Internet Engineering Task Force (IETF)
Request for Comments: 9365
Category: Informational
ISSN: 2070-1721

J. Jeong, Ed.
Sungkyunkwan University

March 2023

IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases

Abstract

This document discusses the problem statement and use cases of IPv6-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document explains use cases using V2V, V2I, and V2X networking. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, mobility management, as well as security and privacy).

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9365.

Table of Contents

1. Introduction

Vehicular networking studies have mainly focused on improving road safety and efficiency and also enabling entertainment in vehicular networks. To proliferate the use cases of vehicular networks, several governments and private organizations have committed to allocating dedicated spectrum for vehicular communications. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC] in the Intelligent Transportation Systems (ITS) with the frequency band of 5.850 - 5.925 GHz (i.e., 5.9 GHz band). In November 2020, the FCC adjusted the lower 45 MHz (i.e., 5.850 - 5.895 GHz) of the 5.9 GHz band for unlicensed use instead of DSRC-dedicated use [FCC-ITS-Modification]. DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. The European Union (EU) allocated radio spectrum for safety-related and non-safety-related applications of ITS with the frequency band of 5.875 - 5.905 GHz, as part of the Commission Decision 2008/671/EC [EU-2008-671-EC]. Most other countries and regions in the world have adopted the 5.9 GHz band for vehicular networks, though different countries use different ways to divide the band into channels.

For direct inter-vehicular wireless connectivity, IEEE has amended standard 802.11 (commonly known as Wi-Fi) to enable safe driving

services based on DSRC for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC layers of the DSRC, while IEEE Std 1609.2 [WAVE-1609.2] covers security aspects, IEEE Std 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE Std 1609.4 [WAVE-1609.4] specifies the multichannel operation. IEEE 802.11p was first a separate amendment but was later rolled into the base 802.11 standard (IEEE Std 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) in 2012 [IEEE-802.11-OCB].

3GPP has standardized Cellular Vehicle-to-Everything (C-V2X) communications to support V2X in LTE mobile networks (called LTE V2X) and V2X in 5G mobile networks (called 5G V2X) [TS-23.285-3GPP] [TR-22.886-3GPP] [TS-23.287-3GPP]. With C-V2X, vehicles can directly communicate with each other without relay nodes (e.g., eNodeB in LTE and gNodeB in 5G).

Along with these WAVE standards and C-V2X standards, regardless of a wireless access technology under the IP stack of a vehicle, vehicular networks can operate IP mobility with IPv6 [RFC8200], that is, Mobile IPv6 protocols, e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy Mobile IPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Network Mobility (NEMO) [RFC3963], and the Locator/ID Separation Protocol (LISP) [RFC9300]. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6] [ISO-ITS-IPv6-AMD1].

This document describes use cases and a problem statement about IPv6-based vehicular networking for ITS, which is named IPv6 Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, mobility management, as well as security and privacy) so that those protocols can be tailored to IPv6-based vehicular networking. Thus, this document is intended to motivate development of key protocols for IPWAVE.

2. Terminology

This document uses the terminology described in [RFC8691]. In addition, the following terms are defined below:

Context-Awareness: A vehicle can be aware of spatial-temporal mobility information (e.g., position, speed, direction, and acceleration/deceleration) of surrounding vehicles for both safety and non-safety uses through sensing or communication [CASD].

Distributed Mobility Management (DMM): See [RFC7333] [RFC7429].

Edge Computing Device (ECD): This is a computing device (or server) at the edge of the network for vehicles and vulnerable road users. It co-locates with or connects to an IP Roadside Unit (IP-RSU), which has a powerful computing capability for different kinds of computing tasks, such as image processing and classification.

Edge Network (EN): This is an access network that has an IP-RSU for wireless communication with other vehicles having an IP On-Board Unit (IP-OBU) and wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and Mobility Anchors (MAs)). It may use a Global Navigation Satellite System (GNSS) such as Global Positioning System (GPS) with a GNSS receiver for its position recognition and the localization service for the sake of vehicles.

Evolved Node B (eNodeB): This is a base station entity that supports the Long Term Evolution (LTE) air interface.

Internet Protocol On-Board Unit (IP-OBU): An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, electric bike, motorcycle, or similar), which has a basic processing ability and can be driven by a low-power CPU (e.g., ARM). It has at least one IP interface that runs in IEEE 802.11-OCB and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP] [TR-22.886-3GPP] [TS-23.287-3GPP]. It can play the role of a router connecting multiple computers (or in-vehicle devices) inside a vehicle. See the definition of the term "IP-OBU" in [RFC8691].

IP Roadside Unit (IP-RSU): An IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode [IEEE-802.11-OCB]. An IP-RSU communicates with the IP-OBU over an 802.11 wireless link operating in OCB mode. One of its IP-enabled interfaces is connected to the wired network for wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and MAs). Also, it may have another IP-enabled wireless interface running in 3GPP C-V2X in addition to the IP-RSU defined in [RFC8691]. An IP-RSU is similar to an Access Network Router (ANR), defined in [RFC3753], and a Wireless Termination Point (WTP), defined in [RFC5415]. See the definition of the term "IP-RSU" in [RFC8691].

Light Detection and Ranging (LiDAR): This is a method for measuring a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.

Mobility Anchor (MA): This is a node that maintains IPv6 addresses and mobility information of vehicles in a road network to support their IPv6 address autoconfiguration and mobility management with a binding table. An MA has end-to-end (E2E) connections (e.g., tunnels) with IP-RSUs under its control for the IPv6 address autoconfiguration and mobility management of the vehicles. This MA is similar to a Local Mobility Anchor (LMA) in PMIPv6 [RFC5213] for network-based mobility management.

Next Generation Node B (gNodeB): This is a base station entity that supports the 5G New Radio (NR) air interface.

Outside the Context of a BSS (OCB): This is a mode of operation in which a station (STA) is not a member of a Basic Service Set (BSS)

and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality [IEEE-802.11-OCB].

802.11-OCB: This refers to the mode specified in IEEE Std 802.11-2016 [IEEE-802.11-OCB] when the MIB attribute dot11OCBActivated is 'true'.

Platooning: Moving vehicles can be grouped together to reduce air resistance for energy efficiency and reduce the number of drivers such that only the lead vehicle has a driver, and the other vehicles are autonomous vehicles without a driver and closely follow the lead vehicle [Truck-Platooning].

Traffic Control Center (TCC): This is a system that manages road infrastructure nodes (e.g., IP-RSUs, MAs, traffic signals, and loop detectors) and also maintains vehicular traffic statistics (e.g., average vehicle speed and vehicle inter-arrival time per road segment) and vehicle information (e.g., a vehicle's identifier, position, direction, speed, and trajectory as a navigation path). TCC is part of a Vehicular Cloud for vehicular networks.

Urban Air Mobility (UAM): This refers to using lower-altitude aircraft to transport passengers or cargo in urban and suburban areas. The carriers used for UAM can be manned or unmanned vehicles, which can include helicopters, electric vertical take-off and landing (eVTOL) aircraft, and unmanned aerial vehicles (UAVs).

Vehicle: This is a node that has an IP-OBU for wireless communication with other vehicles and IP-RSUs. It has a GNSS radio navigation receiver for efficient navigation. Any device having an IP-OBU and a GNSS receiver (e.g., smartphone and tablet PC) can be regarded as a vehicle in this document.

Vehicular Ad Hoc Network (VANET): This is a network that consists of vehicles interconnected by wireless communication. Two vehicles in a VANET can communicate with each other using other vehicles as relays even where they are out of one-hop wireless communication range.

Vehicular Cloud: This is a cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network forwarding elements (e.g., switch and router).

Vehicle to Device (V2D): This is the wireless communication between a vehicle and a device (e.g., smartphone and IoT (Internet of Things) device).

Vehicle to Pedestrian (V2P): This is the wireless communication between a vehicle and a pedestrian's device (e.g., smartphone and IoT device).

Vehicle to Infrastructure to Vehicle (V2I2V): This is the wireless communication between a vehicle and another vehicle via an infrastructure node (e.g., IP-RSU).

Vehicle to Infrastructure to Everything (V2I2X): This is the wireless communication between a vehicle and another entity (e.g., vehicle, smartphone, and IoT device) via an infrastructure node (e.g., IP-RSU).

Vehicle to Everything (V2X): This is the wireless communication between a vehicle and any entity (e.g., vehicle, infrastructure node, smartphone, and IoT device), including V2V, V2I, V2D, and V2P.

Vehicular Mobility Management (VMM): This is IPv6-based mobility management for vehicular networks.

Vehicular Neighbor Discovery (VND): This is an IPv6 ND (Neighbor Discovery) extension for vehicular networks.

Vehicular Security and Privacy (VSP): This is IPv6-based security and privacy for vehicular networks.

Wireless Access in Vehicular Environments (WAVE): See [WAVE-1609.0].

3. Use Cases

This section explains use cases of V2V, V2I, and V2X networking. The use cases of the V2X networking exclude the ones of the V2V and V2I networking but include Vehicle-to-Pedestrian (V2P) and Vehicle-to-Device (V2D).

IP is widely used among popular end-user devices (e.g., smartphone and tablet) in the Internet. Applications (e.g., navigator application) for those devices can be extended such that the V2V use cases in this section can work with IPv6 as a network layer protocol and IEEE 802.11-OCB as a link-layer protocol. In addition, IPv6 security needs to be extended to support those V2V use cases in a safe, secure, privacy-preserving way.

The use cases presented in this section serve as the description and motivation for the need to augment IPv6 and its protocols to facilitate "Vehicular IPv6". Section 5 summarizes the overall problem statement and IPv6 requirements. Note that the adjective "Vehicular" in this document is used to represent extensions of existing protocols, such as IPv6 Neighbor Discovery, IPv6 Mobility Management (e.g., PMIPv6 [RFC5213] and DMM [RFC7429]), and IPv6 Security and Privacy Mechanisms rather than new "vehicular-specific" functions.

3.1. V2V

The use cases of V2V networking discussed in this section include:

* Context-aware navigation for driving safely and avoiding collisions

* Collision avoidance service of end systems of Urban Air Mobility (UAM)

* Cooperative adaptive cruise control on a roadway

* Platooning on a highway

* Cooperative environment sensing

The above use cases are examples for using V2V networking, which can be extended to other terrestrial vehicles, river/sea ships, railed vehicles, or UAM end systems.

A Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely as a context-aware navigation service [CNP] by alerting them to dangerous obstacles and situations. That is, a CASD navigator displays obstacles or neighboring vehicles relevant to possible collisions in real time through V2V networking. CASD provides vehicles with a class-based automatic safety action plan that considers three situations, namely, the Line-of-Sight unsafe, Non-Line-of-Sight unsafe, and safe situations. This action plan can be put into action among multiple vehicles using V2V networking.

A service for collision avoidance of in-air UAM end systems is one possible use case in air vehicular environments [UAM-ITS]. This use case is similar to that of a context-aware navigator for terrestrial vehicles. Through V2V coordination, those UAM end systems (e.g., drones) can avoid a dangerous situation (e.g., collision) in three-dimensional space rather than two-dimensional space for terrestrial vehicles. Also, a UAM end system (e.g., flying car), when only a few hundred meters off the ground, can communicate with terrestrial vehicles with wireless communication technologies (e.g., DSRC, LTE, and C-V2X). Thus, V2V means any vehicle to any vehicle, whether the vehicles are ground level or not.

Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps individual vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles on an urban roadway or a highway. Thus, CACC can help adjacent vehicles to efficiently adjust their speed in an interactive way through V2V networking in order to avoid a collision.

Platooning [Truck-Platooning] allows a series (or group) of vehicles (e.g., trucks) to follow each other very closely. Vehicles can use V2V communication in addition to forward sensors in order to maintain constant clearance between two consecutive vehicles at very short gaps (from 3 to 10 meters). Platooning can maximize the throughput of vehicular traffic on a highway and reduce the gas consumption because the lead vehicle can help the following vehicles experience less air resistance.

Cooperative-environment-sensing use cases suggest that vehicles can share environmental information (e.g., air pollution, hazards, obstacles, slippery areas by snow or rain, road accidents, traffic congestion, and driving behaviors of neighboring vehicles) from various vehicle-mounted sensors, such as radars, LiDAR systems, and cameras, with other vehicles and pedestrians. [Automotive-Sensing]

introduces millimeter-wave vehicular communication for massive automotive sensing. A lot of data can be generated by those sensors, and these data typically need to be routed to different destinations. In addition, from the perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver-operated vehicles. Through cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment. Vehicles can also share their intended maneuvering information (e.g., lane change, speed change, ramp in-and-out, cut-in, and abrupt braking) with neighboring vehicles. Thus, this information sharing can help the vehicles behave as more efficient traffic flows and minimize unnecessary acceleration and deceleration to achieve the best ride comfort.

