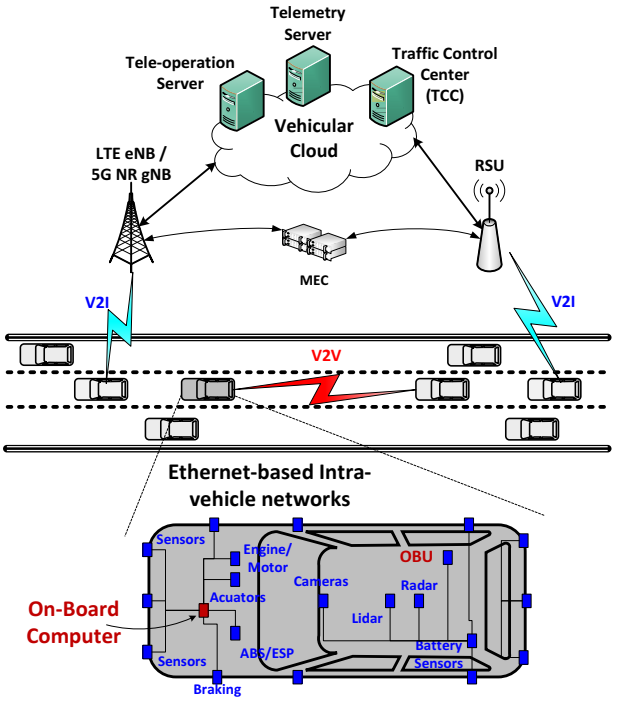


Figure 1: An architecture of vehicular networks.

and the ETSI ITS stacks are exclusive to IP, but IP-specific vehicular networking, notably for safety-related applications, has been subject to less research over the past decade. Both WAVE 1609.3 [9] and CALM [16] allow for UDP/IP layers to transmit non-safety-related messages over the DSRC access technology. ETSI has integrated a GeoNetworking encapsulation for transmitting IP packets over ITS-G5 access technologies [17]. However, IP mechanisms (e.g., retrieving and maintaining IP addresses, IP multihop wireless/wired connectivity, the need for automotive industry-grade security and privacy, and mechanisms to integrate intra-/inter-vehicular networks into an IoT or MEC framework) have not yet been addressed in a coherent way. Fig. 1 shows an architecture of vehicular networks having both V2I and V2V communications using either LTE/5G V2X or DSRC links. Vehicles in this architecture can communicate with a remote traffic control center via a vehicular cloud, and other services provided by vendors can also be used, e.g., tele-operation for vehicles and vehicle telemetry services. A vehicle can share its internal sensors and devices information with others via Ethernet-based intra-vehicle networks by an on-board unit (OBU) for enhanced smart road services.

1.1. Definitions

This subsection defines new terms used in this paper.

Road-Side Unit (RSU): An entity has the Internet access by either a wired or wireless network interface and at least one wireless communication interface for vehicular communications, such as DSRC and/or LTE/5G V2X. It can be placed at different locations, e.g., street intersections, bus stops, and road guide signs. It can be a router for routing IP packets in the Internet, which can be called a wireless Access Router (AR) or an Internet Gateway (IGW).

Table 1: Acronyms and Abbreviations

Acronym	Description
AAA	Authentication, Authorization, and Accounting
AR	Access Router
BU	Binding Update
CALM	Communications Access for Land Mobiles
CMA	Central Mobility Anchor
CN	Corresponding Node (or Correspondent Node)
DAD	Duplicate Address Detection
DetNet	Deterministic Networks
DHCPv6	Dynamic Host Configuration Protocol version 6
DMM	Distributed Mobility Management
DNS	Domain Name System
DSRC	Dedicated Short-Range Communications
DTN	Delay-Tolerant Network
EPC	Evolved Packet Core
GN	Geographic Networking
HA	Home Agent
HMIPv6	Hierarchical Mobile IPv6
ICMPv6	Internet Control Message Protocol version 6
IEEE 802.11-OCB	IEEE 802.11 Outside the Context of a Basic Service Set
IGW	Internet Gateway
IKEv2	Internet Key Exchange version 2
IPsec	Internet Protocol Security
IPWAVE	IP Wireless Access in Vehicular Environments
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MAP	Mobility Anchor Point
MAR	Mobile Access Router
MR	Mobile Router
MEC	Multi-access Edge Computing
MF	Mobility Function
MIPv6	Mobile IPv6
MN (MT)	Mobile Node (Mobile Terminal)
mDNS	Multicast Domain Name System
mMAG	Moving MAG
ND	Neighbor Discovery
NEMO	Network Mobility Basic Support Protocol
OBU	On-Board Unit
OFS	Open-Flow Switch
PBA	Proxy Binding Acknowledgment
PBU	Proxy Binding Update
PDN	Packet Data Network
PDP	Packet Data Protocol
PMIPv6	Proxy Mobile IPv6
RA	Router Advertisement
RS	Router Solicitation
RSU	Road-Side Unit
SDN	Software-Defined Networking
SDO	Standards Developing Organization
SLAAC	Stateless Address Autoconfiguration
TCC	Traffic Control Center
TSN	Time-Sensitive Networking
VANET	Vehicular Ad Hoc Networks
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access in Vehicular Environments
WRA	WAVE Router Advertisement
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

On-Board Unit (OBU): An entity which has at least one dedicated wireless interface, such as DSRC and/or LTE/5G V2X, that can communicate with other OBUs and RSUs; it is installed on a vehicle.

Vehicle: An entity which is an automobile driven by a driver or a computer (in the case of a self-driving vehicle). It includes an OBU and a navigation system using Global Positioning System (GPS) technology. A vehicle can also be called a Mobile Node (MN), or a Mobile Host (MH) in different contexts.

Traffic Control Center (TCC): An entity which manages and orchestrates road systems, including road communication infrastructure (e.g., RSU), traffic lights, navigation systems, road surveillance systems, and loop detectors. It can track vehicles moving on the road networks under its control and maintains traffic statistics per road segment such as average speed, vehicle inter-arrival time, and speed deviation. It is a core part of the vehicular cloud for vehicular networking.

We also use a set of acronyms and abbreviations throughout this paper, as shown in Table 1.

1.2. Existing Surveys

A number of surveys have been published on a variety of areas related to vehicular networking recently. Table 2 shows a list of related recent existing surveys and their focuses.

Khelifi et al. [18] surveyed recent advances and implementations of a named data networking for vehicular networks, focusing on the information-centric networking aspect. Qayyum et al. [19] reviewed security problems using machine learning (ML) techniques in vehicular networks, and highlighted challenges for using the techniques. It particularly focused on adversarial ML attacks on connected and autonomous vehicles. Wang et al. [20] provided a survey about networking and communications in autonomous driving, paying attention to intra- and inter-vehicle communications. Peng et al. [22] studied vehicular communications from a network layer aspect, and investigated different techniques for manual and automated driving vehicular networks, respectively. Rettore et al. [21] introduced a vehicular data space in vehicular networks for ITS, with a perspective of data collection, creation, preparation, processing, and use. Siegel et al. [24] investigated the architectures, enabling technologies, applications, and challenges in connected vehicles environments, especially concentrating on available technologies and applications. MacHardy et al. [25] reviewed various access technologies for V2X communications, and provided a general overview of the current research challenges in each access technology. Ahmed et al. [26] touched advances in several aspects of cooperative vehicular networking, including physical, medium access control, routing protocols, link scheduling, and security. Other surveys focused on different topics in vehicular networking, such as heterogeneous vehicular networking [27], vehicular social networking [28], routing [29], authentication and privacy [23, 30], and pseudonym [31].

Each of these surveys either focused on non-IP vehicular networking or addressed IP-vehicular networks only in a generic context (e.g., only mobility and only routing). Moreover, no recent survey has specifically described the detailed aspects of IP-based vehicular networking, such as network architecture, IP address autoconfiguration, mobility management, activities in Standards Developing Organizations (SDOs), as well as research challenges and issues.

1.3. The Current Survey

The objective of this paper is to provide a coherent survey of the state-of-art of IP vehicular networking in the context of future smart road vertical applications of IoT and MEC, notably integrating intra- and inter-vehicular networks and mobility management in the larger context of global secured IP vehicular networking. Different from the existing surveys, this paper discusses various key aspects in the IP-based vehicular networking, focusing on network architecture, IP address autoconfiguration, and mobility management. In particular, this paper presents the current standardization status in different SDOs for IP-based vehicular networks. Furthermore, it also delivers an in-depth analysis for the problems and issues when the vehicular networking uses the existing IP-based networking mechanisms. More importantly, this paper shares a variety of research challenges and issues for the future IP-based vehicular networking.

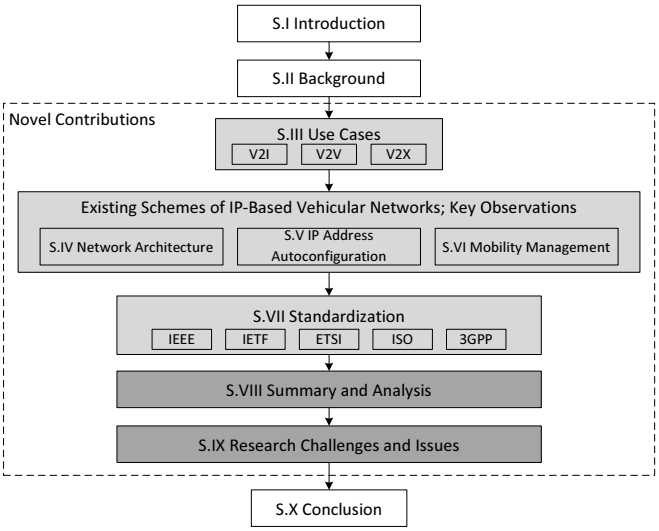


Figure 2: Structure of this paper.

Fig. 2 shows the structure of this paper. First, this paper begins with a short background knowledge introduction and tutorial about IP networks (Section 2), and use cases (Section 3) for IP vehicular networking. Second, it reviews and compares the different IP network architectures (Section 4), IP address configuration schemes (Section 5), identity management, IP networking, and IP mobility management mechanisms (Section 6) that have been developed for vehicular networks. Third, various security challenges and solutions are discussed in the mechanisms for vehicular network architecture and mobility management (Section 4 and 6). Fourth, this paper explains standardization activities in several SDOs for IP vehicular networks (Section 7). Finally, a summary and analysis are provided (Section 8), and the research challenges and issues (Section 9) are discussed. Then we conclude this paper in Section 10.

Table 2: Related Recent Existing Surveys

Year	Survey	Focus
2020	Khelifi et al. [18]	Named data networking for vehicular networks in the context of information-centric networking.
2020	Qayyum et al. [19]	Challenges by adversarial machine learning techniques.
2019	Wang et al. [20]	Intra- and inter-vehicle communications for autonomous driving.
2019	Rettore et al. [21]	Vehicular data space in vehicular networks.
2019	Peng et al. [22]	Communication techniques for manual and automated driving vehicular networks.
2019	Ali et al [23]	Authentication and privacy schemes.
2018	Siegel et al. [24]	Available technologies and applications in connected vehicles environments.
2018	MacHardy et al. [25]	Various access technologies for V2X communications.
2018	Ahmed et al. [26]	Several aspects of cooperative vehicular networking.

2. Background of IP-based Vehicular Networking

The DSRC and IEEE 802.11-Outside the Context of a Basic (OCB) standards have defined a non-IP short message service in vehicular environments and stated that the standard IPv6 operations can work in DSRC-based vehicular networks. The 3GPP V2X architecture also supports both IP and non-IP data packet transmissions. The major operations in the standard IPv6 include router and prefix discovery, address autoconfiguration, neighbor discovery, mobility management, and security. In this section, we review those background protocols and operations.

2.1. Router and Prefix Discovery

For connecting to the Internet, a host with a network interface card needs to have an IP address. In the basic support of IPv6, a host can have a link-local IPv6 address and a unique global IPv6 address. To configure the IPv6 addresses, an interface of a host when powered on firstly multicasts a Router Solicitation (RS) message to all connected routers and hosts. All routers that received the RS message shall reply with a Router Advertisement (RA) message that includes IPv6 address prefix information of the current subnet for the host. With the prefix information, the interface of the host can configure its tentative global IPv6 address based on a certain rule [32, 33]. If receiving several prefixes from different routers, the host needs to select a default router to use [34]. If no RA message is received, then the host only configures a link-local IPv6 address. The prefix discovery process can also be done by Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [35], where a router manages a host's IPv6 address and other information such as DNS server addresses and NTP server addresses.

2.2. Address Autoconfiguration

By receiving the IPv6 address prefix information, a host can autoconfigure its IPv6 address by the prefix and an interface identifier [32] that can uniquely identify itself on the current subnet, which usually is derived from its MAC address. While configuring a global IPv6 address, the host can also configure a link-local address used by the current link.

To ensure the uniqueness of an autoconfigured IPv6 address, IPv6 uses the Duplicate Address Detection (DAD) mechanism [32] as part of IPv6 ND. Through the DAD, a unique link-local address for a host can be autoconfigured. Generating a link-local address uses a predefined prefix, FE80::0, and its interface identifier. The DAD procedure is performed as follows. An IPv6 host sends a Neighbor Solicitation (NS) message to its neighbor hosts on the current link. If any neighbor host replies with a Neighbor Advertisement (NA) message indicating the same link-local address, this indicates that the link-local address is already used by the responding host, so it cannot be used by the host that sent the NS message. In this case, the link-local address of the host should be configured either manually or in other ways with a possible unique interface identifier. On the other hand, if there is no NA message for the NS message, the host can use the link-local address as its own one.

For the autoconfiguration of a global IPv6 address, the IPv6 host needs to perform the DAD of such a global address. Note that some implementation of IPv6 takes advantage of the DAD of its link-local address, and skips the DAD of its global address as an optimization, assuming that the interface identifier of a link-local address is used for that of a global address of every IPv6 host in the same subnet. However, for the privacy concern of a global address, the interface identifier may not be based on the interface identifier of a link-local address so that an eavesdropper cannot track an IPv6 host with a specific global address [36, 37]. Thus, every IPv6 host needs to perform the DAD of its global address in addition to the DAD of its link-local address.

2.3. Neighbor Discovery in IPv6

In addition to the router and prefix discovery as well as the address autoconfiguration, a host also needs to resolve the IPv6 address of other hosts (e.g., terminals and routers) by a table (called Neighbor Cache Entries) that maps an IPv6 address and a MAC address of other hosts. To build this address resolution mapping table, a host sends requests to other hosts to ask their link-layer addresses. For doing so, a host multicasts NS messages to a multicast address of a target host, and the target host unicasts an NA message that includes the link-layer address information back toward the requesting host.

To further detect whether a neighbor host can be reached or not, a host needs to do the Neighbor Unreachability Detection (NUD) [38] procedure. A host can leverage two kinds of information to do that:

- Hints from upper layer messages from a neighbor, such as acknowledgments from TCP layer returned to the host, which can indicate that the neighbor is reachable;

- Unicasting NS messages toward a neighbor, which requests the neighbor to reply with NA messages that can confirm the reachability of it.

After obtaining the reachability information, the host updates its neighbor cache to reflect the latest state of the neighbor. A host needs to maintain the neighbor cache by periodically sending NS messages to neighbors, so that when a new packet arrives in the network layer, the host can immediately send the packet to its destination.

2.4. Mobility Management

Currently there are several standard network-layer mobility management protocols, such as Mobile IPv6 (MIPv6) [39], Hierarchical Mobile IPv6 (HMIPv6) [40], Proxy Mobile IPv6 (PMIPv6) [41], and Network Mobility Basic Support Protocol (NEMO-BS) [42]. Wakikawa et al. surveyed other mobility support schemes for the Internet in [43].

MIPv6 is a protocol that allows an MN (e.g., a vehicle) to communicate with a CN (e.g., a vehicular cloud server) without changing its IPv6 address when the MN moves across different subnets. In MIPv6, an MN needs to send a binding update message to its home agent (HA) when it moves to another subnet away from its HA, and traffic from the CN is redirected to the MN via the HA. Through a route optimization using a binding update of the MN to the CN, the CN can directly send the MN its traffic packets. In doing so, MIPv6 can provide an MN with a global mobility management support.

To reduce the additional delay caused by MIPv6 in certain scenarios, HMIPv6 proposes a hierarchy in which a mobility anchor point (MAP) is placed near an MN to function as a local HA. In HMIPv6, an MN sends binding updates to the local MAP instead of the remote HA and CNs, so the traveling time of packets can be reduced.

In the case of a mobile network (e.g., a vehicle with an onboard IP subnet), the MN becomes a Mobile Router (MR) with routing capabilities. In such a scenario, NEMO-BS provides a solution that constructs a bi-directional tunnel between the MR and its HA, so that all of the traffic from/to the local moving network can be tunneled via the HA for IP mobility support.

To remove the involvement of the MN in the mobility management process, PMIPv6 provides an MN with a network-based mobility mechanism that uses a mobile access gateway (MAG). The MAG works as the attachment entity for the MN and performs all of the signaling for the mobility management process with the local mobility anchor (LMA) on behalf of the MN. In this way, the MN is not involved in the signaling between the MAG and the LMA. PMIPv6 is a localized mobility management protocol, which means that it is designed to work on a single administrative domain (i.e., an autonomous domain that manages the LMA and the MAGs).

The above solutions tackle mobility management problems from different scenarios. However, when dealing with a scene of vehicular networks, those mobility support schemes may burden the wireless network (i.e., the infrastructure) due to the lack of considerations in terms of the high mobility nature of vehicular networks and peer-to-peer (P2P) communication models. For example, since it can pass the wireless coverage of a new MAG during the handoff in PMIPv6, a vehicle may not be served by the new MAG due to either the delay of the handoff or the wrong selection for a new MAG.

2.5. IP Security

The standard IP layer network security mechanisms are Internet Protocol Security (IPsec) [44, 45, 46, 47] and its key exchange protocol, Internet Key Exchange version 2 (IKEv2) [48]. IPsec uses two basic protocols, i.e., IP Authentication Header (AH) [45] and IP Encapsulating Security Payload (ESP) [46], for IP layer security, where any IPsec-enabled system shall support ESP and may support AH. ESP provides both integrity and confidentiality for data traffic, which has two modes, transport mode and tunnel mode. Transport mode lets an ESP header be inserted between an IP header and an upper layer header (e.g., TCP and UDP headers), and tunnel mode adds an ESP header before an IP header. To make IPsec be executed, two peers (e.g., a vehicle and a cloud server) need to make Security Associations (SAs) that build a bidirectional IPsec path between them. An IPsec module in each peer obtains various parameters via SA for securing future data traffic, including data encapsulation mode, encryption algorithm, authentication algorithm, key exchange, and SA lifetime. For encrypting data, IPsec employs different symmetric encryption algorithms, e.g., Advanced Encryption Standard (AES). When a host receives an encrypted packet, the packet needs to be authenticated by Keyed Hash Message Authentication Code (HMAC). A digital signature using HMAC was generated by the transmitter of the packet and included in Integrity Check Value (ICV) of an AH or ESP header of the encrypted IP packet. The receiving host can verify the digital signature in ICV with a manually pre-shared key or an automatic exchanged key by a hash algorithm, such as Message Digest Algorithm (MD5), Secure Hash Algorithm (SHA1), and SHA2. IKEv2 helps distribute encryption keys and authentication keys between two peers by UDP protocol.

For securing the IPv6 ND protocol, a SEcure Neighbor Discovery (SEND) improvement was proposed [49, 50]. SEND introduced a set of mechanisms to improve the ND security, such as an Authorization Delegation Discovery (ADD) process and an address ownership proof mechanism. A host can accept a default router only when this router has a certification path with a trust anchor. If the certification path is not available, then the authorization delegation discovery process can be used. A node uses Cryptographically Generated Addresses (CGA) [37] to ensure the ownership of ND messages by a public-private key pair. SEND also suggested other improvements for ND, such as a new RSA Signature option for integrity of ND messages, and two new ND options to prevent replay attacks.

3. IP Vehicular Networking Use Cases

Various ITS applications and services can be developed in consideration of IP networking. This section surveys the use cases related to V2I, V2V, and V2X communications.