To support applications of these V2V use cases, the required functions of IPv6 include (a) IPv6-based packet exchange in both control and data planes and (b) secure, safe communication between two vehicles. For the support of V2V under multiple radio technologies (e.g., DSRC and 5G V2X), refer to Appendix A.

3.2. V2I

The use cases of V2I networking discussed in this section include:

* Navigation service

* Energy-efficient speed recommendation service

* Accident notification service

* Electric Vehicle (EV) charging service

* UAM navigation service with efficient battery charging

A navigation service (for example, the Self-Adaptive Interactive Navigation Tool [SAINT]) that uses V2I networking interacts with a TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles along appropriate navigation paths in real time. The enhanced version of SAINT [SAINTplus] can give fast-moving paths to emergency vehicles (e.g., ambulance and fire engine) to let them reach an accident spot while redirecting other vehicles near the accident spot into efficient detour paths.

Either a TCC or an ECD can recommend an energy-efficient speed to a vehicle that depends on its traffic environment and traffic signal scheduling [SignalGuru]. For example, when a vehicle approaches an intersection area and a red traffic light for the vehicle becomes turned on, it needs to reduce its speed to save fuel consumption. In this case, either a TCC or an ECD, which has the up-to-date trajectory of the vehicle and the traffic light schedule, can notify the vehicle of an appropriate speed for fuel efficiency. [Fuel-Efficient] covers fuel-efficient route and speed plans for platooned trucks.

The emergency communication between vehicles in an accident (or

emergency-response vehicles) and a TCC can be performed via either IP-RSUs or 4G-LTE or 5G networks. The First Responder Network Authority [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, e.g., emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to the FirstNet's network core. The current RAN is mainly constructed using 4G-LTE for communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Report], but it is expected that DSRC-based vehicular networks [DSRC] will be available for V2I and V2V in the near future. An equivalent project in Europe is called Public Safety Communications Europe [PSCE], which is developing a network for emergency communications.

An EV charging service with V2I can facilitate the efficient battery charging of EVs. In the case where an EV charging station is connected to an IP-RSU, an EV can be guided toward the deck of the EV charging station or be notified that the charging station is out of service through a battery charging server connected to the IP-RSU. In addition to this EV charging service, other value-added services (e.g., firmware/software update over-the-air and media streaming) can be provided to an EV while it is charging its battery at the EV charging station. For a UAM navigation service, an efficient battery charging plan can improve the battery charging schedule of UAM end systems (e.g., drones) for long-distance flying [CBDN]. For this battery charging schedule, a UAM end system can communicate with a cloud server via an infrastructure node (e.g., IP-RSU). This cloud server can coordinate the battery charging schedules of multiple UAM end systems for their efficient navigation path, considering flight time from their current position to a battery charging station, waiting time in a waiting queue at the station, and battery charging time at the station.

In some scenarios, such as vehicles moving on highways or staying in parking lots, a V2V2I network is necessary for vehicles to access the Internet since some vehicles may not be covered by an IP-RSU. For those vehicles, a few relay vehicles can help to build the Internet access. For the nested NEMO described in [RFC4888], hosts inside a vehicle shown in Figure 3 for the case of V2V2I may have the same issue in the nested NEMO scenario.

To better support these use cases, the existing IPv6 protocol must be augmented either through protocol changes or by including a new adaptation layer in the architecture that efficiently maps IPv6 to a diversity of link-layer technologies. Augmentation is necessary to support wireless multihop V2I communications on a highway where RSUs are sparsely deployed so that a vehicle can reach the wireless coverage of an IP-RSU through the multihop data forwarding of intermediate vehicles as packet forwarders. Thus, IPv6 needs to be extended for multihop V2I communications.

To support applications of these V2I use cases, the required functions of IPv6 include IPv6 communication enablement with neighborhood discovery and IPv6 address management; reachability with adapted network models and routing methods; transport-layer session

continuity; and secure, safe communication between a vehicle and an infrastructure node (e.g., IP-RSU) in the vehicular network.

3.3. V2X

The use case of V2X networking discussed in this section is for a protection service for a vulnerable road user (VRU), e.g., a pedestrian or cyclist. Note that the application area of this use case is currently limited to a specific environment, such as construction sites, plants, and factories, since not every VRU in a public area is equipped with a smart device (e.g., not every child on a road has a smartphone, smart watch, or tablet).

A VRU protection service, such as the Safety-Aware Navigation Application [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., Wi-Fi, DSRC, 4G/5G V2X, and Bluetooth Low Energy (BLE)) with an IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU. An ECD behind the IP-RSU can collect the mobility information from vehicles and pedestrians, and then compute wireless communication scheduling for the sake of them. This scheduling can save the battery of each pedestrian's smartphone by allowing it to work in sleeping mode before communication with vehicles, considering their mobility. The location information of a VRU from a smart device (e.g., smartphone) is multicasted only to the nearby vehicles. The true identifiers of a VRU's smart device shall be protected, and only the type of the VRU, such as pedestrian, cyclist, or scooter, is disclosed to the nearby vehicles.

For Vehicle-to-Pedestrian (V2P), a vehicle can directly communicate with a pedestrian's smartphone by V2X without IP-RSU relaying. Light-weight mobile nodes, such as bicycles, may also communicate directly with a vehicle for collision avoidance using V2V. Note that it is true that either a pedestrian or a cyclist may have a higher risk of being hit by a vehicle if they are not with a smartphone in the current setting. For this case, other human-sensing technologies (e.g., moving-object detection in images and wireless signal-based human movement detection [LIFS] [DFC]) can be used to provide motion information to vehicles. A vehicle by V2V2I networking can obtain a VRU's motion information via an IP-RSU that either employs or connects to a human-sensing technology.

The existing IPv6 protocol must be augmented through protocol changes in order to support wireless multihop V2X or V2I2X communications in an urban road network where RSUs are deployed at intersections so that a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an IP-RSU through the multihop data forwarding of intermediate vehicles (or pedestrians' smartphones) as packet forwarders. Thus, IPv6 needs to be extended for multihop V2X or V2I2X communications.

To support applications of these V2X use cases, the required functions of IPv6 include IPv6-based packet exchange; transport-layer session continuity; secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU; and the

protection of identifiers of either a vehicle or smart device (such as the Media Access Control (MAC) address and IPv6 address), which is discussed in detail in Section 6.3.

4. Vehicular Networks

This section describes the context for vehicular networks supporting V2V, V2I, and V2X communications and describes an internal network within a vehicle or an Edge Network (EN). Additionally, this section explains not only the internetworking between the internal networks of a vehicle and an EN via wireless links but also the internetworking between the internal networks of two vehicles via wireless links.

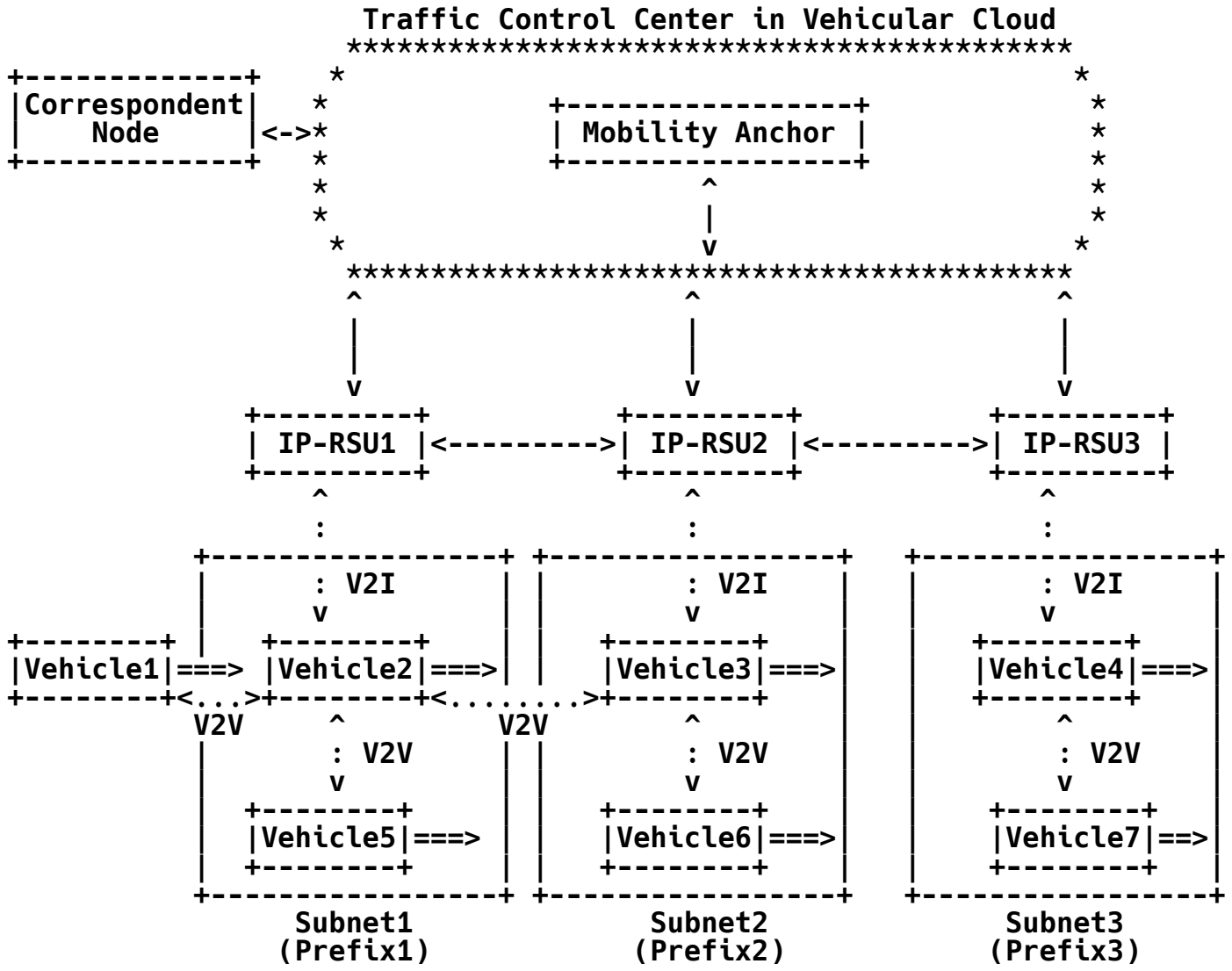


Figure 1: An Example Vehicular Network Architecture for V2I and V2V

4.1. Vehicular Network Architecture

Figure 1 shows an example vehicular network architecture for V2I and

V2V in a road network. The vehicular network architecture contains vehicles (including IP-OBU), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as components. These components are not mandatory, and they can be deployed into vehicular networks in various ways. Some of them (e.g., Mobility Anchor, Traffic Control Center, and Vehicular Cloud) may not be needed for the vehicular networks according to target use cases in Section 3.

Existing network architectures, such as the network architectures of PMIPv6 [RFC5213], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550], Automatic Extended Route Optimization [AERO], and Overlay Multilink Network Interface [OMNI], can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. Refer to Appendix B for the detailed discussion on multihop V2X networking by RPL and OMNI. Also, refer to Appendix A for the description of how OMNI is designed to support the use of multiple radio technologies in V2X. Note that though AERO/OMNI is not actually deployed in the industry, this AERO/OMNI is mentioned as a possible approach for vehicular networks in this document.

As shown in Figure 1, IP-RSUs as routers and vehicles with IP-OBU have wireless media interfaces for VANET. The three IP-RSUs (IP-RSU1, IP-RSU2, and IP-RSU3) are deployed in the road network and are connected with each other through the wired networks (e.g., Ethernet). A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of IP-RSUs and vehicles in the road network. A Mobility Anchor (MA) may be located in the TCC as a mobility management controller. Vehicle2, Vehicle3, and Vehicle4 are wirelessly connected to IP-RSU1, IP-RSU2, and IP-RSU3, respectively. The three wireless networks of IP-RSU1, IP-RSU2, and IP-RSU3 can belong to three different subnets (i.e., Subnet1, Subnet2, and Subnet3), respectively. Those three subnets use three different prefixes (i.e., Prefix1, Prefix2, and Prefix3).

Multiple vehicles under the coverage of an IP-RSU share a prefix just as mobile nodes share a prefix of a Wi-Fi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks. For example, in Figure 1, two vehicles (i.e., Vehicle2 and Vehicle5) can use Prefix1 to configure their IPv6 global addresses for V2I communication. Alternatively, two vehicles can employ a "Bring Your Own Addresses (BYOA)" (or "Bring Your Own Prefix (BYOP)") technique using their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network.

In wireless subnets in vehicular networks (e.g., Subnet1 and Subnet2 in Figure 1), vehicles can construct a connected VANET (with an arbitrary graph topology) and can communicate with each other via V2V communication. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the wireless communication range of each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., IP-RSU2 and IP-RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range of each other.

As a basic definition for IPv6 packets transported over IEEE 802.11-OCB, [RFC8691] specifies several details, including Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure.

An IPv6 mobility solution is needed for the guarantee of communication continuity in vehicular networks so that a vehicle's TCP session can be continued or that UDP packets can be delivered to a vehicle as a destination without loss while it moves from an IP-RSU's wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a correspondent node in the Vehicular Cloud, Vehicle2 can move from IP-RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213], NEMO [RFC3963] [RFC4885] [RFC4888], and AERO [AERO]). This document describes issues in mobility management for vehicular networks in Section 5.2. For improving TCP session continuity or successful UDP packet delivery, the Multipath TCP (MPTCP) [RFC8684] or QUIC protocol [RFC9000] can also be used. IP-OBUs, however, may still experience more session time-out and re-establishment procedures due to lossy connections among vehicles caused by the high mobility dynamics of them.

4.2. V2I-Based Internetworking

This section discusses the internetworking between a vehicle's internal network (i.e., mobile network) and an EN's internal network (i.e., fixed network) via V2I communication. The internal network of a vehicle is nowadays constructed with Ethernet by many automotive vendors [In-Car-Network]. Note that an EN can accommodate multiple routers (or switches) and servers (e.g., ECDs, navigation server, and DNS server) in its internal network.

A vehicle's internal network often uses Ethernet to interconnect Electronic Control Units (ECUs) in the vehicle. The internal network can support Wi-Fi and Bluetooth to accommodate a driver's and passenger's mobile devices (e.g., smartphone or tablet). The network topology and subnetting depend on each vendor's network configuration for a vehicle and an EN. It is reasonable to consider interactions between the internal network of a vehicle and that of another vehicle or an EN. Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. These dangers can include unauthorized driving control input and unauthorized driving information disclosure to an unauthorized third party. A malicious party can be a group of hackers, a criminal group, and a competitor for industrial espionage or sabotage. To minimize this kind of risk, an augmented identification and verification protocol, which has an extra means, shall be implemented based on a basic identity verification process. These extra means could include approaches based on certificates, biometrics, credit, or One-Time Passwords (OTPs) in addition to Host Identity Protocol certificates [RFC8002]. The parties of the verification protocol can be from a built-in verification protocol in the current vehicle, which is pre-installed

by a vehicle vendor. The parties can also be from any verification authorities that have the database of authenticated users. The security properties provided by a verification protocol can be identity-related information, such as the genuineness of an identity, the authenticity of an identity, and the ownership of an identity [RFC7427].

The augmented identification and verification protocol with extra means can support security properties such as the identification and verification of a vehicle, driver, and passenger. First, a credit-based method is when a vehicle classifies the messages it received from another host into various levels based on their potential effects on driving safety in order to calculate the credit of that sender. Based on accumulated credit, a correspondent node can verify the other party to see whether it is genuine or not. Second, a certificate-based method includes a user certificate (e.g., X.509 certificate [RFC5280]) to authenticate a vehicle or its driver. Third, a biometric method includes a fingerprint, face, or voice to authenticate a driver or passenger. Lastly, an OTP-based method lets another already-authenticated device (e.g., smartphone and tablet) of a driver or passenger be used to authenticate a driver or passenger.

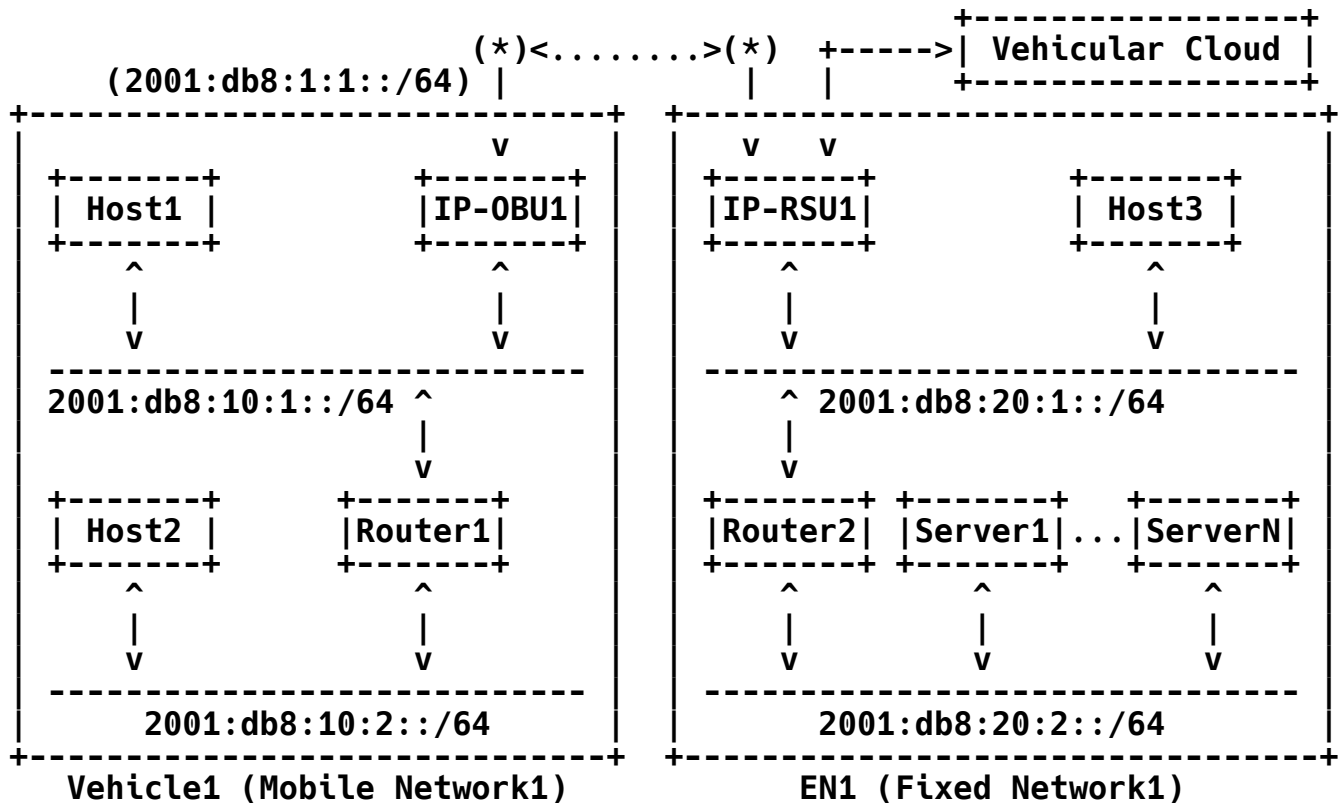


Figure 2: Internetworking between Vehicle and Edge Network

As shown in Figure 2, as internal networks, a vehicle's mobile network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for communication with another vehicle or another EN. The

internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the network prefixes of the internal networks. For the efficiency, the network prefixes of the internal networks (as a mobile network) in a vehicle need to be delegated and configured automatically. Note that a mobile network's network prefix can be called a Mobile Network Prefix (MNP) [RFC3963].

Figure 2 also shows the internetworking between the vehicle's mobile network and the EN's fixed network. There exists an internal network (Mobile Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2) and two routers (IP-OBU1 and Router1). There exists another internal network (Fixed Network1) inside EN1. EN1 has one host (Host3), two routers (IP-RSU1 and Router2), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1's IP-OBU1 (as a mobile router) and EN1's IP-RSU1 (as a fixed router) use 2001:db8:1:1::/64 for an external link (e.g., DSRC) for V2I networking. Thus, a host (Host1) in Vehicle1 can communicate with a server (Server1) in EN1 for a vehicular service through Vehicle1's mobile network, a wireless link between IP-OBU1 and IP-RSU1, and EN1's fixed network.

For the IPv6 communication between an IP-OBU and an IP-RSU or between two neighboring IP-OBUs, they need to know the network parameters, which include MAC layer and IPv6 layer information. The MAC layer information includes wireless link-layer parameters, transmission power level, and the MAC address of an external network interface for the internetworking with another IP-OBU or IP-RSU. The IPv6 layer information includes the IPv6 address and network prefix of an external network interface for the internetworking with another IP-OBU or IP-RSU.

Through the mutual knowledge of the network parameters of internal networks, packets can be transmitted between the vehicle's mobile network and the EN's fixed network. Thus, V2I requires an efficient protocol for the mutual knowledge of network parameters. Note that from a security point of view, perimeter-based policy enforcement [RFC9099] can be applied to protect parts of the internal network of a vehicle.

As shown in Figure 2, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be IPv6 link-local addresses, ULAs, or IPv6 global addresses. When IPv6 addresses are used, wireless interface configuration and control overhead for Duplicate Address Detection (DAD) [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710] [RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways.

Let us consider the upload/download time of a ground vehicle when it passes through the wireless communication coverage of an IP-RSU. For a given typical setting where 1 km is the maximum DSRC communication range [DSRC] and 100 km/h is the speed limit on highways for ground vehicles, the dwelling time can be calculated to be 72 seconds by dividing the diameter of the 2 km (i.e., two times the DSRC communication range where an IP-RSU is located in the center of the

circle of wireless communication) by the speed limit of 100 km/h (i.e., about 28 m/s). For the 72 seconds, a vehicle passing through the coverage of an IP-RSU can upload and download data packets to/from the IP-RSU. For special cases, such as emergency vehicles moving above the speed limit, the dwelling time is relatively shorter than that of other vehicles. For cases of airborne vehicles (i.e., aircraft), considering a higher flying speed and a higher altitude, the dwelling time can be much shorter.

4.3. V2V-Based Internetworking

This section discusses the internetworking between the mobile networks of two neighboring vehicles via V2V communication.

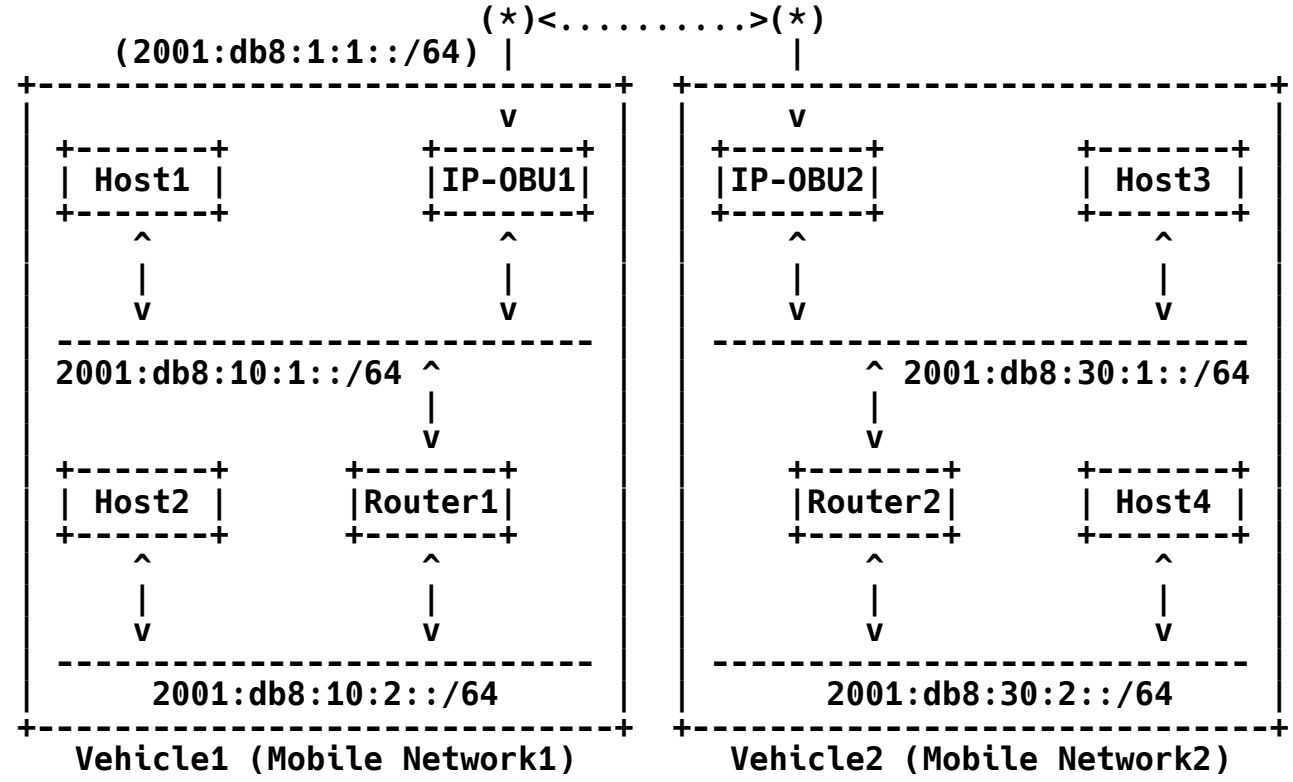


Figure 3: Internetworking between Two Vehicles

Figure 3 shows the internetworking between the mobile networks of two neighboring vehicles. There exists an internal network (Mobile Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2) and two routers (IP-OBU1 and Router1). There exists another internal network (Mobile Network2) inside Vehicle2. Vehicle2 has two hosts (Host3 and Host4) and two routers (IP-OBU2 and Router2). Vehicle1's IP-OBU1 (as a mobile router) and Vehicle2's IP-OBU2 (as a mobile router) use 2001:db8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. Thus, a host (Host1) in Vehicle1 can communicate with another host (Host3) in Vehicle2 for a vehicular service through Vehicle1's mobile network, a wireless link between IP-OBU1 and IP-OBU2, and Vehicle2's mobile network.