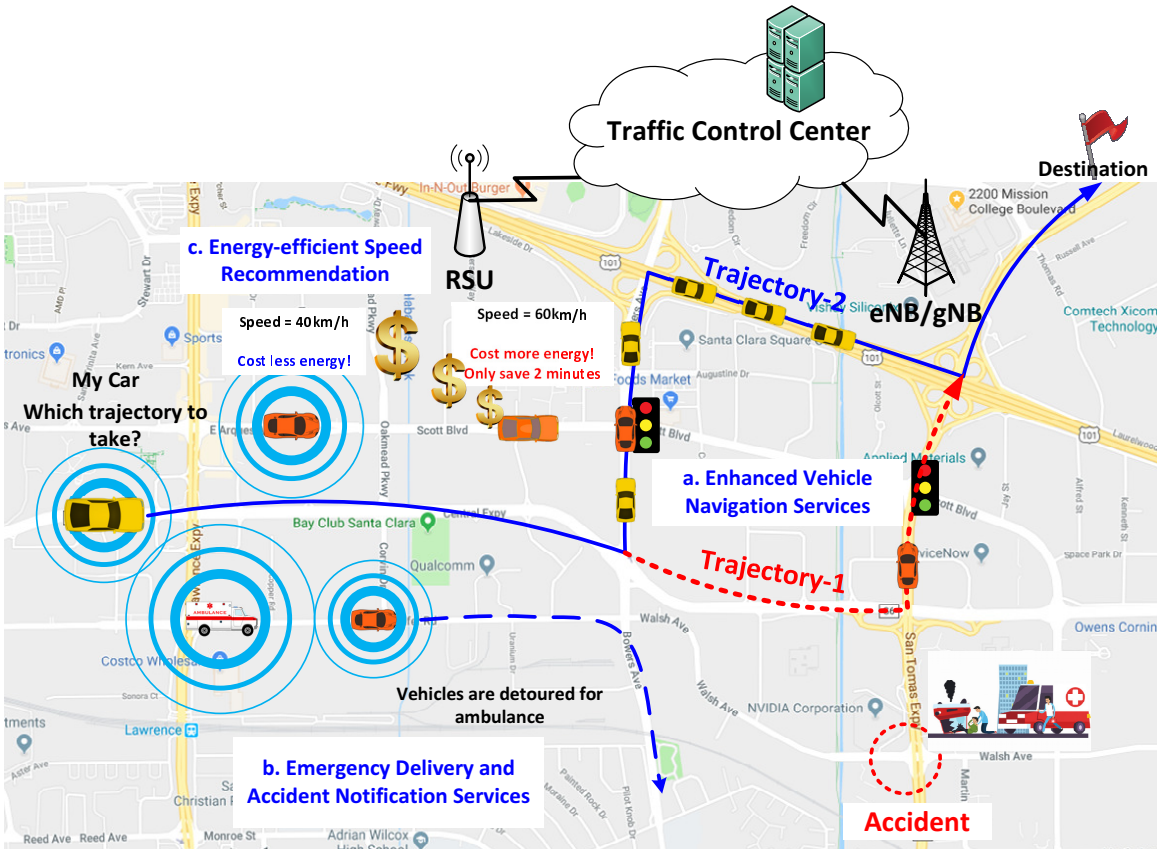


Figure 3: Use cases in V2I networking. (a) Enhanced vehicle navigation service. (b) Emergency delivery and accident notification service. (c) Energy-efficient speed recommendation.

3.1. V2I Networking Use Cases

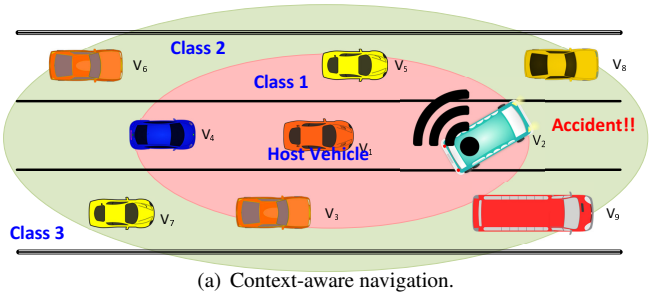
The use cases of V2I involve safety and non-safety services that use V2I and I2V communications, which can be based on an RSU via DSRC (e.g., WAVE) or a base station via Cellular Network Communication (e.g., 4G-LTE/5G). For example, as shown in Fig. 3, there are services for: (a) enhanced navigation, (b) emergency delivery and accident notification, and (c) energy-efficient speed recommendation.

As an enhanced vehicle navigation service shown in Fig. 3, SAINT (Self-Adaptive Interactive Navigation Tool) has been developed using a vehicular cloud [51]. For a road-traffic balanced navigation service, the vehicular cloud with a TCC maintains road traffic statistics, real-time road conditions, the trajectory of each vehicle (i.e., navigation path), and each vehicle's mobility information (e.g., its position, speed, and direction). In addition, it determines each vehicle's navigation path by estimating the near-future congested road segments according to the previously scheduled navigation paths in the vehicular networks. For the congestion estimation, SAINT defines a virtual metric called congestion contribution that indicates how much a vehicle will contribute to road traffic in its future travel.

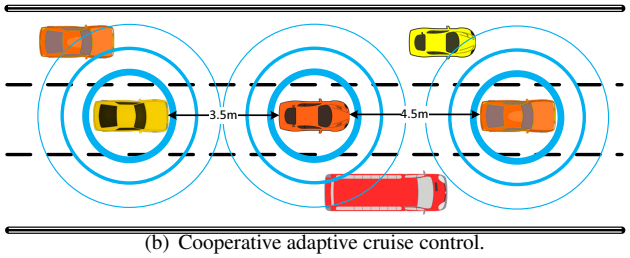
In an emergency navigation service, as shown in Fig. 3, SAINT+ (Self-Adaptive Interactive Navigation Tool plus) has been developed using the interaction between an accident vehicle and an emergency center via a vehicular cloud [52]. SAINT+ inherits the basic navigation features from SAINT [51], and additionally provides vehicles with a navigation service in a road network in which a road accident has happened (e.g., instances of car collision and broken cars). Thus, using SAINT and SAINT+, the vehicular cloud can regulate real-time navigation paths in consideration of the current road network conditions and vehicle trajectories. Also, it can help platooning trucks select their navigation paths with fuel efficiency in the roadway [53].

For the energy-efficient speed recommendation service, as shown in Fig. 3, SignalGuru has been developed using a vehicular cloud [54]. A smartphone mounted on the windshield of a vehicle sends the pictures of traffic signal lights being taken to the vehicular cloud that may figure out traffic signal patterns. The vehicular cloud gives a recommended speed for energy efficiency to each vehicle that approaches the traffic signal area (i.e., intersection). In the current SignalGuru system, the communication between a vehicle and an RSU is performed via a cellular link, but it can also be performed via an IP-based DSRC link.

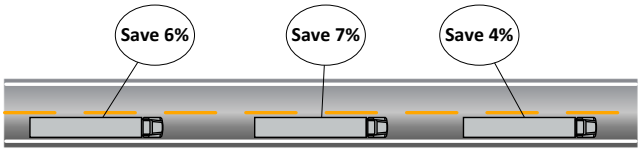
In order to ensure prompt communication between emergency vehicles, accident vehicles, and a vehicular cloud with a TCC, the US government has an emergency road network called the First Responder Network Authority (FirstNet) [55]. This network works on top of public safety broadband networks and provides vehicles with security and safety services, such as emergency help calls and road report calls. This FirstNet



(a) Context-aware navigation.



(b) Cooperative adaptive cruise control.



(c) Truck platooning on a highway.

Figure 4: Use cases in V2V networking. (a) Context-aware navigation. (b) Cooperative adaptive cruise control. (c) Truck platooning on a highway.

is currently constructed by cellular networks including the Radio Access Network (RAN) connected with the core system of FirstNet, but the IP-based DSRC networks using WAVE can also be used in the future.

For a future road environment where all vehicles are fully autonomous and connected, these autonomous vehicles can be fully scheduled to cross signal-free intersections with help of an MEC server [56, 57]. An MEC server, by receiving mobility information of vehicles, can calculate an optimal vehicle crossing schedule for each vehicle. As vehicles continue moving, the calculated schedule can also be updated by the latest mobility information of vehicles in the MEC server. Such kind of signal-free intersection crossing mechanisms can significantly increase throughput of an intersection and improve power efficiency of autonomous vehicles.

3.2. V2V Networking Use Cases

The V2V use cases are safety services that use V2V communications. e examples, as shown in Fig. 4, include context-aware navigation, cooperative adaptive cruise control, and truck platoon on the highway. These three safety services can be implemented for self-driving vehicles. Communication among vehicles can be performed via DSRC (e.g., WAVE).

Context-Awareness Safety Driving (CASD) is a driving safety service for human-driving, self-driving, and hybrid-self-driving (i.e., driving conducted by both a human and a machine) [58]. CASD lets vehicles share driving information with other vehicles and also controls vehicle maneuvers in dangerous situations. As shown in Fig. 4(a), each vehicle classifies any geographically adjacent vehicles (i.e., neighboring vehicles) into three classes: (i) Class-1 Vehicles with Line-of-Sight (LoS) and Unsafe Range, (ii) Class-2 Vehicles with Non-LoS but Unsafe Range, and (iii) Class-3 Vehicles with Safe Range. Vehicles employing a CASD system cooperate with each other in order to plan safe driving-motions in real time via DSRC-based V2V communications in order to avoid collisions on either a highway or an urban road network.

A legacy cruise control can be extended into a Cooperative Adaptive Cruise Control [59] by considering a wider view based on V2V communication. This extended cruise control coordinates adjacent vehicles on a given road segment or highway so that each vehicle can keep a safe inter-distance between all adjacent vehicles via V2V. If a vehicle abruptly reduces its speed or stops in a roadway, it notifies all adjacent vehicles moving behind or in front of it for the emergency situation by V2V-based direct communication in a timely manner. This notification propagates through vehicles in a connected Vehicular Ad Hoc Networks (VANET) in a progressive fashion, and allows them to adjust their speed and direction accordingly.

A truck platoon is a series of trucks moving together in a linear group with a short inter-space (e.g., 3 m to 10 m) on a highway, as shown in Fig. 4(c) [60, 61]. Platooning in this way is useful for road traffic throughput and saving vehicle energy. Through the platooning based on V2V, vehicles move closely and quickly by adjusting their speed so as to maintain inter-spaces that are sufficiently large enough to avoid collisions, so that the road traffic throughput can be improved. In addition, in such platooning, the leading vehicle requires a driver just in case, because the leading vehicle as a leader can control the other vehicles in the platoon. Such truck platooning can save substantial labor expenses for drivers as well as reduce fuel consumption, since the leading truck can block air resistance for the following vehicles in the same platoon of trucks.

A cooperative automated driving (CAD) [62] system can enable autonomous vehicles to coordinate their trajectory maneuvers by a collective perception mechanism that allows the vehicles to share their sensing information with each other by 5G V2X communications. The CAD system can be applied to different traffic scenarios. For example, in a highway on-ramp scenario, merging vehicles can negotiate a proper merging trajectory with mainstream vehicles. However, the CAD system only used Cooperative Awareness Message (CAM) [63] instead of IP based communications. For interconnecting vehicles from different automotive vendors, IP-based vehicular communications can be a good carrier, considering a huge number of existing IP-based protocols.

3.3. V2X Networking Use Cases

The V2X use cases are safety services that use V2V, V2I, and vehicle-to-pedestrian (V2P) communications. For example, as shown in Fig. 5, there is a Safety-Aware Navigation Application (SANA) for pedestrian protections [70]. In the SANA service, a vehicle and a pedestrian's smartphone (or smart watch)

Table 3: Comparison of IP Vehicular Network Architectures

Ref.	Type	Objective	Scenario	Method	Analysis	Sim.	Imp.	Year
[64]	V2I, V2V	IPv6-based architecture design	IPv6-based data communication based on service types	On-demand ND-based DAD; On-demand PMIPv6; Vehicle relay communications.	✓	✓	×	2013
[65]	V2I	Reviewing issues related to IPv6 operation for WAVE	IP addressing model in Ad Hoc	Comparing link model, address model, scopes, and uniqueness; Suggesting challenges in upper layers of network layer.	Partially	×	×	2010
[66]	V2I, V2V	Enabling multicast services in ITS	A distributed geographic multicast	Geographic multicast address autoconfiguration with a group membership management; A dynamic network protocol selection method for both non-IP and IP multicasting.	Partially	×	×	2012
[67]	V2I, V2V	Designing an architecture for both IP networking and access radio	General V2V and V2I communications	A radio frequency assignment strategy that can reuse channels based on the signal interference level.	Partially	×	×	2011
[68]	V2I	Mobility support	V2I communications	PMIP and integrating passengers' mobile devices.	Partially	×	×	2001
[69]	V2I	Secure vehicular IPv6 communication with IKEv2 and IPsec	Security threats in IPv6-based VANET	Implementation and experimental evaluation of IPsec and IKEv2 for IPv6 NEMO in vehicular environments.	Partially	×	✓	2016

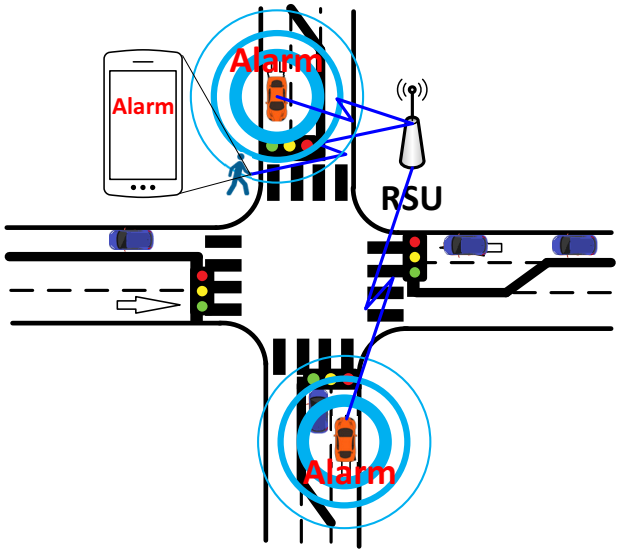


Figure 5: Use case in V2X networking: pedestrian protection.

can communicate with each other via DSRC (e.g., WAVE). Since smartphones do not yet support DSRC devices, Vehicles to infrastructure to pedestrian (V2I2P) communications can be used to achieve communication between a vehicle and a pedestrian via an RSU as a tentative method. Through edge computing in an RSU (or an edge server) [71], vehicles and a pedestrian's smartphone can schedule communication times in consideration of their trajectories in an energy-efficient manner.

The enhanced 5G-V2X architecture [5] suggests that a 5G sidelink-enabled smartphone can directly communicate with a 5G-V2X-enabled vehicle. A pedestrian with such kind of a smartphone can receive warning messages when a possible collision is detected. Since the 3GPP cellular networks are already all-IP networks, certainly the IP-based vehicular networks on DSRC and 3GPP V2X technologies can accelerate ubiquitous connections for humans and vehicles.

4. Vehicular Network Architecture

The network architecture determines the overall working flows of a system. This section reviews several IP-based vehicular network architectures. With knowledge of these architectures, one may better understand the future IP-enabled vehicular networks. Table 3 shows a taxonomy of the vehicular network architectures surveyed in this section.

4.1. Service Type-based IP Architecture

The authors in [64] presented a vehicular IP architecture based on WAVE named VIP-WAVE for applications of I2V and V2I networking. IEEE WAVE 1609.3 specifies a set of protocols that include IPv6 as the main network layer protocol in the data plane [9]. However, the standard WAVE does not support certain IPv6 features, such as seamless communications for Internet services, duplicate address detection (called DAD), and multihop communications between a vehicle and an RSU. Thus, for improving the IP networking support in the standard WAVE, VIP-WAVE suggests three schemes as follows:

- A new IPv6 address assignment mechanism and DAD;
- An on-demand IP mobility management based on PMIPv6;
- A relay mechanism for two-hop I2V and V2I communications.

An RSU can use WAVE service advertisement (WSA) management frames to provide IP configuration information to vehicles without ND. Fig. 6 shows that a vehicle receives a WSA message in CCH from an RSU to start IP-based services. In order to ensure pseudonymity, devices in WAVE may support readdressing, and thus the vehicle MAC address may change over time. However, it should be noted that an updated MAC address may lead to a collision with another IPv6 address based on a MAC address. To avoid such an issue, VIP-WAVE was proposed with a lightweight and on-demand ND process for DAD.

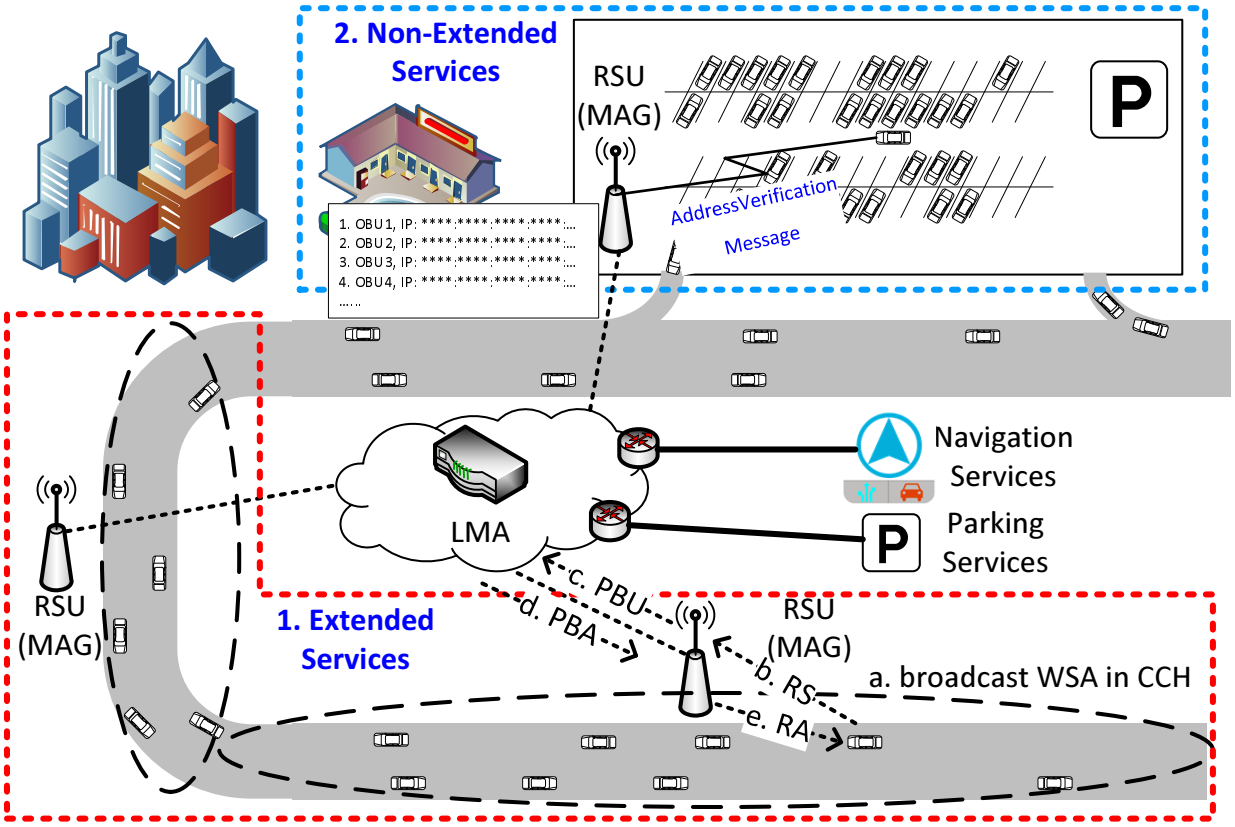


Figure 6: Vehicular IP architecture based on IEEE WAVE standard.

For mobility management, VIP-WAVE defines two types of services in vehicular networks, as shown in Fig. 6: (i) extended services and (ii) non-extended services. In extended services, VIP-WAVE uses the PMIPv6 mechanism [41]. An RSU and a vehicle become a mobile anchor gateway (MAG) and a mobile node (MN), respectively, in the PMIPv6 domain. Based on the PMIPv6 operations, an RSU as a proxy signals the movement of a vehicle to a local mobility anchor (LMA). As shown in Fig. 6, an MAG (i.e., RSU) sends a Proxy Binding Update (PBU) message to an LMA to register or update the mobility information of the MN. The LMA replies to the MAG with a Proxy Binding Acknowledgement (PBA) message that includes a registration or update confirmation and network parameters such as IPv6 address prefix information. The MAG shares the received network parameters with the vehicles by RA messages. When moving through several RSUs, the vehicle can receive IPv6 prefixes from the LMA. The LMA tunnels packets toward the vehicle via the RSUs through which the vehicle travels.