As a V2V use case in Section 3.1, Figure 4 shows a linear network topology of platooning vehicles for V2V communications where Vehicle3 is the lead vehicle with a driver, and Vehicle2 and Vehicle1 are the following vehicles without drivers. From a security point of view, before vehicles can be platooned, they shall be mutually authenticated to reduce possible security risks.

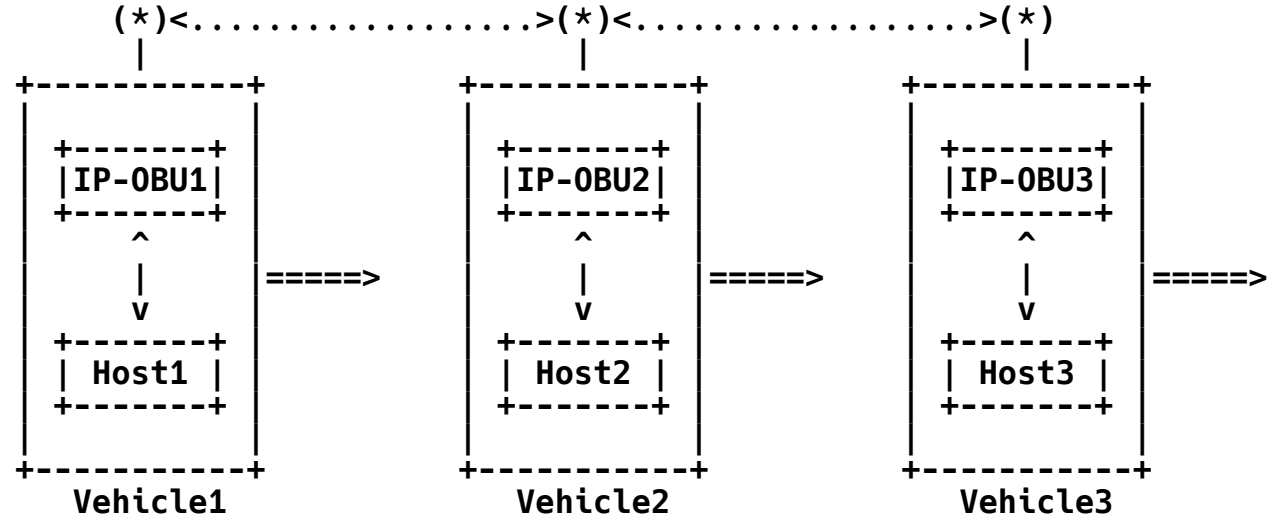
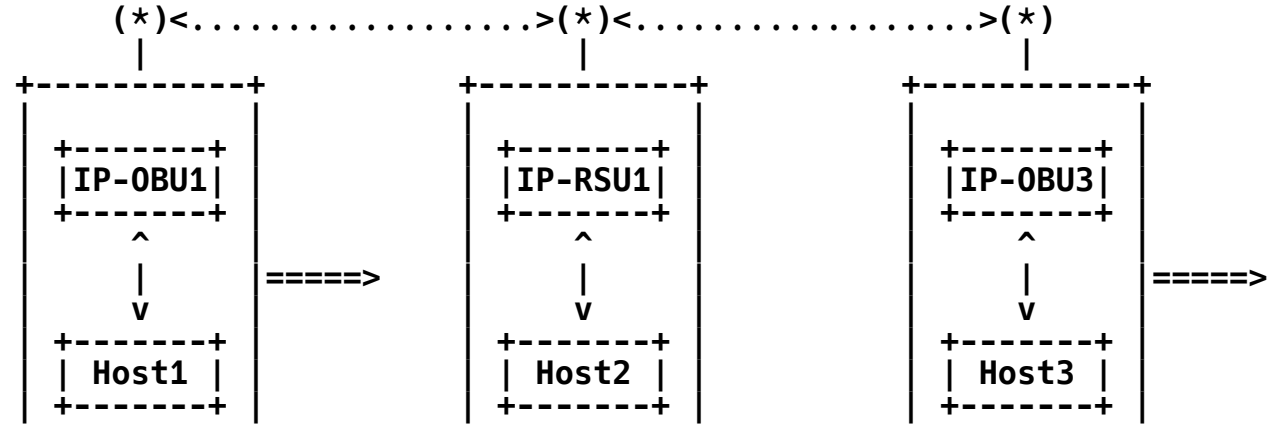


Figure 4: Multihop Internetworking between Two Vehicle Networks

As shown in Figure 4, multihop internetworking is feasible among the mobile networks of three vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-OBU2 in Vehicle2, and IP-OBU3 in Vehicle3 in the VANET, as shown in the figure.

In this section, the link between two vehicles is assumed to be stable for single-hop wireless communication regardless of the sight relationship, such as Line-of-Sight and Non-Line-of-Sight, as shown in Figure 3. Even in Figure 4, the three vehicles are connected to each other with a linear topology, however, multihop V2V communication can accommodate any network topology (i.e., an arbitrary graph) over VANET routing protocols.



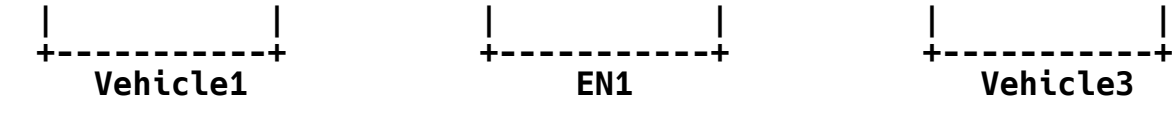


Figure 5: Multihop Internetworking between Two Vehicle Networks via IP-RSU (V2I2V)

As shown in Figure 5, multihop internetworking between two vehicles is feasible via an infrastructure node (e.g., IP-RSU) with wireless connectivity among the mobile networks of two vehicles and the fixed network of an edge network (denoted as EN1) in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-RSU1 in EN1, and IP-OBU3 in Vehicle3 in the VANET, as shown in the figure.

For the reliability required in V2V networking, the ND optimization defined in the Mobile Ad Hoc Network (MANET) [RFC6130] [RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases. This improvement serves the MANET routing protocols, such as the different versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181], Open Shortest Path First (OSPF) derivatives (e.g., [RFC5614]), and Dynamic Link Exchange Protocol (DLEP) [RFC8175] with its extensions [RFC8629] [RFC8757]. In short, the MANET ND mainly deals with maintaining extended network neighbors to enhance the link reliability. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes to improve the reliability, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services. For a more reliable V2V networking, some redundancy mechanisms should be provided in L3 in cases of the failure of L2. For different use cases, the optimal solution to improve V2V networking reliability may vary. For example, a group of platooning vehicles may have stabler neighbors than freely moving vehicles, as described in Section 3.1.

5. Problem Statement

In order to specify protocols using the architecture mentioned in Section 4.1, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a relatively short time compared to the lifetime of a link between a vehicle and an IP-RSU or between two vehicles. In these cases, vehicles may not have enough time either to build link-layer connections with each other and may rely more on connections with infrastructure. In other cases, the relative speed between vehicles may be low when vehicles move toward the same direction or are platooned. For those cases, vehicles can have more time to build and maintain connections with each other.

For safe driving, vehicles need to exchange application messages

every 0.5 seconds [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so the IPv6 control plane (e.g., ND procedure and DAD) needs to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1 km) and 100 km/h as the speed limit on highways (some countries can have much higher speed limits or even no limit, e.g., Germany), the lifetime of a link between a vehicle and an IP-RSU is in the order of a minute (e.g., about 72 seconds), and the lifetime of a link between two vehicles is about a half minute. Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an IP-RSU. This relative speed causes the lifetime of the wireless link between the vehicle and the IP-RSU to be halved. In reality, the DSRC communication range is around 500 m, so the link lifetime will be half of the maximum time. The time constraint of a wireless link between two nodes (e.g., vehicle and IP-RSU) needs to be considered because it may affect the lifetime of a session involving the link. The lifetime of a session varies depending on the session's type, such as web surfing, a voice call over IP, a DNS query, or context-aware navigation (in Section 3.1). Regardless of a session's type, to guide all the IPv6 packets to their destination host(s), IP mobility should be supported for the session. In a V2V scenario (e.g., context-aware navigation [CNP]), the IPv6 packets of a vehicle should be delivered to relevant vehicles efficiently (e.g., multicasting). With this observation, IPv6 protocol exchanges need to be performed as quickly as possible to support the message exchanges of various applications in vehicular networks.

Therefore, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. Meanwhile, the bandwidth of the wireless link determined by the lower layers (i.e., PHY and link layers) can affect the transmission time of control messages of the upper layers (e.g., IPv6) and the continuity of sessions in the higher layers (e.g., IPv6, TCP, and UDP). Hence, the bandwidth selection according to the Modulation and Coding Scheme (MCS) also affects the vehicular network connectivity. Note that usually the higher bandwidth gives the shorter communication range and the higher packet error rate at the receiving side, which may reduce the reliability of control message exchanges of the higher layers (e.g., IPv6). This section presents key topics, such as neighbor discovery and mobility management for links and sessions in IPv6-based vehicular networks. Note that the detailed discussion on the transport-layer session mobility and usage of available bandwidth to fulfill the use cases is left as potential future work.

5.1. Neighbor Discovery

IPv6 ND [RFC4861] [RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for link types including point-to-point, multicast-capable (e.g., Ethernet), and Non-Broadcast Multiple Access (NBMA). It assumes the efficient and reliable support of multicast and unicast from the link layer for various network operations, such

as MAC Address Resolution (AR), DAD, MLD, and Neighbor Unreachability Detection (NUD) [RFC4861] [RFC4862] [RFC2710] [RFC3810].

Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need IPv6 addresses to run IPv6 ND.

The requirements for IPv6 ND for vehicular networks are efficient DAD and NUD operations. An efficient DAD is required to reduce the overhead of DAD packets during a vehicle's travel in a road network, which can guarantee the uniqueness of a vehicle's global IPv6 address. An efficient NUD is required to reduce the overhead of the NUD packets during a vehicle's travel in a road network, which can guarantee the accurate neighborhood information of a vehicle in terms of adjacent vehicles and IP-RSUs.

The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption not valid frequently in vehicular networks. The partitioning and merging of VANETs frequently occurs in vehicular networks. This partitioning and merging should be considered for IPv6 ND, such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. SLAAC is not compatible with the partitioning and merging, and additional work is needed for ND to operate properly under those circumstances. Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the uniqueness of an IPv6 address that will be configured by a vehicle as DAD. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the existence of a vehicle under the network coverage of the MA or IP-RSU as NUD. Thus, SLAAC needs to prevent IPv6 address duplication due to the merging of VANETs, and IPv6 ND needs to detect unreachable neighboring vehicles due to the partitioning of a VANET. According to the partitioning and merging, a destination vehicle (as an IPv6 host) needs to be distinguished as a host that is either on-link or not on-link even though the source vehicle can use the same prefix as the destination vehicle [IPPL].

To efficiently prevent IPv6 address duplication (due to the VANET partitioning and merging) from happening in vehicular networks, the vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD. In this case, two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and IP-RSUs, as shown in Figure 1. By using the vehicular-network-wide DAD, vehicles can assure that their IPv6 addresses are unique in the vehicular network whenever they are connected to the vehicular infrastructure or become disconnected from it in the form of VANET.

For vehicular networks with high mobility and density, DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange driving safety messages (e.g., collision avoidance and accident notification) with each other with a short interval as suggested by the National Highway Traffic Safety Administration (NHTSA) of the U.S. [NHTSA-ACAS-Report]. Since the partitioning and merging of vehicular networks may require re-performing the DAD process repeatedly, the link scope of vehicles may be limited to a small area, which may delay the exchange of driving safety messages. Driving safety messages can include a vehicle's mobility information (e.g., position, speed, direction, and acceleration/deceleration) that is critical to other vehicles. The exchange interval of this message is recommended to be less than 0.5 seconds, which is required for a driver to avoid an emergency situation, such as a rear-end crash.