In VIP-WAVE, a vehicle can also communicate with an RSU via a relay vehicle by two-hop communications. Thus, when exiting the communication range of an RSU, a vehicle can send a relay service announcement to nearby vehicles. Upon receiving such an announcement, a nearby vehicle may register itself into an RSU as a forwarder, and the forwarder can then immediately notify the requesting vehicle of a relay maintenance announcement.

In non-extended services such as parking, a vehicle may obtain a temporary IPv6 address from a serving RSU. As shown in Fig. 6, a vehicle can send an address verification message to an RSU that is dedicated to a service, and the RSU caches the IP addresses of registered vehicles. Once a vehicle exits the service area, after a fixed amount of time, the vehicle's IP address will be removed from the cache of the RSU.

Therefore, VIP-WAVE can be a suitable candidate architecture in IP-based vehicle networking based on the fact that it supports on-demand ND, PMIPv6-based mobility management, and a relay-based V2I communication mechanism for different types of services.

4.2. IEEE 1609-based Standard IPv6 Architecture

Baccelli et al. analyzed the IPv6 operations in the IEEE WAVE 1609 [65] standard. For supporting infotainment traffic, WAVE standard defines basic IPv6 operations along with TCP and UDP stacks. Although WAVE is designed to broadcast safety information, IP-based applications cannot be neglected.

The authors in [65] showed that, for the IEEE 1609.3 standard, it is not recommended to have many IPv6 operations over WAVE, which may require IPv6 network parameter acquisition (e.g., a subnet prefix, DNS suffixes, and DNS server addresses) and IPv6 stateless address autoconfiguration (SLAAC). Moreover, the link-layer assumptions in IPv6 may not be fulfilled in WAVE. For example, the assumptions in IPv6 require symmetric connectivity between two interfaces. However, the nature of wireless communications in WAVE may lead to asymmetric connections between two vehicles due to signal fading and interference. Generally, for an IPv6 subnet, interfaces on

the same subnet may use the same prefix to generate IPv6 addresses, which is considered as one-hop communications among the interfaces. Thus, a link is correlated to a prefix in IPv6 despite the working domain differences between link-local and global addresses. The vehicle mobility and frequent topology changes may nullify the correlation in a WAVE-based vehicular network.

They also showed that using the standard IPv6 stack may be insufficient, as claimed by the IEEE 1609.3. Since the link model of ad-hoc networks defined in [72] is similar to that of vehicular networks, it may be better to follow the principle of [72] regarding the configuration of IP subnet prefixes and IP addresses. In addition, the protocols relying on multicasting (e.g., ND and DHCPv6) defined in the standard IPv6 may not work properly in vehicular networks because of instantaneous link connectivity.

4.3. Internet-based IP Multicast Services Architecture

The authors in [66] proposed an architecture that supports infrastructure-based multicast services for Internet access in vehicular networks. The proposed architecture operates in two different phases: (i) the initialization or bootstrapping phase and (ii) the multicast traffic dissemination phase. The initialization phase involves a multicast address self-configuration process that relies on the geographic position information of a vehicle. This phase also includes a membership construction scheme for routing packets. The second phase has two mechanisms: (i) a network protocol selection mechanism when a packet is transmitted and (ii) a receiver-based multicast mechanism for disseminating multicast packets.

In the initialization phase, a vehicle can use the mechanism called Geographic Multicast Address Autoconfiguration (GMAA) to configure a general multicast address based on its own geographic position information without requiring any additional signal messages. As it moves through multiple areas, a vehicle may update its current multicast address with new geographic position information. For multicast purposes, vehicles are divided into groups, with each group having a group leader that acts as a local multicast manager; the group leader is in charge of disseminating multicast packets to its members.

In the multicast traffic dissemination phase, the architecture provides an approach for selecting a proper network protocol with which to transmit packets. This approach decides a proper network protocol for a packet according to a network profile that considers flow requirements, the availability of interfaces, and so on. Depending on the network profile, a data packet can be encapsulated into a geonetworking packet or an IP packet. Then, in order to better multicast packets, a receiver-based multicast mechanism is also proposed. A group leader periodically reports its profile to the server. The server can execute a reverse geocoding function to determine the target area and the target multicast group leader. The multicast packet is first unicasted to the group leader for the target group, and then the group leader multicasts the packet to its members.

Eventually, the paper detailed the integration of the above proposed process. The integrated framework involved the design of several components, such as a mapper, geodestination table, network selector, mapping table, and network profile manager. Along with these components, the authors also shaped the working flows on both the transmitting and receiving sides.

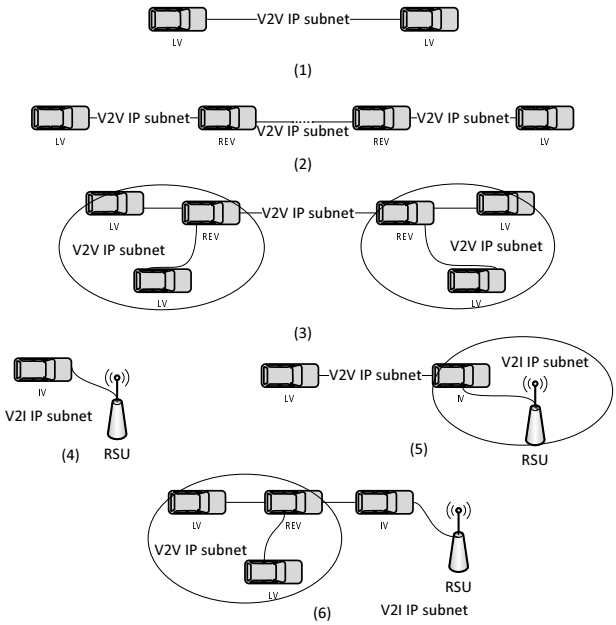


Figure 7: Six types of IP topologies.

4.4. Joint IP Networking and Radio Architecture

The authors in [67] presented a joint IP networking and radio architecture for vehicular networks. The proposed architecture defines one-hop connections as an IP subnet. For an IP subnet, the architecture categorizes vehicles into three types: Leaf Vehicles (LV), Range Extending Vehicles (REV), and Internet Vehicles (IV). According to the definitions used in the paper, the LV group accounts for the major group of vehicles, as end users. A vehicle in the second type (REV) mainly functions as a relay to connect the LV to the Internet via IV. The IV type, as the name suggests, represents a group of vehicles being directly connected to the Internet. In addition to the three types of vehicles, the authors define six types of topologies for vehicular networking. Fig. 7 shows these six types: LV2LV, LV2REV2LV, LV2REV2REV2LV, LV2RSU, LV2IV2RSU, and LV2REV2IV2RSU.

The authors provided an example to illustrate the role of each of the types defined above by modeling connected vehicles to a train. In this train, an LV is an in-wagon node while an REV is an inter-wagon relay, and an IV is a gateway node with Internet access. Based on this train model, the authors also analyzed the routing process among wagons in a train.

For the allocation of radio frequency, the paper suggested a channel reuse scheme to maximally utilize the available channels. The paper did not evaluate the proposed architecture, but the primary analysis indicates that the proposed architecture may have high overhead.

4.5. Mobile IP Access Architecture

The authors in [68] proposed a mobile communication architecture called MOCCA for integrating ad-hoc inter-vehicle

communication (IVC) systems with Internet access. MOCCA, based on the FleetNet system, supports a mobility management scheme, a service discovery process, and legacy architectures for mobile devices inside a vehicle. The FleetNet system was developed to demonstrate an ad-hoc IVC system for distributing data and providing information and services that depend on the locations of vehicles, which have no direct Internet access. MOCCA extends the FleetNet system to include the ability to access the Internet. The extended architecture consists of vehicles, Internet gateways (IGW), a proxy [41], and corresponding nodes (CN). An IGW is an infrastructure node (i.e., RSU) that provides the passing vehicles with Internet access. A proxy is a node that supports different addressing schemes, mobility management, and the interoperability between the FleetNet and the Internet.

Mobility support in MOCCA uses a modified MIPv6 approach called MIPv6*. MIPv6* allows a vehicle to use its global IPv6 address for mobility management rather than an autoconfigured IPv6 address. In addition, the mobility signaling messages for a vehicle are delegated to the IGW, which is quite similar to the PMIPv6 mechanism for network-based mobility management. Thus, the proxy can build a tunnel for routing packets between a vehicle and its CNs.

For service discovery, MOCCA suggests a service discovery protocol using the service location protocol (SLP) based on IPv6 [73, 74, 75]. The suggested SLP has two basic functions: (i) An IGW periodically announces its service list to a geographic area limited by the FleetNet geocasting and (ii) a vehicle receiving the service list caches the available services. Through these two functions, a vehicle can discover a series of serving IGWs for mobility management. In many cases, a vehicle may simultaneously discover several available IGWs. In this situation, a vehicle can select a serving IGW by a number of additional parameters, such as an IGW's capacity, remaining bandwidth, and location. For this selection process, the authors proposed a fuzzy-based method. This fuzzy method categorizes applications into four types: best effort, interactive, AV streaming, and real-time applications. Through this fuzzy selection method, a vehicle can determine the most suitable serving IGW.

When considering that mobile devices (e.g., laptops and tablets) inside a vehicle require Internet access, MOCCA includes a vehicle proxy to function as a proxy for those devices. The mobile devices build TCP connections with the vehicle proxy, and the vehicle proxy caches and forwards the data packets to a serving IGW via FleetNet. In this way, a legacy application in a mobile device is not required to modify its protocol stack to support MOCCA for the Internet access.

4.6. Vehicular IPsec Architecture

In order to secure IPv6 communication for the vehicular networks, Fernandez et al. proposed an approach using Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [69]. Their approach focuses on using MR with multiple wireless interfaces to secure IPv6 NEMO for internal vehicle devices, and the wireless interfaces consist of IEEE 802.16, WiFi, cellular networks, and IEEE 802.11p. Their approach also has three different types of stations, as described below.

- **Vehicle ITS Station (Vehicle ITS-S):** Vehicles communicating with MR.
- **Roadside ITS Station (Roadside ITS-S):** This station provides Internet access to the vehicles.
- **Central ITS Station (Central ITS-S):** This is a TCC as a Home Agent (HA) and manages the locations of the vehicles.

In order to enable secure communication between the MR and HA for control and data traffic, IPsec can be established between the MR and HA. In most cases, a Roadside ITS-S provides Internet access to Vehicle ITS-S using one of the available wireless interfaces. If the Roadside ITS-S is not available for vehicles, a cellular network can be used as a backup for the Internet connectivity instead. The NEMO protocol can be enhanced by a secure communication scheme that interworks with IKEv2 and IPsec.

The authors have experimented on their scheme in a real testbed. The testbed was built using a combination of cellular and IEEE 802.11p networks, and also in-vehicle devices used IEEE 802.11g to connect to an MR within a vehicle. After a few experiments, the results showed that secure IPv6 had minimal overhead and impact on the connection and communication performance.

4.7. Key Observations

Based on the results of the above surveyed papers about vehicular network architectures, several conclusions can be drawn.

- Firstly, we should be aware of the unidirectional links in vehicular communications when designing the IP link model. The unidirectional links may cause ND failure, so reduce the reliability of the IP packets routing and forwarding. Notice that the unidirectional link for ND can happen sporadically for a while and can also be mitigated by subsequently retransmitted ND messages.
- Secondly, from the application perspective, a vehicular network architecture should adapt to different types of services. For instance, VIP-WAVE [64] proposes two types of services for vehicular networking, extended and non-extended services. The extended services may employ full-fledged IP mobility management solutions, such as MIPv6 and PMIPv6, while non-extended services may use a simplified version of IPv6 networking for instance without mobility support.
- Thirdly, in order to protect the privacy of a vehicle, the MAC address as a pseudonym can be changed periodically, leading to a change in the IPv6 address, so a lightweight DAD procedure may be necessary.
- Fourthly, usually vehicles do not have a home network, but location management for vehicles may be required to keep track of them and route packets to them. In order to ensure efficient mobility management, a network-based mobility support may be concealed from both a vehicle itself and the correspondent nodes (CN).

- Fifthly, a VDTN can be supported by a vehicular network layering architecture with a DTN Bundle layer [76]. Separating the control plane and data plane may be a suitable design principle, since it provides flexibility to various underlying radio access technologies (RATs).
- Lastly, security in vehicular networks is very important for providing a secure and reliable communication to vehicles, and the AAA service must be considered in an efficient and effective manner. Since vehicles may have multiple interfaces, both horizontal and vertical handoffs should be considered.

5. IP Address Autoconfiguration

In this section, we investigate the different approaches for vehicles IP address autoconfiguration. Table 4 shows a taxonomy of the IP address autoconfiguration schemes.

5.1. DHCP-based Address Allocation

A Vehicular Address Configuration (VAC) scheme was proposed in [77] for a VANET. The proposed VAC is a distributed scheme of DHCP [81, 82], which stands for Dynamic Host Configuration Protocol. VAC consists of cluster headers and cluster members in the VANET. A cluster header, as a leader, acts as a DHCP server to assign IP addresses to cluster members (as DHCP clients) within the same connected VANET. Note that a connected VANET consists of vehicles that can communicate with each other via DSRC and that can perform multihop communications through a VANET routing protocol. The cluster header maintains the mapping of a cluster member and an IP address in its DHCP database. For example, if a cluster member leaves the current cluster, the cluster header quickly reflects this in its DHCP database, and, as a result, VAC tries to reduce the overhead of IP address maintenance in a high mobility environment.

"Scope" is defined as the number of hops in a confined geographic area, where each cluster member has a unique IP address. If a cluster member has an IP address from a cluster header in a connected VANET within the same scope, it is assured that the cluster member's assigned IP address is unique in the scope. If the cluster member leaves out of the current connected VANET, it requires another IP address assignment from the cluster header in the next connected VANET. The newly assigned IP address should be unique in the new VANET, as shown in Fig. 8. When a vehicle moves on a highway, it can move frequently from a cluster to another cluster over time, meaning that its IP address can change frequently, leading to heavy overhead for address configuration. Therefore, while the VAC can provide vehicles with a possible IP address autoconfiguration for V2V communications, the management overhead is not negligible for the unique IP address assignment in VANET environments (e.g., highway scenarios) where vehicles frequently move to different clusters.

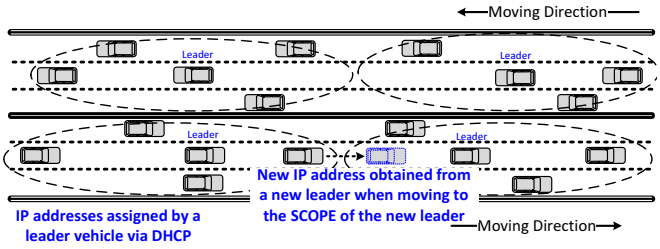


Figure 8: Vehicular address configuration via DHCP.

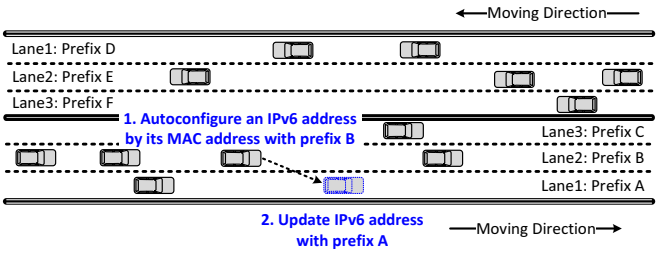


Figure 9: Address Assignment using Lane/Position Information.

5.2. Lane and Position-based Address Allocation

An IPv6 address configuration method was proposed to use a vehicle's road lane position in a roadway [78]. This method assigns an IPv6 prefix to each lane in a roadway so that vehicles moving in different lanes can be assigned to different subnets by combining their MAC address with their current lane prefix. Whenever a vehicle moves to an adjacent lane, it needs to update its IP address, as shown in Fig. 9. Thus, in urban road networks where short road segments are connected at intersections and road segments have multiple lanes, the vehicles will need to frequently update their IP address over time. This means that the IP address autoconfiguration will happen frequently. Even in the IP mobility support for seamless TCP connections, the frequent IP address updates will lead to high overhead messaging for IP address update notification. As a result, this address configuration method will be inefficient.

5.3. Geography-based Address Allocation

An IPv6 Geographic Scalable Address Auto-Configuration (GeoSAC) scheme was proposed for vehicles in large-scale vehicular networks [79]. This GeoSAC extends the legacy IPv6 ND Protocol for road networks such that the address autoconfiguration messages and data messages can be routed to destination nodes using a geographic routing protocol. It defines a geographic area in a road network as a multicast link (i.e., an IP subnet), where vehicles can communicate with each other over multicasting in a wireless radio link, as shown in Fig. 10. Hence, vehicles belonging to this geographic area can construct a connected VANET in which multicast data forwarding is feasible.

The GeoSAC uses a geographic routing protocol to perform IPv6 DAD procedure, which runs in a Car-to-Car (C2C) NET layer, that is, a sub-IP layer. Through the use of this geographic routing protocol, IPv6 RA messages from a router (i.e., RSU) can be disseminated to the vehicles in its geographic area (i.e.,

Table 4: Comparison of IP Address Autoconfiguration Schemes

Ref.	Type	Objective	Scenario	Method	Analysis	Sim.	Imp.	Year
[77]	V2V	Address autoconfiguration by DHCP	Clustered vehicles environments	A leader-vehicle in a vehicle cluster configures IP addresses for other vehicles in this cluster based on DHCP.	Partially	✓	×	2016
[78]	V2I	Address autoconfiguration	Address assignment by road layout	A subnet prefix allocation method by lanes where a vehicle determines its IP address by its current lane and position.	Partially	✓	×	2008
[79]	V2I	Address autoconfiguration by geographic networking	Geographic networking	A subnet prefix allocation method by geographic areas.	✓	✓	✓	2008
[80]	V2I	Privacy protection in address autoconfiguration	Vehicles with pseudonym MAC address	A vehicle determines its IP address by a dynamic and pseudonym-based MAC address.	Partially	×	×	2010

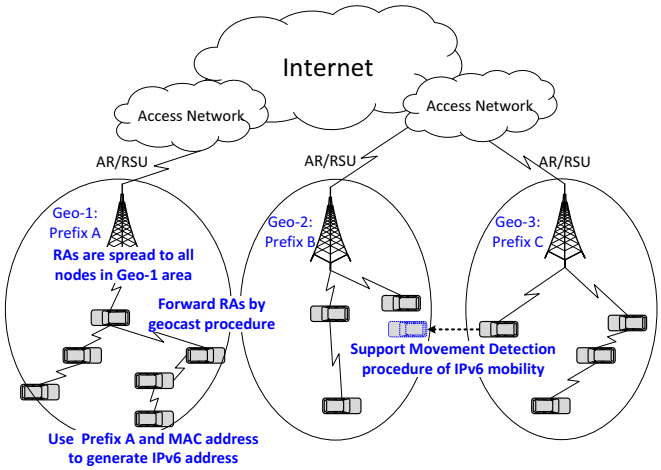


Figure 10: GeoSAC-scalable address autoconfiguration for VANET by geographic networking concepts.

IPv6 subnet). In addition, the DAD messages from a vehicle can be reachable by other vehicles for address uniqueness testing. Therefore, the GeoSAC can effectively support the IP address autoconfiguration in road networks with RSUs as IP routers.

5.4. Cross-layer Identity Management

Vehicular networks may consist of multiple radio technologies such as DSRC, WiFi, and cellular networks, so an efficient cross-layer network architecture that combines those technologies needs to be facilitated. In these vehicular networks, vehicles are equipped with multiple network interfaces for those technologies. As a result, their interfaces have the corresponding identities as communication entities, so the efficient management of those multiple identities are required [80]. Note that, while the framework in [80] is focused on ETSI GeoNetworking for IPv6 networking, it can also accommodate IPv6 over 802.11-OCB for DSRC-based vehicular networks.

For the identity management in cross-layer networks [80], the key requirements are as follows. The first is security and privacy for vehicular networks. For example, in order to prevent vehicles from being tracked by hackers, the network interfaces of vehicles should use MAC address pseudonyms, where the MAC addresses are periodically changed over time for privacy protection. Since the IPv6 address of a network interface is usually based on its MAC address, a change in the MAC address may trigger updates in the corresponding IPv6 address. Such changes in the MAC and IP addresses can cause difficulty for hackers in tracking a vehicle. However, these updates should be done carefully so as not to hinder the communication between adjacent vehicles for safe driving on a highway. When a vehicle changes its MAC and IPv6 addresses, the neighboring vehicles must take time to recognize those changes in the addresses, so they cannot promptly exchange safety messages at that time.

In addition, a framework for cross-layer networks is defined so as to satisfy the requirements of multiple identity management in the aspect of the network layer. When a vehicle communicates with an IPv6 node with multiple interfaces, IPv6 packets from/to the multiple interfaces should be delivered in a harmonized way in order to achieve high performance. In particular, IPv6 packets should be efficiently routed to a TCP session using these multiple interfaces (i.e., multi-TCP) through multiple radio networks and the associated wired networks. Otherwise, the multi-TCP session can suffer from a low performance if a path related to a radio technology cannot promptly deliver TCP segments. Therefore, the multiple identity management should be well-designed and operate according to real-time network situations.

5.5. Key Observations

The IP address autoconfiguration for vehicles can use either a server-based stateful allocation or a location-based stateless configuration. For a server-based stateful allocation, a cluster header with an address pool can be selected as a distributed DHCP server, and it can then allocate IP addresses to its cluster members within their connected VANET. For a location-based stateless configuration, the lanes of a road segment can have unique IPv6 prefixes, or the geographic areas of RSUs can have prefixes. In the case of multiple radio interfaces in a vehicle, a cross-layer identity management is required such that a multi-TCP session is supported efficiently over the multiple radio networks. We also have several other observations as follows:

- Firstly, a stateful address allocation approach [77] managed by a server supports V2V communication among vehicles in a highway. When vehicles move fast on a

Table 5: Comparison of IP Mobility Management Schemes

Ref.	Type	Objective	Scenario	Method	Analysis	Sim.	Imp.	Year
[83]	V2V, V2I	Passing IP addresses to other vehicles	Network handoff environments	An approach where a vehicle obtains a new IP address by the help of other vehicles.	✓	✓	×	2012
[84]	V2I	Network-based mobility support	MT inside a mobile network	A method that binds an MT's mobility information in LMA and caches a new type of flag.	Partially	✓	×	2009
[85]	V2I	Hybrid distributed mobility management	Distributed and centralized mobility support	An MN keeps two prefixes obtained from a central mobility anchor (CMA) and a serving MAR, and updates the latter prefix when moving to a new serving MAR; Both MAR and CMA help to build an IP tunnel for an MN.	✓	Numerical	×	2015
[86]	V2I	Hybrid network mobility	Mobility support for different traffic types	A vehicle can have two sets of prefixes from an MAR and a CMA, respectively; An MN decides the prefixes for different types of traffic flows according to the lifetime of traffic flows.	✓	Numerical	×	2015
[87]	V2V, V2I	Network mobility support for VANET	IP address updates	A vehicle updates its IP address by the help of other vehicles.	×	✓	×	2014
[88]	V2I	Analyzing PMIPv6 and NEMO for VANET	PMIPv6 and NEMO environments	Fast P-NEMO proactively prepares for the handoff of an MN using MAC layer information.	✓	Numerical	×	2012
[89]	V2V, V2I	Mobility support for VANET	Combining VANET and fixed IP networks	Multiple base stations discover connections to a destination vehicle for supporting mobility management.	✓	✓	×	2010
[90]	V2I	DMM based SDN	5G networks	An SDN-based DMM module in a SDN controller manages the mobility of MNs.	✓	✓	✓	2016
[91]	V2V, V2I	Analyzing IP mobility management for vehicular networks	IP mobility management	The improvements and weaknesses of the existing solutions; Open research challenges and issues of IP mobility management in vehicular environments.	×	×	×	2011
[92]	V2I	Handoff support in multi-domain	ISO/ETSI architecture environments	Handoff support in several standard mobility management schemes, such as NEMO and IEEE 802.21 standard.	✓	×	✓	2017
[93]	V2I	Authentication delay minimization for PMIPv6	Vehicular PMIPv6 security	An updated version of the one-time key-based authentication protocol for PMIPv6.	Partially	×	×	2009

highway and change their clusters, they need to acquire a new IP address from a new cluster header. According to the DHCP discovery protocol, such an IP address lease suffers from a delay, so the vehicles newly entering to the cluster need to wait some amount of time before they can communicate with neighboring vehicles in the cluster for driving safety. Thus, prompt V2V communication can be hindered by the IP address acquisition delay.

- Secondly, a stateless address configuration scheme [78] based on lane information can cause substantial overhead for IPv6 address configuration when a vehicle frequently changes its lane. Whenever a vehicle changes its lane, its subnet changes, and it should generate a new IPv6 address based on the prefix associated with the current lane. This method also does not allow adjacent vehicles in different lanes to communicate with each other for driving safety because they belong to different subnets. Thus, for safety applications, this method is not feasible.

- Thirdly, a geography-based stateless address configuration scheme [79] performs better than the the lane-based stateless address configuration scheme in terms of address configuration overhead and communication with adjacent neighbor vehicles. However, when vehicles move quickly through multiple RSUs' coverage, they need to configure their IP addresses. In urban road networks, RSUs will usually be deployed at intersections. In rush hours, when vehicles are moving through intersections, many ND-related messages are generated for DAD for updated IPv6 addresses. The more vehicles are moving in the road networks, the more ND traffic overhead is generated. A more efficient prefix assignment to reduce the ND traffic is thus required.

- Lastly, a cross-layer identity management [80] is required for a vehicle with multiple radio interfaces because when a vehicle switches from a radio technology to another radio technology, it requires a vertical handoff. Since this is involved in different radio technologies and the corresponding wired networks, the packets destined for different IP addresses of a vehicle should be correctly routed to the vehicle. In order to ensure privacy, since the MAC and IP addresses change over time, the routing tables for the multiple interfaces should be quickly updated in the framework with multiple radio technologies, and the continuity of TCP sessions should also be handled with the address update of TCP end points. In addition, in order to support a multi-TCP session, the load balance and synchronous delivery for IP packets for the TCP session should be performed by a coordination function in the framework so as to support multiple identities. Thus, the IP address management for multiple interfaces faces many challenges.

6. IP Mobility Management in Vehicular Networks

Mobility management plays an essential role in vehicular networks. The highly dynamic mobility nature of vehicles requires an efficient solution for dealing with the attachment and detachment to links while vehicles are moving.

This section introduces and surveys several IP mobility management schemes in vehicular networks for the support of handoff. It mainly explains new approaches for vehicular mobility management, such as IP passing protocols, DMM-based approaches, SDN-based approaches, and some hybrid approaches. Table 5 shows a taxonomy of the mobility management schemes surveyed in this section.

6.1. Group- and Individual-Assisted IP Address Passing

When a vehicle travels at a high speed and frequently joins and leaves the coverage of a number of ARs (i.e., RSUs), the ongoing communication sessions of the vehicle may be broken down due to the problem of the inefficient handoff procedure. An IP address passing protocol [94] can help the vehicle maintain the current IP address and obtain a new IP address from various sources (e.g., DHCP server) when the vehicle travels to a new AR. In this way, it is possible to maintain the ongoing sessions for longer periods. For instance, an exiting vehicle can pass its old IP address to a newly entering vehicle in order to reduce the handoff latency. However, when network fragmentation is present (e.g., in a sparse network), the IP passing process may experience some delay or even stop working due to a high packet loss rate.

In order to solve this problem, Chen et al. [83] proposed an IP passing scheme that can delay the release of IP addresses and let a vehicle quickly obtain a new IP address in sparse vehicular networks via a DHCP server. The main idea of the paper is to use cooperation among vehicles. As shown in Fig. 11, an exiting mobile node (i.e., LMN) checks whether or not it can form a virtual bus, which is a group of vehicles, to pass its previous IP address to another vehicle upon receiving a new IP address from the new AR. If a virtual bus is built, the LMN passes its IP address to another mobile node (i.e., KMN), which will keep the IP address, for future entering mobile nodes (i.e., EMN) on the same or opposite directions. When moving into the coverage of an AR, an EMN first broadcasts an IP address request packet to both a KMN and a DHCP server, and then proceeds to obtain an IP address from the earliest assignment, either from a KMN or a DHCP server. This method has been reported to reduce the packet loss rate caused by network fragmentation.

The authors theoretically analyzed the performance of the proposed scheme using a Markov chain model and conducted extensive simulations in a network simulator [95, 96]. The parameters employed in the evaluation include the vehicle speed, vehicular density, network fragmentation ratio, and the length of IP passing (i.e., the number of hops). The simulation results show that, in terms of IP address acquisition time, IP address lifetime, handoff latency, packet loss rate, and throughput, the proposed scheme can outperform other baselines, such as MIPv6 [39] and IP passing [94]. However, for messaging overhead, the proposed scheme consumes more bandwidth due

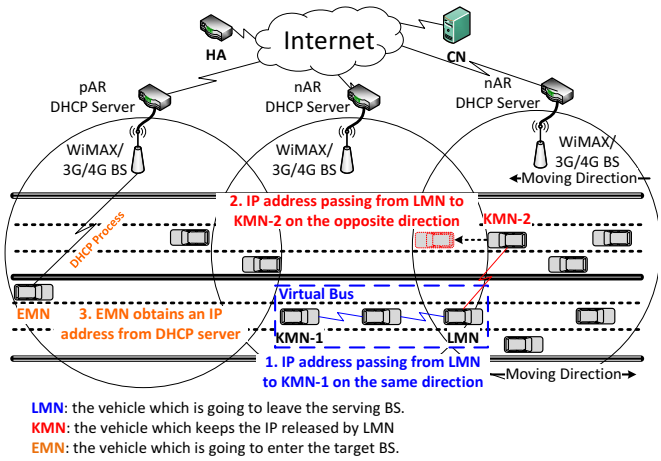


Figure 11: Group- and individual-assisted IP address passing with network fragmentation.

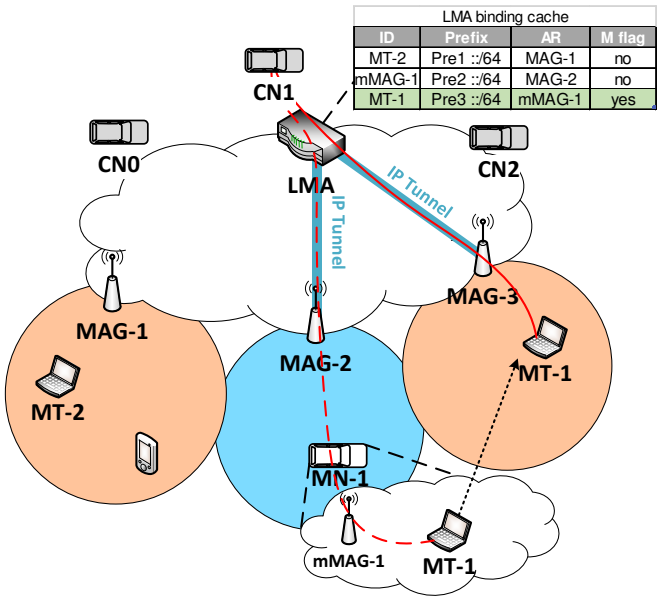


Figure 12: NEMO-enabled localized mobility support.

to the fact that it needs to send more packets as part of the IP passing process.

6.2. NEMO-Enabled Localized Mobility Support

Combining both PMIPv6 and NEMO solutions can improve the transparency of both the network mobility and localized mobility. However, when there is little integration between the two protocols, a mobile terminal (MT), which is changing the attachment between its current MR and a fixed MAG on the infrastructure, requires the MT to change its IP address due to the differences in the prefixes obtained from the PMIPv6 domain versus those obtained from the NEMO-BS domain. In order to solve this problem, Soto et al. proposed a NEMO-enabled PMIPv6 architecture, called N-PMIPv6 [84]. N-PMIPv6 extends the scope of the fixed MAG defined in PMIPv6 to include the moving MR defined in NEMO, so that a mobile terminal with an assigned prefix can roam within a newly defined domain, called the N-PMIPv6 domain, without changing its IP address. Thus, the moving MR becomes a moving MAG, called mMAG.

In the N-PMIPv6 domain, the mobility management of an mMAG is managed in a similar way as a mobile terminal is handled in the PMIPv6 domain. The mobile terminal sees the attached mMAG as a fixed MAG. To route IP packets, the LMA caches binding entries for the mMAGs, and the cached binding entries are extended from the original LMA definition so as to include a flag to show whether or not an mMAG manages the entry. As shown in Fig. 12, the prefix information of MT-1 is stored in the binding cache table. Since mMAG-1 manages MT-1, the "M flag" of the MT-1's entry is set to "yes" in order to indicate that a moving MAG manages this MT. When CN1 communicates with MT-1, the LMA conducts a recursive lookup to search for the prefixes for MT-1. First, the LMA locates the serving mMAG to which the MT-1 is attached, and then, the LMA searches for the fixed serving MAG (i.e., MAG-2) of the mMAG for MT-1 found in the first round. Once the information has been identified, the LMA constructs an IP tunnel for the communications between CN1 and MT-1.

When MT-1 moves away from mMAG-1, mMAG-1 sends a de-registration Proxy Binding Update (PBU) to LMA in order to update the cache entry of MT-1. When MT-1 moves into the coverage of MAG-3, MAG-3 sends the PBU to LMA to update the serving MAG and the flag information. The access router (AR) value is updated with "MAG-3" and the M flag value becomes "no". In this example, the IP address of MT-1 does not needs to change, as shown in Fig. 12, as it always remains with the same assigned prefix, Pre3::/64. Once the LMA finishes updating MT-1's entry in the LMA binding cache, the communications between CN1 and MT-1 can be directed via MAG-3 with a new IP tunnel.

N-PMIPv6 was compared with a combination of NEMO, MIPv6, and PMIPv6 solutions through simulation. In terms of the TCP traffic, N-PMIPv6 can outperform the combined approach. However, when vehicles form a VANET, the proposed scheme did not address a way to extend the mobility management via multihop connections.

6.3. Hybrid Centralized DMM

The concept of distributed mobility management (DMM) was proposed to address several problems found in the standard solutions (e.g., MIPv6 and PMIPv6) [97]. These problems of the existing mobility management schemes include non-optimal routes for data packets, complex or hierarchical architectures that deviate from a desired flat network architecture, scalability concerns for central tunnel management, security concerns for a centralized architecture (e.g., a central node's failure or attack target), and mobility signaling overhead in P2P communication patterns (e.g., V2V communications). Currently, it is necessary to use DMM solutions to provide a set of new functions including the availability of multiple anchors for a moving MN, the dynamic assignment or reallocation of anchors, and the management of multiple IP addresses.

However, for the deployment of DMM in a highly mobile environment, several new challenges may also arise, e.g., managing multiple IP addresses and tunnels, high signaling over-

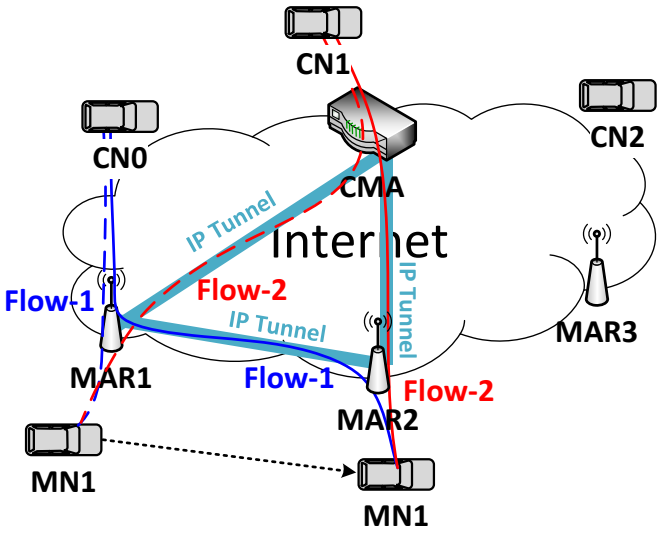


Figure 13: Hybrid centralized DMM for highly mobile nodes.

head due to mobility, and increased handoff delay caused by the increased number of IP addresses and tunnels. In order to address these challenges, the authors in [85] presented a hybrid centralized DMM scheme called H-DMM. The H-DMM scheme combines DMM and PMIPv6 so as to allow an MN to get two different prefixes. The two prefixes are acquired through a Mobile Access Router (MAR) of the DMM solution and a Central Mobility Anchor (CMA) of the PMIPv6 solution, respectively; note that CMA is called LMA in PMIPv6. When moving within the domain of H-DMM, an MN, which is based on the features of the ongoing traffic flows and the count of active prefixes, selects the proper solution (i.e., DMM or PMIPv6) to process mobility management.

Fig. 13 shows the mobility management process suggested by H-DMM. As shown in the figure, the MN1 obtains two prefixes when it is initially attached to MAR1. Meanwhile, the two CNs (i.e., CN0 and CN1) are communicating with MN1, as represented by flows Flow-1 and Flow-2 in dashed lines. When MN1 is attaching to MAR2, Flow-1 follows the operation of DMM by using the IP tunnel constructed between MAR1 and MAR2, whereas Flow-2 uses the process of PMIPv6 that builds an IP tunnel between CMA and MAR2. H-DMM extends the information in the binding cache entry stored in CMA to include both CMA and MAR prefixes for an MN. The results of the numerical analysis in the paper show that H-DMM outperforms the DMM and PMIPv6 schemes in terms of signaling cost, packet delivery cost, and end-to-end delay. However, in terms of handoff latency, H-DMM is worse than PMIPv6 due to the hybrid mobility management.

6.4. Hybrid Centralized NEMO

To support the IP mobility management for moving IP networks, Nguyen et al. introduced a scheme that combines DMM and PMIPv6 to support mobile nodes and mobile routers roaming across different IP subnets. The scheme corresponds to a Hybrid Centralized DMM architecture based on Network Mobility (H-NEMO) [86]. Although there is a standard NEMO-BS protocol [42] to support IP mobility for moving networks, it retains many of the problems found in MIPv6 caused by suboptimal routing. Hence, the authors in [86] proposed a combination of DMM and PMIPv6 that routers (e.g., MRs) and nodes (e.g., MNs) make use of different IP prefixes depending on the lifetimes of the traffic flows. For example, in the case of a long-lived flow, an MR (or MN) chooses an IP address from the prefix obtained from a CMA (i.e., the PMIPv6 anchor entity); by contrast, in the case of a short-lived flow, an MR (or MN) chooses an IP address from the prefix obtained from the MAR (i.e., the DMM anchor entity).

For the mobility support of the MNs and the moving network, H-NEMO considers three scenarios:

- Handoff for a moving network changing the connection point from the current MAR to a new MAR.
- Handoff for an MN traveling in a moving network and attached to an MR; the MN is changing the connection point from the current MR to the subnet of an MAR.
- Handoff for an MN attached to an MAR and changing the connection point to a moving network (i.e., the MN is connecting to a new MR).

H-NEMO also suggests placing a connection manager (CM) application at the MR (or MN) so as to help different traffic flows select appropriate interfaces and IP addresses.

The work provides a numerical performance comparison of H-NEMO and other similar schemes. The metrics used for this evaluation include signaling overhead, packet delivery cost, handoff latency, and end-to-end (E2E) delay. The reported results show that H-NEMO outperforms other centralized and distributed proposals for IP network mobility, particularly in terms of handoff delay, packet delivery cost, and E2E delay. In certain specific cases for increased velocity, H-NEMO was shown to be costly regarding signaling overhead, so it is not suitable for the mobility management for high-speed vehicles in a highway.

6.5. Peer-Assisted IP Address Handoff Method

In order to assist the handoff process on a highway, the authors in [87] proposed that vehicles may acquire IP addresses via V2V communications. In the case where a vehicle moves to an out-of-range zone, the surrounding vehicles, either on the same or opposite roadways, help the vehicle acquire a new IP address from the infrastructure, and may also assist it with the execution of a pre-handoff mechanism. The objective of the peer-assisted handoff is to minimize the handoff delay and maintain Internet connectivity stably.

The system model proposed in [87] is based on a hybrid wireless network with IEEE 802.11 and 802.16 connectivity. The model considers both private vehicles and public transports, with special consideration to a case where a bus requires the assistance of two onboard mobile routers for the pre-handoff mechanism. The proposed handoff procedure is evaluated via simulations, with comparisons to standard protocols such as

NEMO-BS and Fast handoff for MIPv6 [98]. The applicability of the peer-assisted scheme to different road contexts (e.g., urban scenarios) was not addressed by the authors.

6.6. PMIPv6-based NEMO

As mentioned above, the standard PMIPv6 protocol only supports network-based mobility for single nodes. Therefore, in order to extend the support of PMIPv6 to mobile networks, Lee et al. introduced a P-NEMO scheme [88] based on PMIPv6. In P-NEMO, an onboard router, known as an MR, receives a mobile network prefix (MNP) and a home network prefix (HNP), which can be attributed to an extension of the binding update lists located at the infrastructure entities, namely, the MAG and the LMA. With the MNP, the local moving network served by the MR is enabled with IP mobility support. The P-NEMO scheme aims to reduce the signaling load while maintaining Internet connectivity for the moving networks.