ND time-related parameters, such as router lifetime and Neighbor Advertisement (NA) interval, need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its position relative to its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles. The ND time-related parameters can be an operational setting or an optimization point particularly for vehicular networks. Note that the link-scope multicast messages in the ND protocol may cause a performance issue in vehicular networks. [RFC9119] suggests several optimization approaches for the issue.

For IPv6-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular networks, the delay-bounded data delivery is critical. IPv6 ND needs to work to support those IPv6-based safety applications efficiently. [VEHICULAR-ND] introduces a Vehicular Neighbor Discovery (VND) process as an extension of IPv6 ND for IP-based vehicular networks.

From the interoperability point of view, in IPv6-based vehicular networking, IPv6 ND should have minimum changes from the legacy IPv6 ND used in the Internet, including DAD and NUD operations, so that IPv6-based vehicular networks can be seamlessly connected to other intelligent transportation elements (e.g., traffic signals, pedestrian wearable devices, electric scooters, and bus stops) that use the standard IPv6 network settings.

5.1.1. Link Model

A subnet model for a vehicular network needs to facilitate communication between two vehicles with the same prefix regardless of the vehicular network topology as long as there exist bidirectional E2E paths between them in the vehicular network including VANETs and IP-RSUs. This subnet model allows vehicles with the same prefix to communicate with each other via a combination of multihop V2V and multihop V2I with VANETs and IP-RSUs. [WIRELESS-ND] introduces other issues in an IPv6 subnet model.

IPv6 protocols work under certain assumptions that do not necessarily

hold for vehicular wireless access link types [VIP-WAVE] [RFC5889]. For instance, some IPv6 protocols, such as NUD [RFC4861] and MIPv6 [RFC6275], assume symmetry in the connectivity among neighboring interfaces. However, radio interference and different levels of transmission power may cause asymmetric links to appear in vehicular wireless links [RFC6250]. As a result, a new vehicular link model needs to consider the asymmetry of dynamically changing vehicular wireless links.

There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local, unique-local, and global types of IPv6 addresses. In an IPv6 link, it is defined that all interfaces that are configured with the same subnet prefix and with the on-link bit set can communicate with each other on an IPv6 link. However, the vehicular link model needs to define the relationship between a link and a prefix, considering the dynamics of wireless links and the characteristics of VANET.

A VANET can have a single link between each vehicle pair within the wireless communication range, as shown in Figure 4. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Suppose that a global-scope IPv6 prefix (or an IPv6 ULA prefix) is assigned to VANETs in vehicular networks. Considering that two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, if they are not connected in one hop (that is, they have multihop network connectivity between them), then they may not be able to communicate with each other. Thus, in this case, the concept of an on-link IPv6 prefix does not hold because two vehicles with the same on-link IPv6 prefix cannot communicate directly with each other. Also, when two vehicles are located in two different VANETs with the same IPv6 prefix, they cannot communicate with each other. On the other hand, when these two VANETs converge to one VANET, the two vehicles can communicate with each other in a multihop fashion, for example, when they are Vehicle1 and Vehicle3, as shown in Figure 4.

From the previous observation, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model needs to use a prefix that is on-link and a prefix that is not on-link according to the network topology of vehicles, such as a one-hop reachable network and a multihop reachable network (or partitioned networks). If the vehicles with the same prefix are reachable from each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable from each other in one hop due to either the multihop topology in the VANET or multiple partitions, the prefix should not be on-link. In most cases in vehicular networks, due to the partitioning and merging of VANETs and the multihop network topology of VANETs, prefixes that are not on-link will be used for vehicles as default.

The vehicular link model needs to support multihop routing in a connected VANET where the vehicles with the same global-scope IPv6 prefix (or the same IPv6 ULA prefix) are connected in one hop or multiple hops. It also needs to support the multihop routing in

multiple connected VANETs through infrastructure nodes (e.g., IP-RSU) where they are connected to the infrastructure. For example, in Figure 1, suppose that Vehicle1, Vehicle2, and Vehicle3 are configured with their IPv6 addresses based on the same global-scope IPv6 prefix. Vehicle1 and Vehicle3 can also communicate with each other via either multihop V2V or multihop V2I2V. When Vehicle1 and Vehicle3 are connected in a VANET, it will be more efficient for them to communicate with each other directly via VANET rather than indirectly via IP-RSUs. On the other hand, when Vehicle1 and Vehicle3 are farther apart than the direct communication range in two separate VANETs and under two different IP-RSUs, they can communicate with each other through the relay of IP-RSUs via V2I2V. Thus, the two separate VANETs can merge into one network via IP-RSU(s). Also, newly arriving vehicles can merge the two separate VANETs into one VANET if they can play the role of a relay node for those VANETs.

Thus, in IPv6-based vehicular networking, the vehicular link model should have minimum changes for interoperability with standard IPv6 links efficiently to support IPv6 DAD, MLD, and NUD operations.

5.1.2. MAC Address Pseudonym

For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used so that the MAC address can be changed periodically. However, although such a pseudonym of a MAC address can protect to some extent the privacy of a vehicle, it may not be able to resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. Note that [MAC-ADD-RAN] discusses more about MAC address randomization, and [RCM-USE-CASES] describes several use cases for MAC address randomization.

In the ETSI standards, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities (e.g., MAC address) and the corresponding IPv6 addresses [Identity-Management]. Whenever the network interface identifier changes, the IPv6 address based on the network interface identifier needs to be updated, and the uniqueness of the address needs to be checked through a DAD procedure.

5.1.3. Routing

For multihop V2V communications in either a VANET or VANETs via IP-RSUs, a vehicular Mobile Ad Hoc Networks (MANET) routing protocol may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead [RFC9119].

A routing protocol for a VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in a VANET with a dynamic network topology because IPv6 ND is used to check the neighborhood of each vehicle. Thus, the vehicular routing needs to take advantage of IPv6 ND to minimize its control overhead.

RPL [RFC6550] defines a routing LLN protocol, which constructs and maintains Destination-Oriented Directed Acyclic Graphs (DODAGs) optimized by an Objective Function (OF). A defined OF provides route selection and optimization within an RPL topology. The RPL nodes use an anisotropic Distance Vector (DV) approach to form a DODAG by discovering and aggressively maintaining the upward default route toward the root of the DODAG. Downward routes follow the same DODAG, with lazy maintenance and stretched peer-to-peer (P2P) routing in the so-called storing mode. It is well-designed to reduce the topological knowledge and routing state that needs to be exchanged. As a result, the routing protocol overhead is minimized, which allows either highly constrained stable networks or less constrained, highly dynamic networks. Refer to Appendix B for the detailed description of RPL for multihop V2X networking.

An address registration extension for 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) in [RFC8505] can support light-weight mobility for nodes moving through different parents. The extension described in [RFC8505] is stateful and proactively installs the ND cache entries; this saves broadcasts and provides deterministic presence information for IPv6 addresses. Mainly, it updates the Address Registration Option (ARO) of ND defined in [RFC6775] to include a status field (which can indicate the movement of a node) and optionally a Transaction ID (TID) field (which is a sequence number that can be used to determine the most recent location of a node). Thus, RPL can use the information provided by the Extended ARO (EARO) defined in [RFC8505] to deal with a certain level of node mobility. When a leaf node moves to the coverage of another parent node, it should de-register its addresses with the previous parent node and register itself with a new parent node along with an incremented TID.

RPL can be used in IPv6-based vehicular networks, but it is primarily designed for low-power networks, which puts energy efficiency first. For using it in IPv6-based vehicular networks, there have not been actual experiences and practical implementations, though it was tested in IoT Low-Power and Lossy Network (LLN) scenarios. Another concern is that RPL may generate excessive topology discovery messages in a highly moving environment, such as vehicular networks. This issue can be an operational or optimization point for a practitioner.

Moreover, due to bandwidth and energy constraints, RPL does not suggest using a proactive mechanism (e.g., keepalive) to maintain accurate routing adjacencies, such as Bidirectional Forwarding Detection [RFC5881] and MANET Neighborhood Discovery Protocol [RFC6130]. As a result, due to the mobility of vehicles, network fragmentation may not be detected quickly, and the routing of packets between vehicles or between a vehicle and an infrastructure node may fail.

5.2. Mobility Management

The seamless connectivity and timely data exchange between two endpoints requires efficient mobility management including location

management and handover. Most vehicles are equipped with a GNSS receiver as part of a dedicated navigation system or a corresponding smartphone app. Note that the GNSS receiver may not provide vehicles with accurate location information in adverse environments, such as a building area or a tunnel. The location precision can be improved with assistance of the IP-RSUs or a cellular system with a GNSS receiver for location information.

With a GNSS navigator, efficient mobility management can be performed with the help of vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having IP-RSUs and an MA in TCC). This vehicular infrastructure can predict the future positions of the vehicles from their mobility information (e.g., the current position, speed, direction, and trajectory) for efficient mobility management (e.g., proactive handover). For a better proactive handover, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]), can be used to determine the moment of a handover between IP-RSUs along with mobility information.

By predicting a vehicle's mobility, the vehicular infrastructure needs to better support IP-RSUs to perform efficient SLAAC, data forwarding, horizontal handover (i.e., handover in wireless links using a homogeneous radio technology), and vertical handover (i.e., handover in wireless links using heterogeneous radio technologies) in advance along with the movement of the vehicle.

For example, as shown in Figure 1, when a vehicle (e.g., Vehicle2) is moving from the coverage of an IP-RSU (e.g., IP-RSU1) into the coverage of another IP-RSU (e.g., IP-RSU2) belonging to a different subnet, the IP-RSUs can proactively support the IPv6 mobility of the vehicle while performing the SLAAC, data forwarding, and handover for the sake of the vehicle.

For a mobility management scheme in a domain, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213]), DAD is not required because the IPv6 address of a vehicle's external wireless interface is guaranteed to be unique. There is a trade-off between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this trade-off to support efficient mobility management.

Even though SLAAC with classic ND costs DAD overhead during mobility management, SLAAC with the registration extension specified in [RFC8505] and/or with AERO/OMNI does not cost DAD overhead. SLAAC for vehicular networks needs to consider the minimization of the cost of DAD with the help of an infrastructure node (e.g., IP-RSU and MA). Using an infrastructure prefix over VANET allows direct routability to the Internet through the multihop V2I toward an IP-RSU. On the other hand, a BYOA does not allow such direct routability to the Internet since the BYOA is not topologically correct, that is, not routable in the Internet. In addition, a vehicle configured with a

BYOA needs a tunnel home (e.g., IP-RSU) connected to the Internet, and the vehicle needs to know which neighboring vehicle is reachable inside the VANET toward the tunnel home. There is non-negligible control overhead to set up and maintain routes to such a tunnel home [RFC4888] over the VANET.

For the case of a multihomed network, a vehicle can follow the first-hop router selection rule described in [RFC8028]. For example, an IP-OBU inside a vehicle may connect to an IP-RSU that has multiple routers behind. In this scenario, because the IP-OBU can have multiple prefixes from those routers, the default router selection, source address selection, and packet redirect process should follow the guidelines in [RFC8028]. That is, the vehicle should select its default router for each prefix by preferring the router that advertised the prefix.

Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275], PMIPv6 [RFC5213], and NEMO [RFC3963], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications, such as V2V and V2I. [VEHICULAR-MM] discusses a Vehicular Mobility Management (VMM) scheme to proactively do handover for vehicles.

Therefore, for the proactive and seamless IPv6 mobility of vehicles, the vehicular infrastructure (including IP-RSUs and MA) needs to efficiently perform the mobility management of the vehicles with their mobility information and link-layer information. Also, in IPv6-based vehicular networking, IPv6 mobility management should have minimum changes for the interoperability with the legacy IPv6 mobility management schemes, such as PMIPv6, DMM, LISP, and AERO.

6. Security Considerations

This section discusses security and privacy for IPv6-based vehicular networking. Security and privacy are paramount in V2I, V2V, and V2X networking along with neighbor discovery and mobility management.

Vehicles and infrastructure must be authenticated to each other by a password, a key, and/or a fingerprint in order to participate in vehicular networking. For the authentication in vehicular networks, the Vehicular Cloud needs to support a Public Key Infrastructure (PKI) efficiently, as either a dedicated or a co-located component inside a TCC. To provide safe interaction between vehicles or between a vehicle and infrastructure, only authenticated nodes (i.e., vehicle and infrastructure nodes) can participate in vehicular networks. Also, in-vehicle devices (e.g., ECUs) and a driver/passenger's mobile devices (e.g., smartphones and tablet PCs) in a vehicle need to securely communicate with other in-vehicle devices, another driver/passenger's mobile devices in another vehicle, or other servers behind an IP-RSU. Even though a vehicle is perfectly authenticated by another entity and legitimate to use the data generated by another vehicle, it may be hacked by malicious applications that track and collect its and other vehicles' information. In this case, an attack mitigation process may be

required to reduce the aftermath of malicious behaviors. Note that when a driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks due to the exposure of its in-flight traffic packets. [SEC-PRIV] discusses several types of threats for Vehicular Security and Privacy (VSP).