In order to improve the performance of the IP mobility procedure, the authors also proposed integration with the standard fast handoff for PMIPv6, as defined in the RFC5949 [99]. Both modes of operation (i.e., reactive and predictive) are considered for the proposed fast P-NEMO (FP-NEMO). With the integration proposed in FP-NEMO, the transferring of context information between two MAGs handling a handoff also includes the MNP, which provides mobility support for mobile nodes moving together within the vehicle.

This work is evaluated analytically for both P-NEMO and FP-NEMO. Although the evaluation includes comparisons with the standard NEMO-BS, it has not provided a comparative analysis with other PMIPv6-based schemes for mobile networks [84].

6.7. Multiple Base Stations Mobility Support

To fully utilize the connectivity of vehicles with the fixed infrastructure, Peng et al. introduced a scheme with which to provide mobility management to moving vehicles using several base stations belonging to a Roadside Multihop Cell [89]. The main idea is to take advantage of the street layouts as well as the availability of connectivity to more than one base station, so as to reduce the mobility management overhead. Several base stations—as opposed to just one—that are close to a destination vehicle are in charge of discovering the connection to the vehicle simultaneously. The scheme was evaluated using microscopic traffic simulations with SUMO [100], and the results show a reduced overhead as well as an increased data delivery ratio.

6.8. SDN-enabled DMM

In a recent contribution, the authors in [90] introduced a hybrid architecture that combines Software-Defined Networking (SDN) with IPv6 DMM. SDN has attracted attention due to the fact that it provides the ability to divide a network into a control plane through an SDN controller and a data plane through SDN switches [101]. This ability makes the network architecture highly scalable in terms of supporting dynamic flows. In addition, in contrast to the traditional routing and mobility management schemes, in OpenFlow [101], the optimization is based

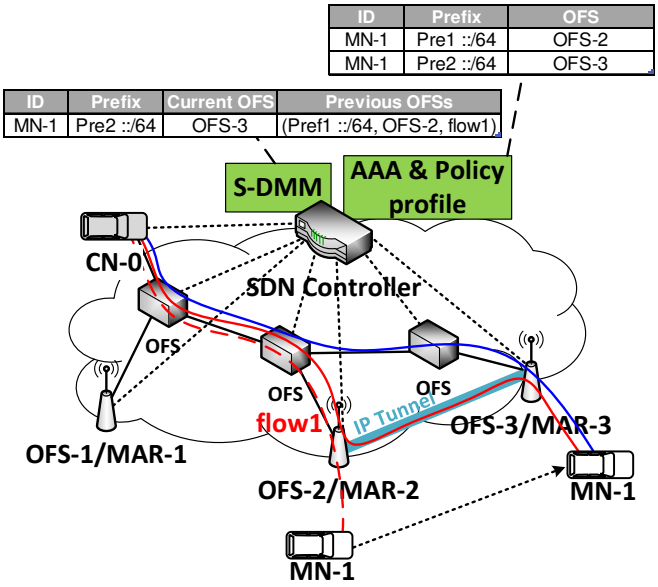


Figure 14: SDN-based distributed mobility management for 5G networks.

on the flows instead of the routes. Hence, with OpenFlow, one can group several flows over the same route, or distribute a single flow over different routes. It is also possible to notice a broken flow earlier than in the traditional networking architectures. An SDN controller can efficiently manage the configuration of the optimal routes between a CN and a vehicle.

In the application of SDN with DMM for IP mobility proposed by Nguyen et al. [90], the mobility function is delegated to the OpenFlow Switches (OFSs) to manage the data plane, whereas one or several SDN controllers can host the control plane of the mobility management. The architecture is illustrated in Fig. 14. The proposed architecture is shown to be more scalable than a standard DMM scheme without SDN.

The authors conclude that IP mobility management schemes in the future should consider an SDN architecture. Aside from the separation of identity and routing functions, the IP mobility management schemes also require the separation of control and data planes, which can be inherently solved by SDN. This separation is critical for providing scalability to VANETs in roads. Further, the flow management with OpenFlow may facilitate the operation of heterogeneous vehicular networks with multiple RAT and multi-protocols. Thus, the combination of DMM and SDN can help to provide easier implementation and reconfiguration of route optimizations together with a dynamic flow detection mechanism.

6.9. NEMO-based Mobility Management

In the survey presented by Céspedes et al., the authors identified the challenges of using NEMO Basic Support (NEMO-BS) [42] in VANET [91]. The NEMO-BS protocol is defined to manage mobility for moving networks, but it was not designed to consider the characteristics of a vehicular network. This work identifies several sub-optimal cases in which the tunneling cost of NEMO-BS results in significant overhead over the wireless network that provides connectivity to the moving

vehicles. Beyond the traditional requirements of an IP mobility management scheme – reduced handoff delay, reduced complexity, and reduced overhead or bandwidth consumption – the authors identified additional requirements specific to the vehicular networks. Among the requirements listed are the separability of traffic (i.e., for IP mobility purposes) at the flow-level, minimum signaling overhead to optimize the route between the vehicle and the correspondent node, and security and binding privacy protection.

The classification of the existing optimization schemes for NEMO-BS considers the use of single-hop or multihop connections to the correspondent nodes. The schemes reviewed for the former category include mobility-related mechanisms such as direct tunneling between the MR (i.e., the vehicle's onboard router) and the correspondent node, the use of MIPv6 by nodes traveling with the vehicle (as a replacement of NEMO-BS), and the bypassing of the home agent (HA). In the case of multihop connections, the presented schemes considered a sub-IP multihop delivery to avoid nested NEMOs as well as the direct tunneling between two vehicles.

The authors concluded that a better use of geographic information at a sub-IP layer should be incorporated in order to establish direct links between vehicles and to reach the access routers in a multihop fashion. They also identified that several route optimization schemes pose a significant overhead over the wireless links or an increased delay due to the need to detour the connections via home agents located far away.

Fernández et al. investigated a NEMO-based multi-domain handover process for IPv6-based vehicular networks [92], which implements an ISO/ETSI reference architecture that combines NEMO, multi-care-of-addresses registration extension, and IEEE 802.21 standard for media independent handoff [102, 103, 104]. Their experiment results showed that the proposed approach can reduce the handoff time for vehicles moving among different domains.

6.10. Vehicle Authentication with Shared Keys or Local Keys by PMIPv6

PMIPv6 was developed to simplify the network control and reduce the signaling overhead in mobility management. Due to the shorter handoff delay and other benefits, implementations of PMIPv6 have become increasingly popular. In order to provide security and privacy to PMIPv6, several schemes were introduced using the AAA server. Zhou et al. introduced an authentication scheme using Diameter protocol and employed a shared key with AAA, MN, LMA, and MAG [108]. However, increasing message exchanges to establish an authentication can be a problem. When a vehicle travels at a high speed, establishing a connection with authentication efficiently and quickly is crucial for sending reliable information to its destination.

To address the delay issue, several schemes have been introduced using a local authentication approach. For example, Song et al. proposed an authentication using a one-time key, where the key is generated using a timestamp method [93]. As an alternative, Lee et al. proposed a ticket-based authentication mechanism for PMIPv6 [109]. The ticket-based approach optimizes the handoff authentication process, which can prove that MN is a legal node.

6.11. Key Observations

IP mobility management in vehicular networking is the most critical aspect for the successful forwarding and delivery of data packets while vehicles are moving along roadways.

- Firstly, the vehicular mobility brings new challenges for the traditional IP mobility management solutions given the particular characteristics of a moving network, including dynamic topologies, various mobility patterns, and spatio-temporal variations in network density.
- Secondly, depending on the applicable scenarios (e.g., highway and urban roadways), mobility management solutions are likely to differ.
- Thirdly, among the reviewed works, the hybrid schemes with combinations of host-based mobility (e.g., MIPv6) and network-based mobility (e.g., PMIPv6 and NEMO), along with more recent proposals with fine-grained mobility management (e.g., PMIPv6 and DMM), typically show better performance than a single protocol.
- Fourthly, the majority of the IP mobility schemes were only tested with computer simulations or analytic modeling; few real experiments and validations have been conducted [110].
- Fifthly, in the near future, the IP mobility management may be potentiated with SDN-based schemes, since SDN may provide better ways to deal with heterogeneous traffic as well as the separation of the control plane and data plane for IP mobility purposes.
- Lastly, for the mobility management of fast moving vehicles, the vehicular networks should provide vehicles with efficient, light-weight authentication, and security session management services. Thus, the layout of vehicular networks and the vehicle trajectories should be utilized to let these services work in a proactive way.

7. Standardization Activities for IPv6-Based Vehicular Networks

This section provides a survey of the standardization activities for vehicular networking. We review IP-based vehicular network standards from different SDOs, such as IEEE, IETF, ETSI, ISO, and 3GPP. Table 6 shows standardization activities for IPv6-based vehicular networks to let the audience see the relationship among those SDOs for IPv6. Fig. 15 shows the standardization scope and relationship of the SDOs.

Table 6: Standardization Activities for IPv6-Based Vehicular Networks

SDO	Standards	Scope
IEEE	IEEE 1609 standards [7, 8, 9, 10] and IEEE 802.11-OCB [105]	A vehicular architectural framework and also vehicular protocol stacks for both safety and non-safety applications
IETF	RFC 8691 [106] and IPWAVE Problem Statement [107]	IPv6 over IEEE 802.11-OCB and also the IPWAVE problem statement with use cases
ETSI	ETSI EN 302 636-6-1 [17]	IPv6 over GeoNetworking with an adaptation sub-layer to provide vehicles with IPv6 networking in geographic networks
ISO	ISO/TC 204 [16]	The support of IPv6 services for using a vehicle as an access router for the sake of the Internet connectivity for other mobile devices
3GPP	TS 23.285 [3], TR 22.886 [4], and TS 23.287 [5]	V2X architecture and functionality to provide vehicles with IPv6 services in cellular networks

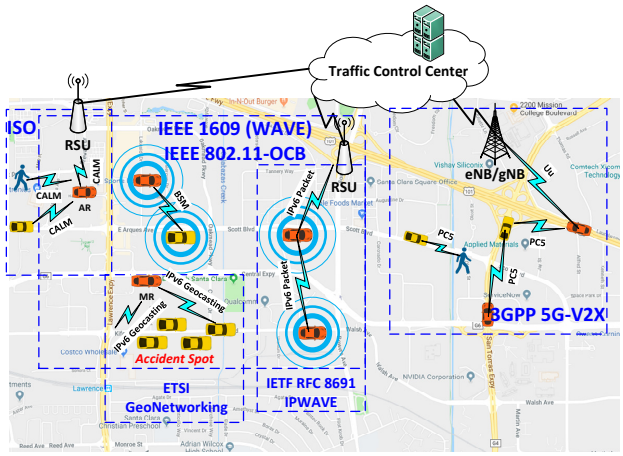


Figure 15: Standardization scope and relationship of SDOs.

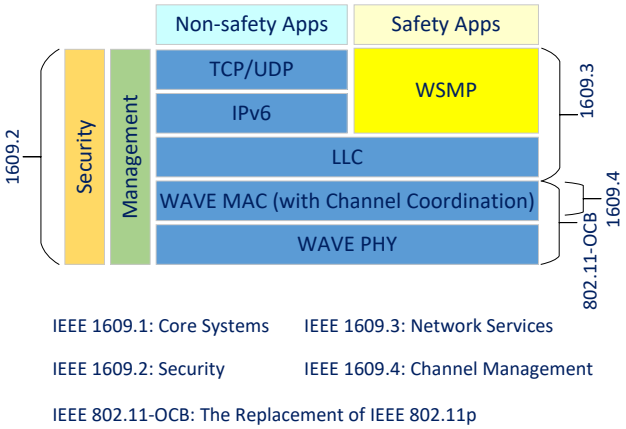


Figure 16: IEEE 1609 WAVE protocol stack.

7.1. IEEE WAVE for Vehicular Communications

IEEE standardized Wireless Access in Vehicular Environments (WAVE) as the IEEE 1609 standards for safety services of road driving. The IEEE 1609 standards include a vehicular architectural framework combined with protocol stacks for both safety and non-safety applications. The base document is IEEE 1609.0 which defines the WAVE architecture [7]. IEEE 1609.2 specifies vehicular security [8], IEEE 1609.3 defines vehicular networking services with network layers and transport layers [9], and IEEE 1609.4 defines multi-channel operations [10]. In addition, IEEE 802.11p defines the PHY and MAC layers of vehicular communications [111], which was renamed IEEE 802.11-OCB in 2016 [105]. The IEEE Task Group 802.11bd (TGbd) has been working on an enhanced DSRC-based vehicular communication standard with several improvements including a higher throughput than IEEE 802.11-OCB [112].

The IEEE 1609.0 standard describes the architecture and operations of the WAVE protocol stacks [7], which is called the WAVE reference model. This reference model is described in Fig. 16, and can accommodate applications for both safety and non-safety use cases. The WAVE PHY and MAC in IEEE 802.11-OCB are common to the protocol stacks for these two kinds of applications. The Logical Link Control (LLC) sublayer in the IEEE 1609.3 standard [9] determines whether a WAVE MAC frame is destined for the safety-application protocol stack or the non-safety-application protocol stack with a MAC frame field called Ethertype in the LLC header. Thus, the IEEE 1609.3 standard specifies the data plane for WAVE networking services, including LLC, IP stack for non-safety applications, and WAVE Short Message Protocol (WSMP) stack for safety applications.

In the network protocol stack, the TCP/IP stack supports IPv6 instead of IPv4 in order to benefit from the abundant address space and various autoconfiguration mechanisms of IPv6. This IP stack supports TCP and UDP as transport layer protocols and forwards the IP payloads according to the port numbers associated with the transport layer protocol. By constrast, the WSMP stack works as the network layer and transport layer for safety applications and forwards the WSMP payloads according to the Provider Service Identifiers (PSIDs) used as the identifiers in the WSMP context. Note that IP packets can only be transmitted via DSRC service channels (SCHs), and WSMP packets can be transmitted via any DSRC channel, including SCHs and the control channel (CCH), for safety-critical message delivery.

The IEEE 1609.3 standard supports the IPv6 address autoconfiguration by its functional feature without using the IPv6 Neighbor Discovery (ND) protocol [9]. This feature is provided by the WAVE service advertisement (WSA) for the available service information delivered by a WSMP message. In particular, the WAVE Routing Advertisement (WRA) as a variable-length field in a WSA message includes Router Lifetime, IP Prefix, Prefix Length, Default Gateway, and Primary DNS Server. This eliminates the IPv6 ND's basic discovery of the IP prefix and DNS information, which uses RA on top of ICMPv6. Thus,

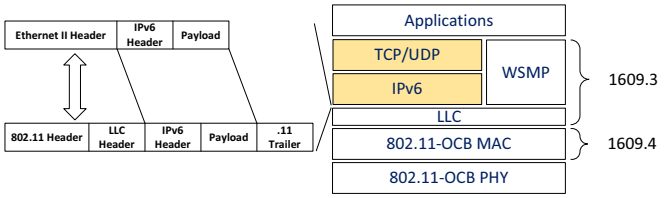


Figure 17: Ethernet adaptation defined in IETF RFC 8691.

an RSU can advertise WSA messages that have the routing advertisement as well as the service information and channel information. When a vehicle receives such WSA messages from the RSU, it can configure the basic network parameters for V2I communication with the RSU.

The IEEE 1609.4 standard describes multi-channel operations for a MAC sublayer that controls the transmission of the data packets received from an upper layer (i.e., IP and WSMP) over the different channels available [10]. These operations consist of channel coordination, channel routing, and user priority. The first operation (i.e., channel coordination) allows WAVE devices' resources to be coordinated among data packets that will be transmitted on an appropriate DSRC channel in an appropriate time slot. The second operation (i.e., channel routing) performs the routing of data packets from an upper layer (e.g., TCP and UDP) to a channel with the appropriate parameter setting (e.g., transmission power) as well as the routing of the received data packets to a designated upper layer protocol. The third operation (i.e., user priority) accommodates eight levels of MAC-sublayer priority according to the priority required by the (safety or non-safety) application. This priority is associated with the function of Enhanced Distributed Channel Access (EDCA) in IEEE 802.11e [105].

7.2. IETF IPWAVE Working Group: Transmission of IPv6 Packets over IEEE 802.11-OCB

IETF has formed a working group to explore potential IP-based solutions for Internet access for vehicles based on IEEE 802.11-OCB [105]. The working group was named the IPWAVE Working Group (WG) [113] (i.e., IP Wireless Access in Vehicular Environments). Note that IEEE 802.11-OCB replaced IEEE 802.11p in 2016. IPWAVE WG has been working on two work items: one aims to standardize the transmission of IPv6 packets on IEEE 802.11-OCB links, which has been published as RFC 8691 [106]; the other one aims to specify a problem statement by surveying the existing vehicular networking solutions, problems, and use cases, and by analyzing the technology gaps and requirements in the area to guide future work to further improve IPv6-based vehicular networks [107].

RFC 8691 [106] specifies several parameters to allow IPv6 packets to be transmitted successfully on the 802.11-OCB link, such as the supported Maximum Transmission Unit (MTU) size, the header format, and the Type value in the header. The document identifies two kinds of exceptions in the IPv6 network layer operating on 802.11-OCB by comparing the operations on Ethernet and 802.11 links. The protocol stack is shown in Fig. 17. For the differences between 802.11-OCB and 802.11

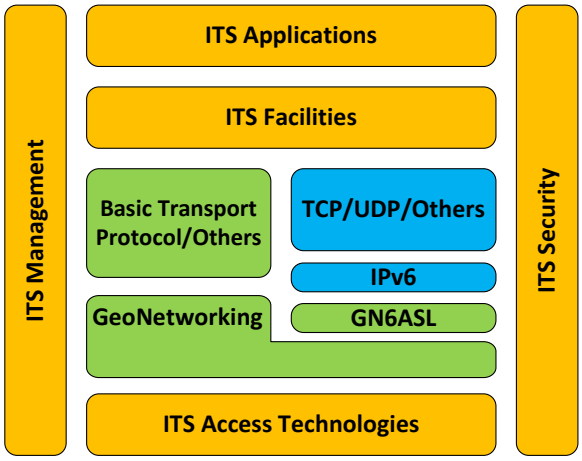


Figure 18: Combination of the GeoNetworking protocol and IPv6.

links, the document recommends using a 64-bit Extended Unique Identifier (EUI-64) [114], which is made by combining 16-bit 0xFFFE and a 48-bit MAC address, to form an IPv6 link-local address [115]. A group of vehicles can form a subnet structure made of 802.11-OCB interfaces, and the subnet needs to use a link-local prefix of IPv6. The interfaces also need to be assigned link-local IPv6 addresses.

The document also suggests some solutions for dealing with security issues and privacy considerations. For general security requirements, IEEE 1609.2 [8] can provide security services in the application layer, and IPsec can provide IP data security to a broader range of applications. The Public Key Infrastructure protocols can also be used to create vehicle credentials. Regarding privacy considerations, the document strongly suggests using privacy protection methods, such as dynamic MAC addresses [116], opaque interface identifiers [33], and stable interface identifiers [117].

The second working document (i.e., IPWAVE problem statement and use cases) [107] attempts to identify the technology gaps between the current IP protocols and the new challenges in vehicular environments. The document focuses on exploring problems in IPv6 neighbor discovery protocol, link model, mobility management, and security. Based on this document, the future work items in IPWAVE WG can include the transmission of IPv6 packets in both DSRC and cellular networks and an extension of IPv6 ND for a vehicle network architecture.

7.3. ETSI Intelligent Transport Systems: Transmission of IPv6 Packets over GeoNetworking Protocols

The ETSI EN 302 636-6-1 [17] standard specifies the transmission of IPv6 packets over the GeoNetworking (GN) Protocol [12]. For such IPv6 packet transmission, an adaptation sublayer is defined, named GeoNetworking to the IPv6 Adaptation Sub-Layer (GN6ASL). This GN6ASL shown in Fig. 18 allows a vehicle (as an IPv6 host) to perform the following three IPv6 operations: (i) the acquisition of a global IPv6 unicast address for packet routing in the Internet, (ii) exchange of IPv6 packets with other vehicles, and (iii) network mobility support through a Mobile Router [42].

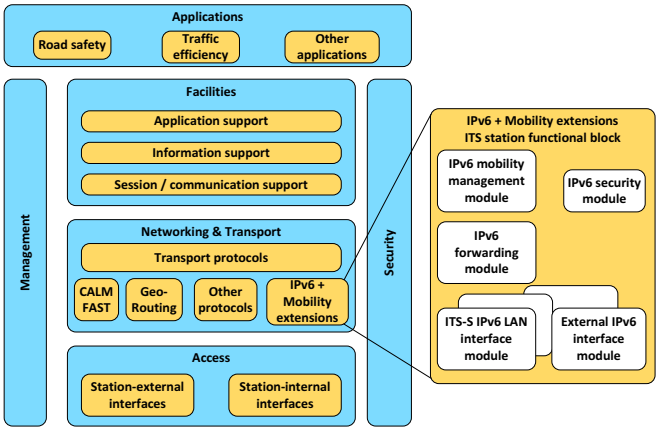


Figure 19: ISO intelligent transport systems: CALM using IPv6 networking.

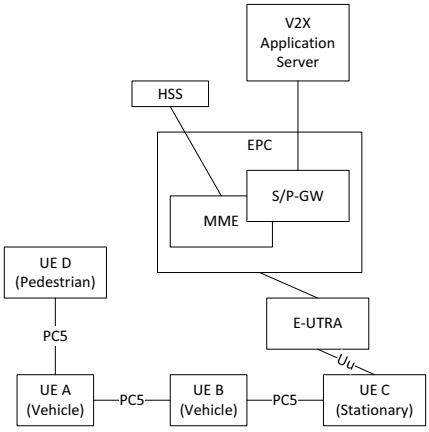


Figure 20: 3GPP LTE V2X architecture.

The standard for GN6ASL defines three kinds of virtual links. The first virtual link is a link with symmetric link reachability while the remaining two links are links in a broadcast domain. These three links support the IPv6 ND with Stateless Address Autoconfiguration (SLAAC) [32], the delivery of IPv6 link-local multicast packets, and the delivery of IPv6 packets between geographic boundaries. Note that these links work via the GN6ASL and IPv6, and that they are constructed by virtual network interfaces. The standard for GN6ASL includes the bridging over the GN6ASL, IPv6 packet encapsulation in GN packets, IPv6 multicast and anycast in the GN, and a rapid neighbor discovery with the SLAAC.

In order to ensure a vehicle's privacy (i.e., the prevention of vehicle tracking), the pseudonym of a GN address is supported. That is, whenever the GN address changes, the corresponding IPv6 address is updated.

7.4. ISO Intelligent Transport Systems: CALM Using IPv6 Networking

An ISO standard specifies the support of an IPv6 protocol and its services [16]. These services include the global reachability of a vehicle (or smartphone) connected to the Internet, the stability of this Internet connectivity, and a handoff for the transfer of Internet connectivity. They allow various types of mobile devices (e.g., smartphones and tablets) to use the vehicle as an Access Router providing them with the connectivity to the Internet. The standard includes an IPv6 configuration for vehicles and the corresponding management function.

The standard supports all types of IPv6 nodes, such as smartphones, vehicles, RSUs, and central cloud nodes. It defines IPv6 functions, such as IPv6 address configuration, IPv6 packet forwarding, IPv6-to-MAC address resolution, IPv6 security, and mobility management; Fig. 19 shows these IPv6 functions. Thus, through the use of these functions, two nodes (e.g., a vehicle and a smartphone) can exchange IPv6 packets through IPv6 address reachability in the Internet.

7.5. IP Support in Conventional Cellular Networks for Intelligent Transportation Systems: 2G/3G and 4G-LTE

IP has been supported in cellular networks since the General Packet Radio Service (GPRS) in the 2nd generation cellular networks of Global System for Mobile communications (2G-GSM) was developed and maintained by the 3rd Generation Partnership Project (3GPP). The 2G- and 3G-based radio accesses separate end-user data traffic (User Plane) from network transport traffic among the network elements (Transport Plane). The two planes run independently in terms of addressing and IP version. The Transport Plane forms tunnels to transport user data traffic [118].

The 4G-Long-Term-Evolution (4G-LTE) radio access simplifies the complex architecture of the GPRS core network by introducing the Evolved Packet Core (EPC). Both 2G/3G and 4G-LTE systems differentiate user data by Access Point Names (APNs). User traffic is transported via the Packet Data Protocol (PDP) Contexts in GPRS and Packet Data Network (PDN) Connections in EPC. Different forms of traffic at a UE side need to connect to the PDNs corresponding to different APNs through multiple PDP Contexts or PDN Connections. Each of the contexts and connections needs to have its own IP address.

IPv6 is partially supported in 2G/3G and 4G-LTE. In 2G/3G, a UE can be allocated an IPv6 address in two different ways: IPv6 and IPv4v6 PDP Contexts. With the IPv4v6 PDP Contexts, both an IPv4 address and a /64 IPv6 prefix are allocated. The IPv6 address allocation of 4G-LTE networks has a process different from that of 2G/3G networks. The major difference is that 4G-LTE builds the IP connectivity at the beginning of a UE attachment, whereas the IP connectivity of 2G/3G networks is created on demand. Each of the 3GPP networks (i.e., 2G/3G and 4G-LTE) only supports SLAAC address allocation, and it is not suggested to perform DAD in any of the networks. In addition, the 3GPP networks remove the link-layer address resolution, which is a function of the IPv6 ND protocol, due to the assumption that either the GGSN (Gateway GPRS Support Node) in 2G/3G networks or the P-GW (Packet Data Network Gateway) in the 4G-LTE networks is always configured as the first-hop router for a UE through either 2G/3G PDP Contexts or 4G-LTE PDN Connections, respectively.

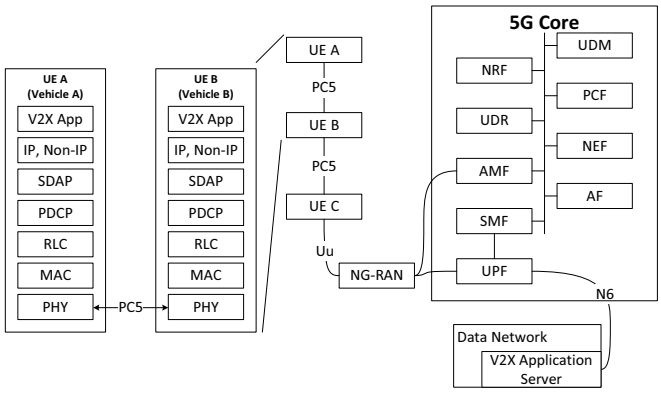


Figure 21: 3GPP 5G V2X architecture.

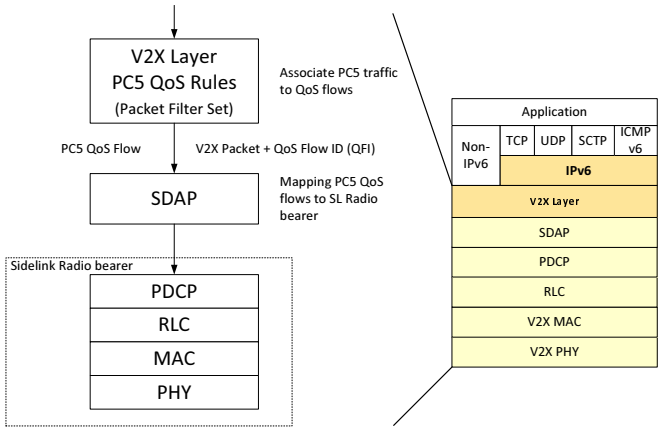


Figure 22: 3GPP 5G V2X protocol stack for a UE.

7.6. IP Support in 5G-NR V2X for Intelligent Transportation Systems

Recently, 3GPP has proposed a new technical set of specifications [4, 3, 119], which provides an enhanced architecture for vehicle-to-everything (V2X) services using the modified sidelink interface that was originally designed for LTE Device-to-Device (LTE-D2D) communications. As shown in Fig. 20, UEs can communicate with each other by the PC5 interface in the new LTE V2X architecture. A stationary UE (i.e., RSU) can also communicate with a remote V2X application server via the existing Uu interface by the physical sidelink, as UE C shown in Fig. 20. According to this architecture, a pedestrian with a UE can communicate with another UE (i.e., vehicle) directly via the sidelink too. This architecture can facilitate more applications to be developed on both smartphones and a vehicle's on-board computers that can provide smartphone users with an enforced vehicle traffic safety service. The enhanced architecture for V2X services [3] specifies that V2X services only support IPv6 implementation. However, different from the assumption of the subnet model in the cellular networks, if UEs only running at the PC5 interface have no first-hop router to configure IPv6 parameters, then only link-local IPv6 addresses are configured for them and are used for data communication between them while the DAD procedure is disabled.

In addition, 3GPP has been continuously studying new V2X service requirements in 5G new radio (5G-NR) networks [5]. Fig. 21 shows a further enhanced 5G V2X architecture. Similar to the 4G-LTE V2X architecture, UEs can communicate with each other by the PC5 interface in 5G V2X architecture. A UE can also communicate with a V2X application server via a Next Generation Radio Access Network (NG-RAN, e.g., gNodeB in 5G network) by the Uu interface [5, 120]. Following the overall design of 5G networks, the protocol stack of a UE particularly pays attention to the QoS function by adding a new Service Data Adaptation Protocol (SDAP) layer [120] to map QoS flows to an underlying sidelink radio bearer in this 5G V2X architecture. Fig. 22 shows a detailed protocol stack of a UE in 5G V2X architecture. Both IP and non-IP data units coming from a higher layer that use PC5 interface are associated with a QoS flow at the V2X layer in line with PC5 QoS rules [5], and an associated PC5 QoS flow is further mapped to a sidelink radio bearer at SDAP layer. This sidelinke radio bearer follows the predefined QoS mapping metrics [5] to allocate resources for PC5 QoS flows.

8. Summary and Analysis

We have investigated the up-to-date technologies of IP vehicular networks, including the vehicular network architecture, IP address autoconfiguration, mobility management, and security & privacy. This section summarizes those technologies and analyzes them for vehicular networking problems in order to identify possible solutions of IP-based vehicular networking in V2X-based autonomous vehicle driving environments.

8.1. Vehicular Network Architecture

This paper shows that IP vehicular networking technologies can work well on top of the IEEE WAVE protocol suite, such as the IEEE 1609 standards and 802.11-OCB standard. Note that the WAVE protocol has its own autoconfiguration function that uses WSA as opposed to the legacy IPv6 ND-based autoconfiguration function for performance optimization in efficient communication and rapid vehicle speed support [38]. However, the WAVE support of TCP/IP-based applications requires further clarification for the IPv6 ND's features in an IP-based vehicular network architecture, such as the IPv6 link model, IPv6 address update by MAC address pseudonym, and movement detection for fast handoff. Thus, the IPv6 ND needs to be adapted to the vehicular network's characteristics, such as high vehicle speed, predictable vehicle mobility, and V2X-based multihop VANET.

For an efficient vehicular network architecture, the IPv6 ND needs to be enhanced for efficient IPv6 network operations. This IPv6 ND determines the performance of the IPv6 in mobile environments such as vehicular networks. It includes network parameter configuration (e.g., subnet prefix, default gateway, DNS servers, and DNS search list), neighboring node detection, and subnetwork movement detection. On the other hand, the WAVE can provide vehicles with the subnet information of the prefix, default gateway, and DNS server, but cannot provide the vehicles with DNS search list.

In order to facilitate seamless IP-based services in vehicular networks, the IPv6 ND needs to be extended in terms of

ND timing parameters (e.g., router lifetime for a gateway and message transmission interval). For example, IPv6 Neighbor Advertisement (NA) messages can be used to sense neighboring vehicles. The transmission intervals of these NA messages should be adapted according to the vehicle speed for prompt neighborhood sensing and according to the vehicle density for IPv6 ND message congestion. That is, the faster that vehicles are moving on a two-way highway, the shorter the NA interval is for prompt neighborhood sensing. In addition, the higher the vehicle density is in roadways, the longer the NA interval is to avoid NA packet collisions.

Furthermore, an IPv6 link in a vehicular network architecture should be defined for V2V and V2I in vehicular networks. In the legacy IPv6 link model, when the IPv6 nodes in a link reside in the same subnet, they can directly communicate with each other. However, in vehicular networks, a radio link is different from a wired link (e.g., an Ethernet link) in that the radio link is defined as communication coverage (i.e., geographical area) rather than as a line. In particular, in a V2V scenario, vehicles can construct a connected VANET with multihop relays using intermediate vehicles as packet forwarders. In this scenario, the vehicles in the VANET can have their IPv6 addresses configured with the same subnet prefix. In this case, when two vehicles are in the same subnet and further away from each other than the one-hop communication range, they cannot directly communicate with each other.

Thus, the legacy IPv6 link model does not hold in the vehicular networks. In order to overcome this limitation of the IPv6 link model, a vehicular link can be defined as a multi-link subnet with multiple V2V links in a connected VANET. For this vehicular link model to have the ability to support a multi-link subnet, the IPv6 ND should be extended to work in a connected VANET such that a hop count is added for an entry in a neighbor cache [38] so as to indicate the distance to the neighbor vehicle in the connected VANET. The NA messages need to be extended like routing protocol packets in order to include multihop-away neighbors in the connected VANET [107].

Vehicular nodes (e.g., vehicle and RSU) can have internal networks with IPv6 nodes such as in-vehicle devices and servers [107]. In this case, two IPv6 nodes within the internal networks of two vehicular nodes can communicate with each other. In order to allow for wireless communication between those internal nodes in different internal networks, the network prefix dissemination or exchange is required among vehicular nodes. A vehicular node can communicate with another node through its external network interface.

Thus, for IP-based vehicular networks, the legacy IPv6 ND [38] needs to be extended to a vehicular ND [121] in order to allow for communication between the internal network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) of vehicular nodes via the external network interfaces by letting each of them know the other side's prefix with a new ND option for internal network prefixes. Therefore, this ND extension for routing information of internal networks can reduce control traffic without needing to run additional routing protocols in vehicular networks.

8.2. IP Address Autoconfiguration

IP address autoconfiguration is the first step in vehicular networking configuration so that vehicles can start communicating with other vehicles or RSUs. This IP address autoconfiguration can be performed using a server-based stateful approach and a location-based stateless approach. As discussed in Section 5, these two approaches have pros and cons. First, the server-based stateful approach has a little long delay and a little high overhead for searching for a DHCP server when vehicles join another cluster. Second, the prefix assignment per lane in the location-based stateless approach has a high overhead by the IPv6 DAD messages when vehicles change their lanes frequently. Also, it does not allow for direct V2V communication between adjacent vehicles in different lanes. Third, the prefix assignment per geographical area associated with an RSU's communication coverage may be better than the prefix assignment per lane in terms of control traffic reduction and one-hop communication between adjacent vehicles. However, when a vehicle is moving across the coverage of multiple RSUs, they still need to reconfigure their IPv6 addresses with different prefixes, leading to high overhead.

In order to overcome the limitations of the legacy IP address autoconfiguration schemes, efficient ways to disseminate IPv6 prefixes should be designed for both V2I scenarios and V2V scenarios. For the V2I scenarios, as in the prefix assignment per geographical area, RSUs can share a prefix for a radio vehicular link, so they can construct an extended subnet, like an extended service set in a WiFi LAN [107]. In this extended subnet, when a vehicle moves across the coverage of two adjacent RSUs, it does not update its IPv6 address, because the two coverage areas have the same network prefix as the same subnet. Thus, this method can reduce the frequency of IP address updates, leading to the reduced number of ND-related messages.

For the V2V scenarios, vehicles can continue to use the prefix that was advertised by the latest RSUs during their travel where those RSUs share the same network prefix for a radio vehicular link. In that case, the vehicles can communicate with the next RSU without changing their IPv6 addresses for V2I communication because the RSUs share the prefix. In addition, the IPv6 DAD can be extended as a multihop DAD to support an efficient duplicate address verification in a multi-link subnet [121]. For this extension, it is assumed that a mobility anchor in a TCC is connected to RSUs, RSUs have extended neighbor caches with the IPv6 addresses of the vehicles under their radio coverage, and a mobility anchor (e.g., LMA in PMIPv6) has a merged neighbor cache table with all of the neighbor caches of the RSUs under its control. When a vehicle performs DAD for its newly configured IPv6 address, it can verify the uniqueness of the IPv6 address through the current RSU and the mobility anchor. Thus, a vehicle can move fast across the coverage of multiple RSUs without changing its IPv6 address in the case where those RSUs share the same subnet prefix.

8.3. Routing and Mobility Management

The multihop data exchange between far-away vehicular nodes requires routing and mobility management. Currently,

autonomous vehicles and many other vehicles are equipped with GPS receivers for self-driving and navigation service, respectively. Using these GPS receivers, vehicles can localize their positions in road networks and recognize their moving directions and speeds. This GPS-based mobility information (e.g., position, direction, and speed) can give RSUs and the mobility anchor an important decision-making factor in routing for packet forwarding and mobility management for handoff.

Furthermore, navigation systems including GPS receivers are installed in most vehicles and all autonomous vehicles. Since a navigation system provides the future trajectory of a vehicle to RSUs and the mobility anchor, they can perform routing and mobility management for the vehicle in a more proactive manner by predicting the mobility of the vehicle based on its trajectory and mobility information [122]. For an improved proactive handoff, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator [64]), can be used to determine the moment of a handoff between RSUs. Further, the DAD can be performed proactively by the network rather than the vehicle itself [121]. In a vehicular multi-domain environment (e.g., WLAN, IEEE 802.11-OCB, and cellular networks), the handoff issue becomes more acute, since the dynamic of vehicle mobility becomes more random. A recent research has suggested a mobility prediction approach to improve the experience [123], however, new concepts and new paradigms are necessary for improving vehicular handoff.

With the previous observations, host-based mobility (e.g., MIPv6) and network-based mobility (e.g., PMIPv6 and NEMO) need to be designed such that they take advantage of the vehicle trajectories, road network layouts, and link-layer parameters in a proactive way.

Multihop packet forwarding among vehicles in 802.11-OCB mode may show unfavorable performance due to the commonly-known broadcast-storm problem [124]. This broadcast-storm problem can be mitigated by the coordination (or scheduling) of a cluster head in a connected VANET or an RSU in an intersection area, where the cluster head can work as a coordinator for access to wireless channels.

IP multicast in vehicular network environments is particularly useful for various services. For instance, an automobile manufacturer can multicast a service notification to a particular group/class/type of vehicles. As another example, a vehicle or an RSU can disseminate alert messages in a particular area [125]. In general, with IEEE 802.11 wireless media, some performance issues regarding multicast are found and described in [126]. Since several procedures and functions based on IPv6 use multicast for control-plane messages, such as ND and Service Discovery [127], the authors in [126] describes that the ND process may fail due to unreliable wireless links, leading to the failure of the DAD process. In addition, RA messages can be lost in multicasting. Thus, the multicasting in vehicular networks should be performed in a reliable way under such packet loss.

8.4. Service Discovery

A service discovery may be required for an application in a vehicular node to search for another application (e.g., cooperative cruise control) or server in another vehicular node, which resides in either the same internal network or another internal network. In V2I or V2V networking, such a service discovery can be provided by either DNS-based Service Discovery [127] with mDNS [128] or the vehicular ND [121] with a new option for service discovery [121]. However, using multicast-based approaches may lead to unreliable service discovery for the reason described in Section 8.3.

In addition, for efficient and effective operations, the service discovery needs to take advantage of the characteristics of road networks (e.g., road network layout and traffic signals) and the characteristics of vehicular networks (e.g., vehicle trajectories and infrastructure nodes (e.g., RSUs and mobility anchor)).

8.5. Security and Privacy

It is important to ensure security and privacy in order to protect vehicles from security attacks and tracking from hackers. For security, packets in vehicular networks can be encrypted by security keys and only decrypted by the intended recipients. For privacy, the identity information of a vehicle should be hidden from hackers. One popular method for such identity protection, an MAC address pseudonym, can be used [116, 36]. The major issue in the MAC address pseudonym is ensuring the correct delivery of IPv6 packets to destinations despite the fact that the IPv6 address related to a MAC address can change over time. Since a TCP session is identified by the pair of the IP addresses of the two end points, the update of the pseudonymous IP addresses of the TCP session should be notified to the TCP end points. For the support of TCP session continuity, whenever the network interface identifier changes, the notification of the IPv6 address change can be performed by a host-based mobility scheme (e.g., MIPv6). This pseudonym activity should be done so that hackers cannot figure out the identities of the vehicles.

9. Research Challenges and Issues

This section suggests several research challenges and issues in IPv6-based vehicular networks. They will motivate future research for IP-based solutions in vehicular networks.