For secure V2I communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 2 [RFC4301] [RFC4302] [RFC4303] [RFC4308] [RFC7296]. Also, for secure V2V communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in another vehicle needs to be established, as shown in Figure 3.

For secure V2I/V2V communication, an element in a vehicle (e.g., an in-vehicle device and a driver/passenger's mobile device) needs to establish a secure connection (e.g., TLS) with another element in another vehicle or another element in a Vehicular Cloud (e.g., a server). Note that any key management approach can be used for the secure communication, and particularly for IPv6-based vehicular networks, a new or enhanced key management approach resilient to wireless networks is required.

IEEE Std 1609.2 [WAVE-1609.2] specifies security services for applications and management messages, but this WAVE specification is optional. Thus, if the link layer does not support the security of a WAVE frame, either the network layer or the transport layer needs to support security services for the WAVE frame.

6.1. Security Threats in Neighbor Discovery

For the classical IPv6 ND (i.e., the legacy ND), DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. [RFC6959] introduces threats enabled by IP source address spoofing. This possibility indicates that vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. [RFC8928] introduces a mechanism that protects the ownership of an address for 6LoWPAN ND from address theft and impersonation attacks. Based on the SEND mechanism [RFC3971], the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, Cryptographically Generated Addresses (CGAs) can be used to verify the true owner of a received ND message, which requires using the CGA ND option in the ND protocol. This CGA can protect vehicles against DAD flooding by DAD filtering based on the verification for the true owner of the received DAD message. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based approach [Vehicular-BlockChain] can be used. However, for a scenario where a trustable router or an authentication path cannot be obtained, it is desirable to find a solution in which vehicles and infrastructure nodes can authenticate each other without any support

from a third party.

When applying the classical IPv6 ND process to VANET, one of the security issues is that an IP-RSU (or IP-OBU) as a router may receive deliberate or accidental DoS attacks from network scans that probe devices on a VANET. In this scenario, the IP-RSU (or IP-OBU) can be overwhelmed by processing the network scan requests so that the capacity and resources of the IP-RSU (or IP-OBU) are exhausted, causing the failure of receiving normal ND messages from other hosts for network address resolution. [RFC6583] describes more about the operational problems in the classical IPv6 ND mechanism that can be vulnerable to deliberate or accidental DoS attacks and suggests several implementation guidelines and operational mitigation techniques for those problems. Nevertheless, for running IPv6 ND in VANET, those issues can be acuter since the movements of vehicles can be so diverse that there is a wider opportunity for rogue behaviors, and the failure of networking among vehicles may lead to grave consequences.

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes that are controlled by hackers. For safe driving applications (e.g., context-aware navigation, cooperative adaptive cruise control, and platooning), as explained in Section 3.1, the cooperative action among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) for disturbing safe driving. For example, a Sybil attack, which tries to confuse a vehicle with multiple false identities, may disturb a vehicle from taking a safe maneuver. Since cybersecurity issues in vehicular networks may cause physical vehicle safety issues, it may be necessary to consider those physical safety concerns when designing protocols in IPWAVE.

To identify malicious vehicles among vehicles, an authentication method may be required. A Vehicle Identification Number (VIN) (or a vehicle manufacturer certificate) and a user certificate (e.g., X.509 certificate [RFC5280]) along with an in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or its driver (having a user certificate) through a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the Vehicular Cloud. This authentication can be used to identify the vehicle that will communicate with an infrastructure node or another vehicle. In the case where a vehicle has an internal network (called a mobile network) and elements in the network (e.g., in-vehicle devices and a user's mobile devices), as shown in Figure 2, the elements in the network need to be authenticated individually for safe authentication. Also, Transport Layer Security (TLS) certificates [RFC8446] [RFC5280] can be used for an element's authentication to allow secure E2E vehicular communications between an element in a vehicle and another element in a server in a Vehicular Cloud or between an element in a vehicle and another element in another vehicle.

6.2. Security Threats in Mobility Management

For mobility management, a malicious vehicle can construct multiple virtual bogus vehicles and register them with IP-RSUs and MAs. This

registration makes the IP-RSUs and MAs waste their resources. The IP-RSUs and MAs need to determine whether a vehicle is genuine or bogus in mobility management. Also, for the confidentiality of control packets and data packets between IP-RSUs and MAs, the E2E paths (e.g., tunnels) need to be protected by secure communication channels. In addition, to prevent bogus IP-RSUs and MAs from interfering with the IPv6 mobility of vehicles, mutual authentication among the IP-RSUs, MAs, and vehicles needs to be performed by certificates (e.g., TLS certificate).

6.3. Other Threats

For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC or 5G V2X (or LTE V2X) is required on a highway. In this case, multiple intermediate vehicles as relay nodes can help to forward association and authentication messages toward an IP-RSU (or gNodeB/eNodeB) connected to an authentication server in the Vehicular Cloud. In this kind of process, the authentication messages forwarded by each vehicle can be delayed or lost, which may increase the construction time of a connection or cause some vehicles to not be able to be authenticated.

Even though vehicles can be authenticated with valid certificates by an authentication server in the Vehicular Cloud, the authenticated vehicles may harm other vehicles. To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded in either a centralized approach through a logging server (e.g., TCC) in the Vehicular Cloud or a decentralized approach (e.g., an ECD and blockchain [Bitcoin]) by the help of other vehicles and infrastructure.

There are trade-offs between centralized and decentralized approaches in logging of vehicles' behaviors (e.g., location, speed, direction, acceleration/deceleration, and lane change) and communication activities (e.g., transmission time, reception time, and packet types, such as TCP, UDP, SCTP, QUIC, HTTP, and HTTPS). A centralized approach is more efficient than a decentralized approach in terms of log data collection and processing in a central server in the Vehicular Cloud. However, the centralized approach may cause a higher delay than a decentralized approach in terms of the analysis of the log data and counteraction in a local ECD or a distributed database like a blockchain. The centralized approach stores log data collected from VANET into a remote logging server in a Vehicular Cloud as a central cloud, so it takes time to deliver the log data to a remote logging server. On the other hand, the decentralized approach stores the log data into a nearby edge computing device as a local logging server or a nearby blockchain node, which participates in a blockchain network. On the stored log data, an analyzer needs to perform a machine learning technique (e.g., deep learning) and seek suspicious behaviors of the vehicles. If such an analyzer is located either within or near the edge computing device, it can access the log data with a short delay, analyze it quickly, and generate feedback to allow for a quick counteraction against such malicious behaviors. On the other hand, if the Vehicular Cloud with the log data is far away from a problematic VANET with malicious behaviors, the centralized approach takes a longer time with the

analysis of the log data and the decision-making on malicious behaviors than the decentralized approach. If the log data is encrypted by a secret key, it can be protected from the observation of a hacker. The secret key sharing among legal vehicles, ECDs, and Vehicular Clouds should be supported efficiently.

Log data can release privacy breakage of a vehicle. The log data can contain the MAC address and IPv6 address for a vehicle's wireless network interface. If the unique MAC address of the wireless network interface is used, a hacker can track the vehicle with that MAC address and can track the privacy information of the vehicle's driver (e.g., location information). To prevent this privacy breakage, a MAC address pseudonym can be used for the MAC address of the wireless network interface, and the corresponding IPv6 address should be based on such a MAC address pseudonym. By solving a privacy issue of a vehicle's identity in logging, vehicles may observe each other's activities to identify any misbehaviors without privacy breakage. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles.

For completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles where no vehicle is trustable and verifying every message (such as IPv6 control messages including ND, DAD, NUD, and application-layer messages) is necessary. In this way, vehicular networks can defend against many possible cyberattacks. Thus, we need to have an efficient zero-trust framework or mechanism for vehicular networks.

For the non-repudiation of the harmful activities from malicious vehicles, as it is difficult for other normal vehicles to identify them, an additional and advanced approach is needed. One possible approach is to use a blockchain-based approach [Bitcoin] as an IPv6 security checking framework. Each IPv6 packet from a vehicle can be treated as a transaction, and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast-moving vehicles, either a new consensus algorithm needs to be developed, or an existing consensus algorithm needs to be enhanced. In addition, a consensus-based mechanism for the security of vehicular networks in the IPv6 layer can also be considered. A group of servers as blockchain infrastructure can be part of the security checking process in the IP layer.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, especially for a long-living transport-layer session (e.g., voice call over IP and video streaming service), a MAC address pseudonym needs to be provided to each vehicle; that is, each vehicle periodically updates its MAC address, and the vehicle's IPv6 address needs to be updated accordingly by the MAC address change [RFC4086] [RFC8981]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality (using either IPsec or TLS), there will be no privacy

benefit from changing MAC and IPv6 addresses because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses. Thus, the MAC address pseudonym and the IPv6 address update should be performed with strong E2E confidentiality.

The privacy exposure to the TCC via V2I is mostly about the location information of vehicles and may also include other in-vehicle activities, such as transactions of credit cards. The assumed, trusted actors are the owner of a vehicle, an authorized vehicle service provider (e.g., navigation service provider), and an authorized vehicle manufacturer for providing after-sales services. In addition, privacy concerns for excessively collecting vehicle activities from roadway operators, such as public transportation administrators and private contractors, may also pose threats on violating privacy rights of vehicles. It might be interesting to find a solution from a technological point of view along with public policy development for the issue.

The "multicasting" of the location information of a VRU's smartphone means IPv6 multicasting. There is a possible security attack related to this multicasting. Attackers can use "fake identifiers" as source IPv6 addresses of their devices to generate IPv6 packets and multicast them to nearby vehicles in order to cause confusion that those vehicles are surrounded by other vehicles or pedestrians. As a result, navigation services (e.g., Google Maps [Google-Maps] and Waze [Waze]) can be confused with fake road traffic by those vehicles or smartphones with "fake identifiers" [Fake-Identifier-Attack]. This attack with "fake identifiers" should be detected and handled by vehicular networks. To cope with this attack, both legal vehicles and legal VRUs' smartphones can be registered with a TCC and their locations can be tracked by the TCC. With this tracking, the TCC can tell the road traffic conditions caused by those vehicles and smartphones. In addition, to prevent hackers from tracking the locations of those vehicles and smartphones, either a MAC address pseudonym [MAC-ADD-RAN] or secure IPv6 address generation [RFC7721] can be used to protect the privacy of those vehicles and smartphones.

7. IANA Considerations

This document has no IANA actions.

8. References

8.1. Normative References

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

[RFC8691] Benamar, N., Härri, J., Lee, J., and T. Ernst, "Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11", RFC 8691, DOI 10.17487/RFC8691, December 2019, <https://www.rfc-editor.org/info/rfc8691>.

8.2. Informative References

[AERO] Templin, F. L., Ed., "Automatic Extended Route Optimization (AERO)", Work in Progress, Internet-Draft, draft-templin-intarea-aero-27, 23 February 2023, <https://datatracker.ietf.org/doc/html/draft-templin-intarea-aero-27>.

[Automotive-Sensing] Choi, J., Va, V., Gonzalez-Prelcic, N., Daniels, R., Bhat, C., and R. Heath, "Millimeter-Wave Vehicular Communication to Support Massive Automotive Sensing", IEEE Communications Magazine, Volume 54, Issue 12, pp. 160-167, DOI 10.1109/MCOM.2016.1600071CM, December 2016, <https://doi.org/10.1109/MCOM.2016.1600071CM>.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", <https://bitcoin.org/bitcoin.pdf>.

[CA-Cruise-Control] California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", <https://path.berkeley.edu/research/connected-and-automated-vehicles/cooperative-adaptive-cruise-control>.

[CASD] Shen, Y., Jeong, J., Oh, T., and S. H. Son, "CASD: A Framework of Context-Awareness Safety Driving in Vehicular Networks", 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA), DOI 10.1109/WAINA.2016.74, March 2016, <https://doi.org/10.1109/WAINA.2016.74>.

[CBDN] Kim, J., Kim, S., Jeong, J., Kim, H., Park, J., and T. Kim, "CBDN: Cloud-Based Drone Navigation for Efficient Battery Charging in Drone Networks", IEEE Transactions on Intelligent Transportation Systems, Volume 20, Issue 11, pp. 4174-4191, DOI 10.1109/TITS.2018.2883058, November 2019, <https://doi.org/10.1109/TITS.2018.2883058>.