9.1. Quality of Service in Heterogeneous Vehicular Networks

While DSRC-based IEEE 802.11-OCB vehicular network technology has been investigated for years, 3GPP recently also has published its V2X standard in 4G-LTE/5G networks, and especially it supports V2V communications without the management of a cellular station. The DSRC-based IEEE 802.11-OCB technology adopts a Quality of Service (QoS) function introduced from EDCA (i.e., Enhanced Distributed Channel Access) of IEEE 802.11e standard, which categorizes data traffic into four classes and gives each class a channel access priority. At 3GPP side, the latest enhanced architecture for V2X services in 5G networks [5] also adopts a more detailed flow-based QoS scheme in line with the major 5G standard [120]. It is expected that the two technologies will co-exit in the future, and a vehicle can have two major wireless interfaces: DSRC-based

Table 7: Research Challenges and Issues

Topic	Challenges
QoS in Heterogeneous Vehicular Networks	Different IP data traffic classifications between IEEE WAVE and 3GPP V2X protocols
TSN and DetNet in Vehicular Networks	Time-sensitive tasks handled by vehicle internal and external IP data packets
Privacy Protection	Efficient DAD and NUD operations of IPv6 ND for LISP and ILNP; Permanent identifier used in the LISP and ILNP; Privacy breakage in V2V using identifier of LISP and ILNP.
Vehicular Key Management	The distribution and maintenance of the public keys of vehicles.
Vehicular Blockchain	Blockchain technologies for road event logging and vehicle data sharing.
Vehicular MEC	New approaches and new paradigms for vehicular task offloading.
Vehicular Cloud Computing	Vehicle privacy breakages in vehicular networks

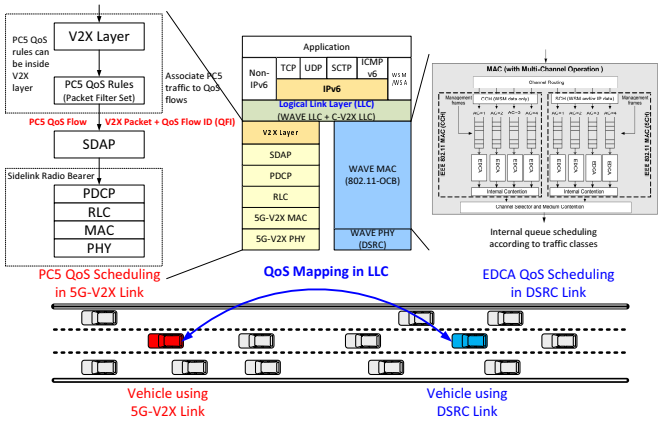


Figure 23: Challenge on QoS performances in heterogeneous vehicular networks.

IEEE 802.11-OCB and 3GPP V2X. However, they have different kinds of QoS mechanism, and it is still not clear how the two QoS mechanisms would affect IP data flows when the two technologies are used simultaneously. Fig. 23 shows a scenario where two vehicles are using LTE/5G V2X and DSRC links, respectively. Traffic flows between the two vehicles may have an issue on QoS performances. Thus, the vehicular network architecture needs to be designed to support the integration of QoS over multiple radio technologies (e.g., DSRC and LTE/5G).

9.2. Time Sensitive Networking and Deterministic Networking in Vehicular Networks

Time Sensitive Networking (TSN) [129] aims to provide a reliable, low-latency, and low-jitter traffic flow service at the link layer. TSN includes four aspects to provision the service, namely, synchronization, reliability, latency, and resource management [130]. For the reliability, TSN suggests a set of mechanisms, such as frame replications and eliminations, path control, per-stream filtering, and improved time synchronization. In the latency aspect, TSN proposes several approaches to achieve a bounded low latency, such as credit-based shaper, preemption, scheduled traffic, cyclic queuing and forwarding, and asynchronous shaping. These mechanisms and approaches are necessary for time-critical tasks in intra-/inter-vehicle networks [131]. However, the current TSN standards largely focus on wired Ethernet-based networks, which make it difficult to be applied directly to vehicular networks, considering the time-variant wireless communication environments. In addition, since the mechanisms in TSN mainly run at the link layer without any routing abilities, it is not clear how these mechanisms would affect IP-based traffic flows in multihop and multi-domain networks. As an example, an autonomous vehicle can also be tele-operated from a remote control center and some control commands embedded in IP packets from the control center have strict deadlines, these IP packets may experience congestion and packet loss on the way toward the target vehicle. If we consider mobility of the vehicle, the things become more complicated.

To address those issues, some tasks for Deterministic Networking (DetNet) on top of TSN have been proposed in DetNet WG of IETF, focusing on solutions in the network layer [132, 133]. So far, an overall DetNet architecture [134] has been proposed, and other work, such as DetNet data plane specifications, data flow informational model, and solutions over IP and Multi-Protocol Label Switch (MPLS), are ongoing. Nevertheless, since the primary purpose of DetNet is for wired networks, DetNet may not be able to mitigate unreliability, latency, and jittery issues caused by an uncertain wireless environment for IP-based vehicular networks. Thus, the above issues can hinder a reliable control process and bring high delay variations for connected autonomous vehicles.

9.3. Privacy Protection in Vehicular Networks

The MAC address pseudonym can partially protect the privacy of a vehicle (or driver) by periodically changing the MAC address of the DSRC wireless interface, and the corresponding IP address based on the interface's MAC address. A hacker can still keep track of the changes of the MAC address by observation, so (s)he can track the vehicle.

An approach for privacy protection is the separation of an identifier (ID) and a locator of a vehicle [135]. This separation allows a vehicle to be assigned a new IP address as a locator that corresponds to the subnet of an RSU having the vehicle. An ID-locator separation protocol, such as Locator/ID Separation Protocol (LISP) [136] and Identifier-Locator Network Protocol (ILNP) [137], facilitates a vehicle to have a new locator in a privacy-preserving manner whenever it visits the coverage of a new RSU. Thus, this separation disallows a hacker to track a

vehicle with its IP address or MAC address because the short-lived IP address and MAC address can be allocated to a vehicle only under the coverage of an RSU.

There are four research challenges related to the ID-locator separation [135]. The first research challenge is the extension of the IPv6 ND protocol for such ID-locator separation such that the IPv6 ND works efficiently in the DAD and NUD operations. The second one is the mobility management of a fast moving vehicle. The locator of the vehicle should be updated by the RSUs along the trajectory of the vehicle in a proactive manner. The third one is the privacy protection of an identifier associated with a vehicle. Since in the current approaches (e.g., LISP and ILNP), the identifier is permanent and is used by the ID-locator separation protocol, there is still some possibility that a hacker can identify a vehicle with its identifier at the initial stage of the ID-locator separation protocol. Thus, an additional method is required to protect the identifier. The fourth one is the privacy protection in a V2V (or V2X) scenario with no RSU. In this scenario, vehicles communicate directly with each other since there exists no RSU as a packet relay. In this case, if they use their identifiers (e.g., vehicle identification number), a hacker may identify and track them. Thus, a privacy protection scheme for the V2V (or V2X) scenario is required to mitigate a hacker's tracking trial.

9.4. Vehicular Key Management

A key management is important for the efficiency of asymmetric cryptography in vehicular networks. A Public Key Infrastructure (PKI) can be used for such a key management. However, this PKI-based solution assumes that a host (or server) is a stationary node without mobility or with a little mobility like a laptop computer with WLAN access. To support the high mobility of a vehicle, a vehicular network architecture needs to accommodate the quick registration of a vehicle's public key and the quick retrieval of other vehicles' public keys.

A vehicle has in-vehicle devices (e.g., Electronic Control Unit) and a driver/passenger's mobile devices (e.g., smartphone and tablet PC) where they are assigned unique IPv6 addresses in a vehicle. They can have individually their own certificate (e.g., X.509 certificate [138] and TLS certificate [139]). The registration and deregistration of those certificates should be supported by a vehicle and a vehicular infrastructure.

The operations related to the public keys and certificates can be performed using edge computing [15]. An edge computing device (ECD) near by an RSU can fetch the public keys of vehicles with which a vehicle will communicate in advance. The ECD plays a role of a local Certificate Authority (CA) for the operations of certificates of vehicles, which communicates with a central CA that shares the information of certificates with the local CA.

9.5. Vehicular Blockchain

A blockchain is a distributed database to maintain an increasing list of blocks which have transactions and are chained to each other [140]. This blockchain can provide vehicles with a distributed ledger for road event logging and vehicle data sharing in vehicular networks [107]. First, for road event logging, a blockchain-based incentive system can be constructed, and vehicles can be encouraged in participating in cooperative environmental sensing. Vehicles, which provide other vehicles with useful information (e.g., accident and hazard) in road networks, can get reward from such an incentive system. A vehicle's sensing data is disseminated as a transaction to neighboring vehicles and vehicular infrastructure. The neighboring vehicles and vehicular infrastructure perform a consensus method of a blockchain as a distributed ledger.

Second, for vehicle data sharing, a blockchain-based data sharing system can be constructed, and vehicles can participate in cooperative data sharing such as remote software update [141]. For remote software update for a vehicle, a software provider for an ECU in a vehicle can efficiently distribute a new software for the ECU to a blockchain of an overlay architecture. For a lightweight blockchain architecture [142], this overlay architecture consists of overlay block managers as cluster heads performing intensive blockchain operations (e.g., the construction and dissemination of a block with vehicle software updates as transactions) and vehicles as cluster members performing lightweight blockchain operations (e.g., the verification of a block with the transactions).

The research challenges for vehicular blockchain include how to make a lightweight overlay architecture for vehicular networks in terms of initialization and maintenance cost, how to make the overlay blockchain be resilient to various security attacks such as a DDoS attack for blockchain choking, and how to make the blockchain preserve user privacy from a link attack for user privacy disclosure.

9.6. Vehicular Multi-Access Edge Computing

The vehicular MEC is showing to be a new paradigm for edge computing tasks [15]. For a vehicular MEC, computation tasks can be distributed to the on-board computer of many vehicles. When finished, these distributed tasks are able to report their results toward the initiating entity, either a vehicle or a remote MEC client [143, 144, 145, 146]. To enable this kind of computing paradigm, an evolved IP-based vehicular network is pivotal. An improved IP-based network architecture can enhance the computation data sharing and distributing. The existing mobility management solutions for VANET shall be extended or redesigned to support the distributed computation tasks, especially when vehicles move among different domains that may cause computation tasks broken. From the security point of view, it would be challenging to secure the distributed tasks and guarantee the data integrity of a returned computation result. Thus, it becomes a pressing issue to design and improve a feasible IP-based approach to satisfy the new vehicular MEC paradigm.

9.7. Vehicular Cloud Computing

To improve the road traffic efficiency in the future, data generated by connected vehicles can be sent to a vehicular cloud (VC) [147] in which a transportation administration entity analyzes the traffic status and searches for more efficient traffic control solutions. Such a kind of vehicular big data brings new

challenges to IP-based vehicular networks. One of the most important issues is that the privacy breakages pose a major threat to the VC. Since the packets transmitted to the VC include sensitive information, e.g., positions, sensor data, and even in-vehicle personnel conversations, a more secure and breakage-safe IP-based vehicular network data encryption approach is necessary. The Quantum communication technology [148] and blockchain [140] for security and privacy can be good candidates, but more research is needed to find a succinct solution.

10. Conclusion

This paper surveyed IP vehicular networking for ITS providing smart road services to drivers and pedestrians. First, it explained the background knowledge and the use cases of IP vehicular networking employing V2I, V2V, or V2X. Three important aspects for such IP vehicular networks were investigated and discussed along with security & privacy considerations as follows: (i) vehicular network architecture, (ii) vehicular address autoconfiguration, and (iii) vehicular mobility management. This paper also investigated the recent standardization activities related to IP vehicular networks. Then, this paper summarized and analyzed the existing research and standardization activities regarding IP vehicular networking. Finally, this paper presented several research challenges and issues for the future IP vehicular networks. Therefore, through the in-depth analysis of state-of-the-art research and standardization activities related to IP vehicular networking, this paper proposes the requirements, design principles, and research directions of IP-based vehicular networking for smart roads. It is believed that this paper opens a new door to researchers, designers, and implementers to work on IP vehicular networking technologies to facilitate human-driving, semi-autonomous, and autonomous vehicles in the future.

Declaration of Competing Interest

The authors declare that there is no conflict of interest.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government, the Ministry of Science and ICT (MSIT) (No. 2020R1F1A1048263). This work is also supported in part by the DGIST R&D Program of the MSIT under Grant 18-EE-01. This work was also supported in part by the MSIT, Korea, for the ITRC (Information Technology Research Center) support program (IITP-2020-2017-0-01633) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). This work was supported in part by Cisco Systems Research Grant 2019-199458 (3696) and by the Advanced Center for Electrical and Electronic Engineering, AC3E, Basal Project FB0008, ANID. EURECOM acknowledges the support of its industrial members, namely, BMW Group, IABG, Monaco Telecom, Orange, SAP and Symantec.

References

[1] Y. L. Morgan, Notes on dsrc & wave standards suite: Its architecture, design, and characteristics, IEEE Communications Surveys & Tutorials 12 (4) (2010) 504–518. doi:10.1109/SURV.2010.033010.00024.

[2] ETSI Technical Committee Intelligent Transport Systems, Intelligent Transport Systems (ITS); ITS-G5 Access layer Specification for Intelligent Transport Systems Operating in the 5 GHz Frequency Band, ETSI EN 302 663V1.3.1 (Jan. 2020).

[3] 3GPP, Architecture Enhancements for V2X Services, Technical Specification (TS) 23.285, 3rd Generation Partnership Project (3GPP), version 16.2.0 (Dec. 2019).

[4] 3GPP, Study on Enhancement of 3GPP Support for 5G V2X Services, Technical Report (TR) 22.886, 3rd Generation Partnership Project (3GPP), version 16.2.0 (Dec. 2018).

[5] 3GPP, Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services, Technical Specification (TS) 23.287, 3rd Generation Partnership Project (3GPP), version 16.2.0 (Mar. 2020).

[6] European Union, Commission Decision of 5 August 2008 on the Harmonised Use of Radio Spectrum in the 5875 - 5905 MHz Frequency Band for Safety-related Applications of Intelligent Transport Systems (ITS), EU 2008/671/EC (Aug. 2008).

[7] IEEE 1609 Working Group, IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture, IEEE Std 1609.0-2013 (Mar. 2014).

[8] IEEE 1609 Working Group, IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE Std 1609.2-2016 (Mar. 2016).

[9] IEEE 1609 Working Group, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, IEEE Std 1609.3-2016 (Apr. 2016).

[10] IEEE 1609 Working Group, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation, IEEE Std 1609.4-2016 (Mar. 2016).

[11] ISO/TC 204, Intelligent Transport Systems – Communications Access for Land Mobiles (CALM) – Architecture, ISO 21217:2014 (Apr. 2014).

[12] ETSI Technical Committee Intelligent Transport Systems, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality, ETSI EN 302 636-4-1 (Jan. 2020).

[13] ETSI Technical Committee Intelligent Transport Systems, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, ETSI EN 302 637-2V1.4.1 (Apr. 2019).

[14] ETSI Technical Committee Intelligent Transport Systems, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service, ETSI EN 302 637-3V1.3.1 (Apr. 2019).

[15] G. Qiao, S. Leng, K. Zhang, Y. He, Collaborative task offloading in vehicular edge multi-access networks, IEEE Communications Magazine 56 (8) (2018) 48–54. doi:10.1109/MCOM.2018.1701130.

[16] ISO/TC 204, Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking, ISO 21210:2012 (Jun. 2012).

[17] ETSI Technical Committee Intelligent Transport Systems, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols, ETSI EN 302 636-6-1 (May 2014).

[18] H. Khelifi, S. Luo, B. Nour, H. Moungla, Y. Faheem, R. Hussain, A. Ksentini, Named Data Networking in Vehicular Ad Hoc Networks: State-of-the-Art and Challenges, IEEE Communications Surveys & Tutorials 22 (1) (2020) 320–351.

[19] A. Qayyum, M. Usama, J. Qadir, A. Al-Fuqaha, Securing Future Autonomous & Connected Vehicles: Challenges Posed by Adversarial Machine Learning and The Way Forward, IEEE Communications Surveys & Tutorials (2020) 1–1.

[20] J. Wang, J. Liu, N. Kato, Networking and Communications in Autonomous Driving: A Survey, IEEE Communications Surveys & Tutorials 21 (2) (2019) 1243–1274.