[CNP] Mugabarigira, B., Shen, Y., Jeong, J., Oh, T., and H. Jeong, "Context-Aware Navigation Protocol for Safe Driving in Vehicular Cyber-Physical Systems", IEEE Transactions on Intelligent Transportation Systems, Volume 24, Issue 1, pp. 128-138, DOI 10.1109/TITS.2022.3210753, January 2023, <https://doi.org/10.1109/TITS.2022.3210753>.

[DFC] Jeong, J., Shen, Y., Kim, S., Choe, D., Lee, K., and Y. Kim, "DFC: Device-free human counting through WiFi fine-grained subcarrier information", IET Communications, Volume 15, Issue 3, pp. 337-350, DOI 10.1049/cmu2.12043, February 2021, <https://doi.org/10.1049/cmu2.12043>.

[DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), DOI 10.1520/E2213-03R10, September 2018, <https://doi.org/10.1520/E2213-03R10>.

[EU-2008-671-EC] European Union, "COMMISSION DECISION of 5 August 2008 on the harmonised use of radio spectrum in the 5 875-5 905 MHz frequency band for safety-related applications of Intelligent Transport Systems (ITS)", EU 2008/671/EC, August 2008, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0671&rid=7>.

[Fake-Identifier-Attack] ABC News, "Berlin artist uses handcart full of smartphones to trick Google Maps' traffic algorithm into thinking there is traffic jam", February 2020, <https://www.abc.net.au/news/2020-02-04/man-creates-fake-traffic-jam-on-google-maps-by-carting-99-phones/11929136>.

[FCC-ITS-Modification] Federal Communications Commission, "FCC Modernizes 5.9 GHz Band to Improve Wi-Fi and Automotive Safety", November 2020, <https://www.fcc.gov/document/fcc-modernizes-59-ghz-band-improve-wi-fi-and-automotive-safety-0>.

[FirstNet] FirstNet Authority, "First Responder Network Authority | FirstNet", <https://www.firstnet.gov/>.

[FirstNet-Report] FirstNet, "FY 2017: ANNUAL REPORT TO CONGRESS, Advancing Public Safety Broadband Communications", FirstNet FY 2017, December 2017, <https://www.firstnet.gov/system/tdf/FirstNet-Annual-Report-FY2017.pdf?file=1&type=node&id=449>.

[FPC-DMM] Matsushima, S., Bertz, L., Liebsch, M., Gundavelli, S., Moses, D., and C. E. Perkins, "Protocol for Forwarding Policy Configuration (FPC) in DMM", Work in Progress, Internet-Draft, draft-ietf-dmm-fpc-cpdp-14, 22 September 2020, <https://datatracker.ietf.org/doc/html/draft-ietf-dmm-fpc-cpdp-14>.

[Fuel-Efficient] van de Hoef, S., Johansson, K., and D. Dimarogonas, "Fuel-Efficient En Route Formation of Truck Platoons", IEEE Transactions on Intelligent Transportation Systems, Volume

19, Issue 1, pp. 102-112, DOI 10.1109/TITS.2017.2700021, January 2018, <https://doi.org/10.1109/TITS.2017.2700021>.

[Google-Maps] Google, "Google Maps", <https://www.google.com/maps/>.

[Identity-Management] Wetterwald, M., Hrizi, F., and P. Cataldi, "Cross-layer identities management in ITS stations", 10th IEEE International Conference on ITS Telecommunications, November 2010, <https://www.eurecom.fr/fr/publication/3205>.

[IEEE-802.11-OCB] IEEE, "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", DOI 10.1109/IEEESTD.2016.7786995, IEEE Std 802.11-2016, December 2016, <https://doi.org/10.1109/IEEESTD.2016.7786995>.

[IEEE-802.11p] IEEE, "IEEE Standard for Information technology-- Local and metropolitan area networks-- Specific requirements-- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments", DOI 10.1109/IEEESTD.2010.5514475, IEEE Std 802.11p-2010, July 2010, <https://doi.org/10.1109/IEEESTD.2010.5514475>.

[In-Car-Network] Lim, H., Volker, L., and D. Herrscher, "Challenges in a future IP/Ethernet-based in-car network for real-time applications", Proceedings of the 48th Design Automation Conference, pp. 7-12, DOI 10.1145/2024724.2024727, June 2011, <https://doi.org/10.1145/2024724.2024727>.

[IPPL] Nordmark, E., "IP over Intentionally Partially Partitioned Links", Work in Progress, Internet-Draft, draft-ietf-intarea-ippl-00, 30 March 2017, <https://datatracker.ietf.org/doc/html/draft-ietf-intarea-ippl-00>.

[ISO-ITS-IPv6] ISO/TC 204, "Intelligent transport systems - Communications access for land mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012, <https://www.iso.org/standard/46549.html>.

[ISO-ITS-IPv6-AMD1] ISO/TC 204, "Intelligent transport systems - Communications access for land mobiles (CALM) - IPv6 Networking - Amendment 1", ISO 21210:2012/AMD 1:2017, September 2017, <https://www.iso.org/standard/65691.html>.

[LIFS] Wang, J., Xiong, J., Jiang, H., Jamieson, K., Chen, X., Fang, D., and C. Wang, "Low Human-Effort, Device-Free Localization with Fine-Grained Subcarrier Information", IEEE Transactions on Mobile Computing, Volume 17, Issue 11, pp. 2550-2563, DOI 10.1109/TMC.2018.2812746, November 2018, <https://doi.org/10.1109/TMC.2018.2812746>.

[MAC-ADD-RAN] Zuniga, JC., Bernardos, CJ., Ed., and A. Andersdotter, "Randomized and Changing MAC Address", Work in Progress, Internet-Draft, draft-ietf-madinas-mac-address-randomization-06, 11 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-madinas-mac-address-randomization-06>.

[NHTSA-ACAS-Report] National Highway Traffic Safety Administration (NHTSA), "Automotive Collision Avoidance Systems (ACAS) Program Final Report", DOT HS 809 080, August 2000, <https://one.nhtsa.gov/people/injury/research/pub/ACAS/ACAS_index.htm>.

[OMNI] Templin, F. L., Ed., "Transmission of IP Packets over Overlay Multilink Network (OMNI) Interfaces", Work in Progress, Internet-Draft, draft-templin-intarea-omni-27, 23 February 2023, <https://datatracker.ietf.org/doc/html/draft-templin-intarea-omni-27>.

[PARCELS] Templin, F. L., Ed., "IP Parcels and Advanced Jumbos", Work in Progress, Internet-Draft, draft-templin-intarea-parcels-55, 28 February 2023, <https://datatracker.ietf.org/doc/html/draft-templin-intarea-parcels-55>.

[PSCE] European Commission, "PSCEurope Public Safety Communications Europe", <https://www.psc-europe.eu/>.

[RCM-USE-CASES] Henry, J. and Y. Lee, "Randomized and Changing MAC Address Use Cases and Requirements", Work in Progress, Internet-Draft, draft-ietf-madinas-use-cases-05, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-madinas-use-cases-05>.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999, <https://www.rfc-editor.org/info/rfc2710>.

[RFC3626] Clausen, T., Ed. and P. Jacquet, Ed., "Optimized Link State Routing Protocol (OLSR)", RFC 3626, DOI 10.17487/RFC3626, October 2003, <https://www.rfc-editor.org/info/rfc3626>.

[RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related

Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <https://www.rfc-editor.org/info/rfc3753>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <https://www.rfc-editor.org/info/rfc3963>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, DOI 10.17487/RFC4308, December 2005, <https://www.rfc-editor.org/info/rfc4308>.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, DOI 10.17487/RFC4821, March 2007, <https://www.rfc-editor.org/info/rfc4821>.

[RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, DOI 10.17487/RFC4885, July 2007, <https://www.rfc-editor.org/info/rfc4885>.

[RFC4888] Ng, C., Thubert, P., Watari, M., and F. Zhao, "Network Mobility Route Optimization Problem Statement", RFC 4888, DOI 10.17487/RFC4888, July 2007, <https://www.rfc-editor.org/info/rfc4888>.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <https://www.rfc-editor.org/info/rfc5213>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[RFC5614] Ogier, R. and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding", RFC 5614, DOI 10.17487/RFC5614, August 2009, <https://www.rfc-editor.org/info/rfc5614>.

[RFC5881] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, DOI 10.17487/RFC5881, June 2010, <https://www.rfc-editor.org/info/rfc5881>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <https://www.rfc-editor.org/info/rfc5889>.

[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, DOI 10.17487/RFC6130, April 2011, <https://www.rfc-editor.org/info/rfc6130>.

[RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250, DOI 10.17487/RFC6250, May 2011, <https://www.rfc-editor.org/info/rfc6250>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

[RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, DOI 10.17487/RFC6583, March 2012, <https://www.rfc-editor.org/info/rfc6583>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012,

<https://www.rfc-editor.org/info/rfc6775>.

[RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <https://www.rfc-editor.org/info/rfc6959>.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <https://www.rfc-editor.org/info/rfc7149>.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <https://www.rfc-editor.org/info/rfc7181>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC7333] Chan, H., Ed., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, DOI 10.17487/RFC7333, August 2014, <https://www.rfc-editor.org/info/rfc7333>.

[RFC7427] Kivinen, T. and J. Snyder, "Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)", RFC 7427, DOI 10.17487/RFC7427, January 2015, <https://www.rfc-editor.org/info/rfc7427>.

[RFC7429] Liu, D., Ed., Zuniga, JC., Ed., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, DOI 10.17487/RFC7429, January 2015, <https://www.rfc-editor.org/info/rfc7429>.

[RFC7466] Dearlove, C. and T. Clausen, "An Optimization for the Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 7466, DOI 10.17487/RFC7466, March 2015, <https://www.rfc-editor.org/info/rfc7466>.

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <https://www.rfc-editor.org/info/rfc7721>.

[RFC8002] Heer, T. and S. Varjonen, "Host Identity Protocol Certificates", RFC 8002, DOI 10.17487/RFC8002, October 2016, <https://www.rfc-editor.org/info/rfc8002>.

[RFC8028] Baker, F. and B. Carpenter, "First-Hop Router Selection by Hosts in a Multi-Prefix Network", RFC 8028, DOI 10.17487/RFC8028, November 2016, <https://www.rfc-editor.org/info/rfc8028>.

[RFC8175] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <https://www.rfc-editor.org/info/rfc8175>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

[RFC8629] Cheng, B. and L. Berger, Ed., "Dynamic Link Exchange Protocol (DLEP) Multi-Hop Forwarding Extension", RFC 8629, DOI 10.17487/RFC8629, July 2019, <https://www.rfc-editor.org/info/rfc8629>.

[RFC8684] Ford, A., Raiciu, C., Handley, M., Bonaventure, O., and C. Paasch, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 8684, DOI 10.17487/RFC8684, March 2020, <https://www.rfc-editor.org/info/rfc8684>.

[RFC8757] Cheng, B. and L. Berger, Ed., "Dynamic Link Exchange Protocol (DLEP) Latency Range Extension", RFC 8757, DOI 10.17487/RFC8757, March 2020, <https://www.rfc-editor.org/info/rfc8757>.

[RFC8899] Fairhurst, G., Jones, T., Tüxen, M., Rüngeler, I., and T. Völker, "Packetization Layer Path MTU Discovery for Datagram Transports", RFC 8899, DOI 10.17487/RFC8899, September 2020, <https://www.rfc-editor.org/info/rfc8899>.

[RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November 2020, <https://www.rfc-editor.org/info/rfc8928>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RFC9099] Vyncke, É., Chittimaneni, K., Kaeo, M., and E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099, DOI 10.17487/RFC9099, August 2021, <https://www.rfc-editor.org/info/rfc9099>.

[RFC9119] Perkins, C., McBride, M., Stanley, D., Kumari, W., and JC. Zúñiga, "Multicast Considerations over IEEE 802 Wireless Media", RFC 9119, DOI 10.17487/RFC9119, October 2021, <https://www.rfc-editor.org/info/rfc9119>.

[RFC9300] Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, Ed., "The Locator/ID Separation Protocol (LISP)", RFC 9300, DOI 10.17487/RFC9300, October 2022, <https://www.rfc-editor.org/info/rfc9300>.

[SAINT] Jeong, J., Jeong, H., Lee, E., Oh, T., and D. H. C. Du, "SAINT: Self-Adaptive Interactive Navigation Tool for Cloud-Based Vehicular Traffic Optimization", IEEE Transactions on Vehicular Technology, Volume 65, Issue 6, pp. 4053-4067, DOI 10.1109/TVT.2015.2476958, June 2016, <https://doi.org/10.1109/TVT.2015.2476958>.