[21] P. H. Rettore, G. Maia, L. A. Villas, A. A. F. Loureiro, Vehicular Data Space: The Data Point of View, IEEE Communications Surveys & Tutorials 21 (3) (2019) 2392–2418.
[22] H. Peng, Le Liang, X. Shen, G. Y. Li, Vehicular communications: A network layer perspective, IEEE Transactions on Vehicular Technology 68 (2) (2019) 1064–1078.
[23] I. Ali, A. Hassan, F. Li, Authentication and privacy schemes for vehicular ad hoc networks (vanets): A survey, Vehicular Communications 16 (2019) 45 – 61.
[24] J. E. Siegel, D. C. Erb, S. E. Sarma, A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas, IEEE Transactions on Intelligent Transportation Systems 19 (8) (2018) 2391–2406. doi:10.1109/TITS.2017.2749459.
[25] Z. MacHardy, A. Khan, K. Obana, S. Iwashina, V2X Access Technologies: Regulation, Research, and Remaining Challenges, IEEE Communications Surveys & Tutorials 20 (3) (2018) 1858–1877. doi:10.1109/COMST.2018.2808444.
[26] E. Ahmed, H. Gharavi, Cooperative vehicular networking: A survey, IEEE Transactions on Intelligent Transportation Systems 19 (3) (2018) 996–1014.
[27] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, Y. Zhou, Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions, IEEE Communications Surveys & Tutorials 17 (4) (2015) 2377–2396. doi:10.1109/COMST.2015.2440103.
[28] A. M. Vegni, V. Loscrí, A Survey on Vehicular Social Networks, IEEE Communications Surveys & Tutorials 17 (4) (2015) 2397–2419. doi:10.1109/COMST.2015.2453481.
[29] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, C. Liu, Routing in Internet of Vehicles: A Review, IEEE Transactions on Intelligent Transportation Systems 16 (5) (2015) 2339–2352. doi:10.1109/TITS.2015.2423667.
[30] M. Muhammad, G. A. Safdar, Survey on existing authentication issues for cellular-assisted v2x communication, Vehicular Communications 12 (2018) 50 – 65.
[31] A. Boualouache, S. Senouci, S. Moussaoui, A Survey on Pseudonym Changing Strategies for Vehicular Ad-Hoc Networks, IEEE Communications Surveys & Tutorials 20 (1) (2018) 770–790. doi:10.1109/COMST.2017.2771522.
[32] S. Thomson, T. Narten, T. Jinmei, IPv6 Stateless Address Autoconfiguration, RFC 4862 (Sep. 2007).
URL https://rfc-editor.org/rfc/rfc4862.txt
[33] F. Gont, A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC), RFC 7217 (Apr. 2014). doi:10.17487/RFC7217.
URL https://rfc-editor.org/rfc/rfc7217.txt
[34] F. Baker, B. E. Carpenter, First-Hop Router Selection by Hosts in a Multi-Prefix Network, RFC 8028 (Nov. 2016). doi:10.17487/RFC8028.
URL https://rfc-editor.org/rfc/rfc8028.txt
[35] T. Mrugalski, M. Siodelski, B. Volz, A. Yourtchenko, M. Richardson, S. Jiang, T. Lemon, T. Winters, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 8415 (Nov. 2018). doi:10.17487/RFC8415.
URL https://rfc-editor.org/rfc/rfc8415.txt
[36] T. Narten, R. P. Draves, S. Krishnan, Privacy Extensions for Stateless Address Autoconfiguration in IPv6, RFC 4941 (Sep. 2007).
URL https://rfc-editor.org/rfc/rfc4941.txt
[37] T. Aura, Cryptographically Generated Addresses (CGA), RFC 3972 (Mar. 2005).
URL https://rfc-editor.org/rfc/rfc3972.txt
[38] W. A. Simpson, D. T. Narten, E. Nordmark, H. Soliman, Neighbor Discovery for IP version 6 (IPv6), RFC 4861 (Sep. 2007).
URL https://rfc-editor.org/rfc/rfc4861.txt
[39] C. Perkins, D. Johnson, J. Arkko, Mobility Support in IPv6, RFC 6275 (Jul. 2011).
[40] L. Bellier, K. E. Malki, C. Castelluccia, H. Soliman, Hierarchical Mobile IPv6 (HMIPv6) Mobility Management, RFC 5380 (Oct. 2008).
URL https://rfc-editor.org/rfc/rfc5380.txt
[41] K. Chowdhury, K. Leung, B. Patil, V. Devarapalli, S. Gundavelli, Proxy Mobile IPv6, RFC 5213 (Aug. 2008).
URL https://rfc-editor.org/rfc/rfc5213.txt
[42] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, Network Mobility (NEMO) Basic Support Protocol, RFC 3963 (Jan. 2005).
[43] R. Wakikawa, Z. Zhu, L. Zhang, A Survey of Mobility Support in the Internet, RFC 6301 (Jul. 2011). doi:10.17487/RFC6301.
URL https://rfc-editor.org/rfc/rfc6301.txt
[44] S. Kent, K. Seo, Security Architecture for the Internet Protocol, RFC 4301 (Dec. 2005).
[45] S. Kent, IP Authentication Header, RFC 4302 (Dec. 2005).
[46] S. Kent, IP Encapsulating Security Payload (ESP), RFC 4303 (Dec. 2005).
[47] P. Hoffman, Cryptographic Suites for IPsec, RFC 4308 (Dec. 2005).
[48] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, Internet Key Exchange Protocol Version 2 (IKEv2), RFC 7296 (Oct. 2014).
[49] J. Kempf, J. Arkko, B. Zill, P. Nikander, SEcure Neighbor Discovery (SEND), RFC 3971 (Mar. 2005). doi:10.17487/RFC3971.
URL https://rfc-editor.org/rfc/rfc3971.txt
[50] J. Kempf, P. Nikander, E. Nordmark, IPv6 Neighbor Discovery (ND) Trust Models and Threats, RFC 3756 (May 2004).
[51] J. Jeong, H. Jeong, E. Lee, T. Oh, D. Du, SAINT: Self-Adaptive Interactive Navigation Tool for Cloud-Based Vehicular Traffic Optimization, IEEE Transactions on Vehicular Technology 65 (6) (2016) 4053–4067.
[52] Y. Shen, J. Lee, H. Jeong, J. Jeong, E. Lee, D. Du, SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization, IEEE Transactions on Intelligent Transportation Systems 19 (4) (2018) 1038–1053.
[53] S. van de Hoef, K. H. Johansson, D. V. Dimarogonas, Fuel-Efficient En Route Formation of Truck Platoons, IEEE Transactions on Intelligent Transportation Systems 19 (1) (2018) 102–112.
[54] E. Koukoumidis, L.-S. Peh, M. R. Martonosi, Signalguru: Leveraging mobile phones for collaborative traffic signal schedule advisory, in: Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services, MobiSys '11, ACM, New York, NY, USA, 2011, pp. 127–140.
[55] U.S. National Telecommunications and Information Administration (NTIA), First Responder Network Authority (FirstNet) (2020).
URL https://www.firstnet.gov/
[56] P. Tallapragada, J. Cortés, Hierarchical-Distributed Optimized Coordination of Intersection Traffic, IEEE Transactions on Intelligent Transportation Systems (2019) 1–14.
[57] Y. Zhang, C. G. Cassandras, Joint Time and Energy-Optimal Control of Connected Automated Vehicles at Signal-Free Intersections with Speed-Dependent Safety Guarantees, in: 2019 IEEE 58th Conference on Decision and Control (CDC), 2019, pp. 329–334.
[58] Y. Shen, J. Jeong, T. Oh, S. H. Son, CASD: A Framework of Context-Awareness Safety Driving in Vehicular Networks, in: 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2016, pp. 252–257.
[59] California Partners for Advanced Transportation Technology (PATH), Cooperative Adaptive Cruise Control, (Accessed: 08.20.2020) (2020).
URL https://path.berkeley.edu/research/connected-and-automated-vehicles/cooperative-adaptive-cruise-control
[60] California Partners for Advanced Transportation Technology (PATH): Automated Truck Platooning, (Accessed: 08.20.2020) (2020).
URL https://path.berkeley.edu/research/connected-and-automated-vehicles/truck-platooning
[61] K. Serizawa, M. Mikami, K. Moto, H. Yoshino, Field Trial Activities on 5G NR V2V Direct Communication Towards Application to Truck Platooning, in: 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 2019, pp. 1–5.
[62] I. Llatser, T. Michalke, M. Dolgov, F. Wildschütte, H. Fuchs, Cooperative Automated Driving Use Cases for 5G V2X Communication, in: 2019 IEEE 2nd 5G World Forum (5GWF), 2019, pp. 120–125.
[63] N. Lyamin, A. Vinel, M. Jonsson, B. Bellalta, Cooperative Awareness in VANETs: On ETSI EN 302 637-2 Performance, IEEE Transactions on Vehicular Technology 67 (1) (2018) 17–28.
[64] S. Cespedes, N. Lu, X. Shen, VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks, IEEE Transactions on Intelligent Transportation Systems 14 (1) (2013) 82–97.
[65] E. Baccelli, T. Clausen, R. Wakikawa, IPv6 Operation for WAVE - Wireless Access in Vehicular Environments, in: Proceedings of IEEE Vehicular Networking Conference, IEEE, 2010, pp. 160–165.
[66] I. Jemaa, O. Shagdar, T. Ernst, A Framework for IP and non-IP Multicast

Services for Vehicular Networks, in: Proceedings of the Third International Conference on the Network of the Future, 2012, pp. 1–6.
[67] A. Petrescu, M. Boc, C. Ibars, Joint IP Networking and Radio Architecture for Vehicular Networks, in: Proceedings of the 11th International Conference on ITS Telecommunications, 2011, pp. 230–236.
[68] M. Bechler, W. Franz, L. Wolf, Mobile Internet Access in FleetNet, in: Proceedings of the 13th Fachtagung Kommunikation in verteilten Systemen, 2001.
[69] P. J. Fernández, J. Santa, F. Bernal, A. F. Skarmeta, Securing Vehicular IPv6 Communications, IEEE Transactions on Dependable and Secure Computing 13 (1) (2016) 46–58.
[70] T. Hwang, J. Jeong, SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks, Springer Lecture Notes in Computer Science (LNCS) 9502 (Dec. 2015).
[71] G. Kar, S. Jain, M. Gruteser, F. Bai, R. Govindan, Real-time traffic estimation at vehicular edge nodes, in: Proceedings of the Second ACM/IEEE Symposium on Edge Computing, SEC '17, ACM, New York, NY, USA, 2017, pp. 3:1–3:13.
[72] E. Baccelli, M. Townsley, IP Addressing Model in Ad Hoc Networks, RFC 5889 (Sep. 2010).
[73] E. Guttman, Service Location Protocol Modifications for IPv6, RFC 3111 (May 2001).
URL https://rfc-editor.org/rfc/rfc3111.txt
[74] E. Guttman, C. Perkins, J. Veizades, M. Day, Service Location Protocol, Version 2, RFC 2608 (Jun. 1999).
URL https://rfc-editor.org/rfc/rfc2608.txt
[75] E. Guttman, Vendor Extensions for Service Location Protocol, Version 2, RFC 3224 (Jan. 2002).
URL https://rfc-editor.org/rfc/rfc3224.txt
[76] K. Fall, A Delay-tolerant Network Architecture for Challenged Internets, in: 2003 Proceedings ACM SIGCOMM, ACM, New York, NY, USA, 2003, pp. 27–34.
[77] M. Fazio, C. Palazzi, S. Das, M. Gerla, Automatic IP Address Configuration in VANETs, in: Proceedings of ACM International Workshop on Vehicular Inter-networking, ACM, New York, NY, USA, 2016.
[78] T. Kato, K. Kadowaki, T. Koita, K. Sato, Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network, in: Proceedings of Asia-Pacific Services Computing Conference, IEEE, 2008.
[79] R. Baldessari, C. Bernardos, M. Calderon, GeoSAC - Scalable Address Autoconfiguration for VANET Using Geographic Networking Concepts, in: Proceedings of IEEE International Sycmposium on Personal, Indoor and Mobile Radio Communications, IEEE, 2008.
[80] M. Wetterwald, F. Hrizi, P. Cataldi, Cross-layer Identities Management in ITS Stations, in: Proceedings of the 10th International Conference on ITS Telecommunications, IEEE, 2010.
[81] R. Droms, Dynamic Host Configuration Protocol, RFC 2131 (Mar. 1997).
[82] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315 (Jul. 2003).
[83] Y.-S. Chen, C.-S. Hsu, W.-H. Yi, An IP Passing Protocol for Vehicular Ad Hoc Networks with Network Fragmentation, Comput. Math. Appl. 63 (2) (2012) 407–426.
[84] I. Soto, C. J. Bernardos, M. Calderon, A. Banchs, A. Azcorra, Nemo-enabled localized mobility support for internet access in automotive scenarios, IEEE Communications Magazine 47 (5) (2009) 152–159.
[85] T. Nguyen, C. Bonnet, A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users, in: Proceedings of IEEE International Conference on Communications, 2015.
[86] T. Nguyen, C. Bonnet, A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility, in: Proceedings of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2015.
[87] Y.-S. Chen, C.-S. Hsu, C.-H. Cheng, Network Mobility Protocol for Vehicular Ad Hoc Networks, International Journal of Communication Systems 27 (11) (2014) 3042–3063.
[88] J. Lee, T. Ernst, N. Chilamkurti, Performance Analysis of PMIPv6-Based NEtwork MObility for Intelligent Transportation Systems, IEEE Transactions on Vehicular Technology 61 (1) (2012) 74–85.
[89] Y. Peng, J. Chang, A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks and Fixed IP Networks, Springer Mobile Networks and Applications (2010) –.
[90] T. Nguyen, C. Bonnet, J. Harri, SDN-based Distributed Mobility Management for 5G Networks, in: Proceedings of IEEE Wireless Communications and Networking Conference, IEEE, 2016.
[91] S. Cespedes, X. Shen, C. Lazo, IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions, IEEE Communications Magazine 49 (5) (2011) 187–194.
[92] P. J. Fernández, J. Santa, F. Pereñíguez, A. F. Skarmeta, Towards Seamless Inter-Technology Handovers in Vehicular IPv6 Communications, Computer Standards & Interfaces 52 (2017) 85 – 96.
[93] J. Song, S. Han, Mobile Node Authentication Protocol for Proxy Mobile, in: International Conference on Computer and Information Technology, Vol. 6, 2009, pp. 10–19.
[94] T. Arnold, W. Lloyd, J. Zhao, G. Cao, IP Address Passing for VANETs, in: 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom), 2008, pp. 70–79. doi:10.1109/PERCOM.2008.80.
[95] S. Keshav, The Network Simulator - ns-2, (Accessed: 08.20.2020) (2020).
URL https://www.isi.edu/nsnam/ns/
[96] NS-3 Consortium, The Network Simulator - ns-3, (Accessed: 10.22.2020) (2020).
URL https://www.nsnam.org/
[97] A. Chan, D. Liu, P. Seite, H. Yokota, J. Korhonen, Requirements for Distributed Mobility Management, RFC 7333 (Aug. 2014).
URL https://rfc-editor.org/rfc/rfc7333.txt
[98] R. Koodli, Fast Handovers for Mobile IPv6, RFC 4068 (Jul. 2005). doi:10.17487/RFC4068.
URL https://rfc-editor.org/rfc/rfc4068.txt
[99] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, F. Xia, Fast Handovers for Proxy Mobile IPv6, RFC 5949 (Sep. 2010).
[100] Simulation of Urban MObility (SUMO) (May 2020).
URL https://sumo.dlr.de/docs/index.html
[101] Open Networking Foundation (ONF), OpenFlow Switch Specification - Version 1.5.1 (Mar. 2015).
URL https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf
[102] IEEE, IEEE Standard for Local and Metropolitan Area networks–Part 21: Media Independent Services Framework, IEEE Std 802.21-2017 (2017) 1–314.
[103] IEEE, IEEE Standard for Local and Metropolitan Area Networks–Part 21.1: Media Independent Services, IEEE Std 802.21.1-2017 (2017) 1–211.
[104] A. Stamou, N. Dimitriou, K. Kontovasilis, S. Papavassiliou, Autonomic Handover Management for Heterogeneous Networks in a Future Internet Context: A Survey, IEEE Communications Surveys Tutorials 21 (4) (2019) 3274–3297.
[105] IEEE 802.11 Working Group, IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) (2016) 1–3534.
[106] N. Benamar, J. Härri, J.-H. Lee, T. Ernst, Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11, RFC 8691 (Dec. 2019). doi:10.17487/RFC8691.
URL https://rfc-editor.org/rfc/rfc8691.txt
[107] J. P. Jeong, IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases, Internet-Draft draft-ietf-ipwave-vehicular-networking-19, Internet Engineering Task Force, Work in Progress (Jul. 2020).
URL https://datatracker.ietf.org/doc/html/draft-ietf-ipwave-vehicular-networking-19
[108] H. Zhou, H. Zhang, An Authentication Protocol for Proxy Mobile IPv6, in: 2008 The 4th International Conference on Mobile Ad-hoc and Sensor Networks, 2008, pp. 129–136.
[109] J. Lee, J. Lee, T. Chung, Ticket-Based Authentication Mechanism for Proxy Mobile IPv6 Environment, in: 2008 Third International Conference on Systems and Networks Communications, 2008, pp. 304–309.
[110] M. I. Sanchez, A. de la Oliva, V. Mancuso, Experimental evaluation of an sdn-based distributed mobility management solution, in: Proceedings

of the Workshop on Mobility in the Evolving Internet Architecture, MobiArch '16, ACM, New York, NY, USA, 2016, pp. 31–36.
[111] IEEE 802.11 Working Group, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Wireless Access in Vehicular Environments, IEEE Std 802.11p-2010 (Jun. 2010).
[112] G. Naik, B. Choudhury, J. Park, Ieee 802.11bd 5g nr v2x: Evolution of radio access technologies for v2x communications, IEEE Access 7 (2019) 70169–70184. doi:10.1109/ACCESS.2019.2919489.
[113] IETF IPWAVE Working Group, IP Wireless Access in Vehicular Environments (ipwave) (Mar. 2019).
URL https://datatracker.ietf.org/wg/ipwave/documents/
[114] IEEE, Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID), Tech. rep., The IEEE Standards Association (Aug. 2017).
[115] R. Hinden, S. Deering, IP Version 6 Addressing Architecture, RFC 4291 (Feb. 2006).
[116] D. Eastlake, J. Schiller, S. Crocker, Randomness Requirements for Security, RFC 4086 (Jun. 2005).
[117] F. Gont, A. Cooper, D. Thaler, W. Liu, Recommendation on Stable IPv6 Interface Identifiers, RFC 8064 (Feb. 2017).
[118] J. Soininen, J. Korhonen, Survey of IPv6 Support in 3GPP Specifications and Implementations, IEEE Communications Surveys & Tutorials 17 (3) (2015) 1634–1648.
[119] 3GPP, Proximity-based Services (ProSe); Stage 2, Technical Specification (TS) 23.303, 3rd Generation Partnership Project (3GPP), version 15.1.0 (Jun. 2018).
[120] 3GPP, System Architecture for the 5G System (5GS); Stage 2, Technical Specification (TS) 23.501, 3rd Generation Partnership Project (3GPP), version 16.3.0 (Dec. 2019).
[121] J. P. Jeong, Y. C. Shen, Z. Xiang, S. Cespedes, Vehicular Neighbor Discovery for IP-Based Vehicular Networks, Internet-Draft draft-jeong-ipwave-vehicular-neighbor-discovery, Internet Engineering Task Force, Work in Progress (May 2020).
[122] J. P. Jeong, Y. C. Shen, Z. Xiang, Vehicular Mobility Management for IP-Based Vehicular Networks, Internet-Draft draft-jeong-ipwave-vehicular-mobility-management-03, Internet Engineering Task Force, Work in Progress (May 2020).
[123] K.-L. Yap, Y.-W. Chong, W. Liu, Enhanced handover mechanism using mobility prediction in wireless networks, PLOS ONE 15 (1) (2020) 1–31.
[124] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, V. Sadekar, Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks, IEEE Wireless Communications 14 (6) (2007) 84–94.
[125] D. Camara, C. Bonnet, N. Nikaein, M. Wetterwald, Multicast and virtual road side units for multi technology alert messages dissemination, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 947–952.
[126] C. E. Perkins, M. McBride, D. Stanley, W. A. Kumari, J.-C. Zuniga, Multicast Considerations over IEEE 802 Wireless Media, Internet-Draft draft-ietf-mboned-ieee802-mcast-problems-11, Internet Engineering Task Force, Work in Progress (Dec. 2019).
[127] S. Cheshire, M. Krochmal, DNS-Based Service Discovery, RFC 6763 (Feb. 2013).
URL https://rfc-editor.org/rfc/rfc6763.txt
[128] S. Cheshire, M. Krochmal, Multicast DNS, RFC 6762 (Feb. 2013).
URL https://rfc-editor.org/rfc/rfc6762.txt
[129] N. Finn, Introduction to Time-Sensitive Networking, IEEE Communications Standards Magazine 2 (2) (2018) 22–28.
[130] IEEE, IEEE Standard for Local and Metropolitan Area Network–Bridges and Bridged Networks, IEEE Std 802.1Q-2018 (Revision of IEEE Std 802.1Q-2014) (2018) 1–1993.
[131] S. Samii, H. Zinner, Level 5 by Layer 2: Time-Sensitive Networking for Autonomous Vehicles, IEEE Communications Standards Magazine 2 (2) (2018) 62–68.
[132] N. Finn, P. Thubert, Deterministic Networking Problem Statement, RFC 8557 (May 2019).
[133] E. Grossman, Deterministic Networking Use Cases, RFC 8578 (May 2019).
[134] N. Finn, P. Thubert, B. Varga, J. Farkas, Deterministic Networking Architecture, RFC 8655 (Oct. 2019).
[135] K. Sun, Y. Kim, Considerations for ID/Location Separation Protocols in IP-based Vehicular Networks, Internet-Draft draft-kjsun-ipwave-id-loc-separation-02, Internet Engineering Task Force, Work in Progress (Mar. 2020).
URL https://datatracker.ietf.org/doc/html/draft-kjsun-ipwave-id-loc-separation-02
[136] D. Farinacci, V. Fuller, D. Meyer, D. Lewis, The Locator/ID Separation Protocol (LISP), RFC 6830 (Jan. 2013). doi:10.17487/RFC6830.
URL https://rfc-editor.org/rfc/rfc6830.txt
[137] R. Atkinson, S. Bhatti, Identifier-Locator Network Protocol (ILNP) Architectural Description, RFC 6740 (Nov. 2012). doi:10.17487/RFC6740.
URL https://rfc-editor.org/rfc/rfc6740.txt
[138] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280 (May 2008).
[139] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446 (Aug. 2018).
[140] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, IEEE Communications Magazine (2009) 119–125.
URL https://bitcoin.org/bitcoin.pdf
[141] A. Dorri, M. Steger, S. S. Kanhere, R. Jurdak, BlockChain: A Distributed Solution to Automotive Security and Privacy, IEEE Communications Magazine 55 (12) (2017) 119–125.
[142] A. Dorri, S. S. Kanhere, R. Jurdak, Towards an Optimized BlockChain for IoT, in: Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, 2017, pp. 173–178.
[143] S. Zhou, P. P. Netalkar, Y. Chang, Y. Xu, J. Chao, The mec-based architecture design for low-latency and fast hand-off vehicular networking, in: 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), 2018, pp. 1–7.
[144] Y. Wang, P. Lang, D. Tian, J. Zhou, X. Duan, Y. Cao, D. Zhao, A Game-Based Computation Offloading Method in Vehicular Multiaccess Edge Computing Networks, IEEE Internet of Things Journal 7 (6) (2020) 4987–4996.
[145] Z. Xiao, X. Dai, H. Jiang, D. Wang, H. Chen, L. Yang, F. Zeng, Vehicular Task Offloading via Heat-Aware MEC Cooperation Using Game-Theoretic Method, IEEE Internet of Things Journal 7 (3) (2020) 2038–2052.
[146] P. Dai, K. Hu, X. Wu, H. Xing, F. Teng, Z. Yu, A Probabilistic Approach for Cooperative Computation Offloading in MEC-Assisted Vehicular Networks, IEEE Transactions on Intelligent Transportation Systems (2020) 1–13doi:10.1109/TITS.2020.3017172.
[147] S. Olariu, A Survey of Vehicular Cloud Research: Trends, Applications and Challenges, IEEE Transactions on Intelligent Transportation Systems 21 (6) (2020) 2648–2663.
[148] N. Gisin, R. T. Thew, Quantum Communication Technology, Electronics Letters 46 (14) (2010) 965–967.