[SAINTplus] Shen, Y., Lee, J., Jeong, H., Jeong, J., Lee, E., and D. H. C. Du, "SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization", IEEE Transactions on Intelligent Transportation Systems, Volume 19, Issue 4, pp. 1038-1053, DOI 10.1109/TITS.2017.2710881, June 2017, <https://doi.org/10.1109/TITS.2017.2710881>.

[SANA] Hwang, T. and J. Jeong, "SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks", Lecture Notes in Computer Science book series (LNISA, Volume 9502), DOI 10.1007/978-3-319-27293-1_12, December 2015, <https://doi.org/10.1007/978-3-319-27293-1_12>.

[Scrambler-Attack] Bloessl, B., Sommer, C., Dressier, F., and D. Eckhoff, "The scrambler attack: A robust physical layer attack on location privacy in vehicular networks", 2015 International Conference on Computing, Networking and Communications (ICNC), DOI 10.1109/ICCNC.2015.7069376, February 2015, <https://doi.org/10.1109/ICCNC.2015.7069376>.

[SEC-PRIV] Jeong, J., Ed., Shen, Y., Jung, H., Park, J., and T. Oh, "Basic Support for Security and Privacy in IP-Based Vehicular Networks", Work in Progress, Internet-Draft, draft-jeong-ipwave-security-privacy-07, 4 February 2023, <https://datatracker.ietf.org/doc/html/draft-jeong-ipwave-security-privacy-07>.

[SignalGuru] Koukoumidis, E., Peh, L., and M. Martonosi, "SignalGuru:

leveraging mobile phones for collaborative traffic signal schedule advisory", MobiSys '11: Proceedings of the 9th international conference on Mobile systems, applications, and services, pp. 127-140, DOI 10.1145/1999995.2000008, June 2011, <https://doi.org/10.1145/1999995.2000008>.

[TR-22.886-3GPP]
3GPP, "Study on enhancement of 3GPP support for 5G V2X services", 3GPP TS 22.886 16.2.0, December 2018, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3108>.

[Truck-Platooning]
California Partners for Advanced Transportation Technology (PATH), "Truck Platooning", <https://path.berkeley.edu/research/connected-and-automated-vehicles/truck-platooning>.

[TS-23.285-3GPP]
3GPP, "Architecture enhancements for V2X services", 3GPP TS 23.285 16.2.0, December 2019, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3078>.

[TS-23.287-3GPP]
3GPP, "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services", 3GPP TS 23.287 16.2.0, March 2020, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3578>.

[UAM-ITS] Templin, F., Ed., "Urban Air Mobility Implications for Intelligent Transportation Systems", Work in Progress, Internet-Draft, draft-templin-ipwave-uam-its-04, 4 January 2021, <https://datatracker.ietf.org/doc/html/draft-templin-ipwave-uam-its-04>.

[Vehicular-BlockChain]
Dorri, A., Steger, M., Kanhere, S., and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", IEEE Communications Magazine, Volume 55, Issue 12, pp. 119-125, DOI 10.1109/MCOM.2017.1700879, December 2017, <https://doi.org/10.1109/MCOM.2017.1700879>.

[VEHICULAR-MM]
Jeong, J., Ed., Mugabarigira, B., Shen, Y., and H. Jung, "Vehicular Mobility Management for IP-Based Vehicular Networks", Work in Progress, Internet-Draft, draft-jeong-ipwave-vehicular-mobility-management-09, 4 February 2023, <https://datatracker.ietf.org/doc/html/draft-jeong-ipwave-vehicular-mobility-management-09>.

[VEHICULAR-ND]
Jeong, J., Ed., Shen, Y., Kwon, J., and S. Cespedes, "Vehicular Neighbor Discovery for IP-Based Vehicular

Networks", Work in Progress, Internet-Draft, draft-jeong-ipwave-vehicular-neighbor-discovery-15, 4 February 2023, <https://datatracker.ietf.org/doc/html/draft-jeong-ipwave-vehicular-neighbor-discovery-15>.

[VIP-WAVE] Cespedes, S., Lu, N., and X. Shen, "VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks", IEEE Transactions on Intelligent Transportation Systems, Volume 14, Issue 1, pp. 82-97, DOI 10.1109/TITS.2012.2206387, March 2013, <https://doi.org/10.1109/TITS.2012.2206387>.

[WAVE-1609.0] IEEE, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture", DOI 10.1109/IEEESTD.2014.6755433, IEEE Std 1609.0-2013, March 2014, <https://doi.org/10.1109/IEEESTD.2014.6755433>.

[WAVE-1609.2] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", DOI 10.1109/IEEESTD.2016.7426684, IEEE Std 1609.2-2016, March 2016, <https://doi.org/10.1109/IEEESTD.2016.7426684>.

[WAVE-1609.3] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services", DOI 10.1109/IEEESTD.2016.7458115, IEEE Std 1609.3-2016, April 2016, <https://doi.org/10.1109/IEEESTD.2016.7458115>.

[WAVE-1609.4] IEEE, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation", DOI 10.1109/IEEESTD.2016.7435228, IEEE Std 1609.4-2016, March 2016, <https://doi.org/10.1109/IEEESTD.2016.7435228>.

[Waze] Google, "Waze", <https://www.waze.com/>.

[WIRELESS-ND] Thubert, P., Ed. and M. Richardson, "Architecture and Framework for IPv6 over Non-Broadcast Access", Work in Progress, Internet-Draft, draft-thubert-6man-ipv6-over-wireless-15, 8 March 2023, <https://datatracker.ietf.org/doc/html/draft-thubert-6man-ipv6-over-wireless-15>.

Appendix A. Support of Multiple Radio Technologies for V2V

Vehicular networks may consist of multiple radio technologies, such as DSRC and 5G V2X (or LTE V2X). Although a Layer 2 solution can provide support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains

when vehicles need to disseminate or forward packets toward destinations that are multiple hops away. In addition, the IPv6-based approach for V2V as a network-layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X (or LTE V2X). Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., OMNI [OMNI] and DLEP [RFC8175]) and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard information on a highway having multiple radio technologies.

Appendix B. Support of Multihop V2X Networking

The multihop V2X networking can be supported by RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] and Overlay Multilink Network Interface [OMNI] with AERO [AERO].

RPL defines an IPv6 routing protocol for Low-Power and Lossy Networks (LLNs) as being mostly designed for home automation routing, building automation routing, industrial routing, and urban LLN routing. It uses a Destination-Oriented Directed Acyclic Graph (DODAG) to construct routing paths for hosts (e.g., IoT devices) in a network. The DODAG uses an Objective Function (OF) for route selection and optimization within the network. A user can use different routing metrics to define an OF for a specific scenario. RPL supports multipoint-to-point, point-to-multipoint, and point-to-point traffic; and the major traffic flow is the multipoint-to-point traffic. For example, in a highway scenario, a vehicle may not access an IP-RSU directly because of the distance of the DSRC coverage (up to 1 km). In this case, the RPL can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the IP-RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

RPL is primarily designed to minimize the control plane activity, which is the relative amount of routing protocol exchanges versus data traffic; this approach is beneficial for situations where the power and bandwidth are scarce (e.g., an IoT LLN where RPL is typically used today), but also in situations of high relative mobility between the nodes in the network (also known as swarming, e.g., within a variable set of vehicles with a similar global motion, or a variable set of drones flying toward the same direction).

To reduce the routing exchanges, RPL leverages a Distance Vector (DV) approach, which does not need a global knowledge of the topology, and only optimizes the routes to and from the root, allowing peer-to-peer (P2P) paths to be stretched. Although RPL installs its routes proactively, it only maintains them lazily, that is, in reaction to actual traffic or as a slow background activity. Additionally, RPL leverages the concept of an OF, which allows adapting the activity of the routing protocol to use cases, e.g., type, speed, and quality of the radios. RPL does not need to converge and provides connectivity to most nodes most of the time. The default route toward the root is maintained aggressively and may change while a packet progresses

without causing loops, so the packet will still reach the root. There are two modes for routing in RPL: non-storing mode and storing mode. In non-storing mode, a node inside the mesh or swarm that changes its point(s) of attachment to the graph informs the root with a single unicast packet flowing along the default route, and the connectivity is restored immediately; this mode is preferable for use cases where Internet connectivity is dominant. On the other hand, in storing mode, the routing stretch is reduced for better P2P connectivity, and the Internet connectivity is restored more slowly during the time for the DV operation to operate hop-by-hop. While an RPL topology can quickly scale up and down and fit the needs of mobility of vehicles, the total performance of the system will also depend on how quickly a node can form an address, join the mesh (including Authentication, Authorization, and Accounting (AAA)), and manage its global mobility to become reachable from another node outside the mesh.

OMNI defines a protocol for the transmission of IPv6 packets over Overlay Multilink Network Interfaces that are virtual interfaces governing multiple physical network interfaces. OMNI supports multihop V2V communication between vehicles in multiple forwarding hops via intermediate vehicles with OMNI links. It also supports multihop V2I communication between a vehicle and an infrastructure access point by multihop V2V communication. The OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD messaging.

In the OMNI protocol, an OMNI virtual interface can have a ULA [RFC4193] indeed, but wireless physical interfaces associated with the OMNI virtual interface can use any prefixes. The ULA supports both V2V and V2I multihop forwarding within the vehicular network (e.g., via a VANET routing protocol) while each vehicle can communicate with Internet correspondents using IPv6 global addresses via OMNI interface encapsulation over the wireless interface.

For the control traffic overhead for running both vehicular ND and a VANET routing protocol, the AERO/OMNI approach may avoid this issue by using MANET routing protocols only (i.e., no multicast of IPv6 ND messaging) in the wireless underlay network while applying efficient unicast IPv6 ND messaging in the OMNI overlay on an as-needed basis for router discovery and NUD. This greatly reduces the overhead for VANET-wide multicasting while providing agile accommodation for dynamic topology changes.

Appendix C. Support of Mobility Management for V2I

The seamless application communication between two vehicles or between a vehicle and an infrastructure node requires mobility management in vehicular networks. The mobility management schemes include a host-based mobility scheme, network-based mobility scheme, and software-defined networking scheme.

In the host-based mobility scheme (e.g., MIPv6), an IP-RSU plays the role of a home agent. On the other hand, in the network-based mobility scheme (e.g., PMIPv6), an MA plays the role of a mobility

management controller, such as a Local Mobility Anchor (LMA) in PMIPv6, which also serves vehicles as a home agent, and an IP-RSU plays the role of an access router, such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213]. The host-based mobility scheme needs client functionality in the IPv6 stack of a vehicle as a mobile node for mobility signaling message exchange between the vehicle and home agent. On the other hand, the network-based mobility scheme does not need such client functionality of a vehicle because the network infrastructure node (e.g., MAG in PMIPv6) as a proxy mobility agent handles the mobility signaling message exchange with the home agent (e.g., LMA in PMIPv6) for the sake of the vehicle.

There are a scalability issue and a route optimization issue in the network-based mobility scheme (e.g., PMIPv6) when an MA covers a large vehicular network governing many IP-RSUs. In this case, a distributed mobility scheme (e.g., DMM [RFC7429]) can mitigate the scalability issue by distributing multiple MAs in the vehicular network such that they are positioned closer to vehicles for route optimization and bottleneck mitigation in a central MA in the network-based mobility scheme. All these mobility approaches (i.e., a host-based mobility scheme, network-based mobility scheme, and distributed mobility scheme) and a hybrid approach of a combination of them need to provide an efficient mobility service to vehicles moving fast and moving along with relatively predictable trajectories along the roadways.

In vehicular networks, the control plane can be separated from the data plane for efficient mobility management and data forwarding by using the concept of Software-Defined Networking (SDN) [RFC7149] [FPC-DMM]. Note that Forwarding Policy Configuration (FPC) in [FPC-DMM], which is a flexible mobility management system, can manage the separation of data plane and control plane in DMM. In SDN, the control plane and data plane are separated for the efficient management of forwarding elements (e.g., switches and routers) where an SDN controller configures the forwarding elements in a centralized way, and they perform packet forwarding according to their forwarding tables that are configured by the SDN controller. An MA as an SDN controller needs to efficiently configure and monitor its IP-RSUs and vehicles for mobility management and security services.

Appendix D. Support of MTU Diversity for IP-Based Vehicular Networks

The wireless and/or wired-line links in paths between both mobile nodes and fixed network correspondents may configure a variety of Maximum Transmission Units (MTUs), where all IPv6 links are required to support a minimum MTU of 1280 octets and may support larger MTUs. Unfortunately, determining the path MTU (i.e., the minimum link MTU in the path) has proven to be inefficient and unreliable due to the uncertain nature of the loss-oriented ICMPv6 messaging service used for path MTU discovery. Recent developments have produced a more reliable path MTU determination service for TCP [RFC4821] and UDP [RFC8899]; however, the MTUs discovered are always limited by the most restrictive link MTU in the path (often 1500 octets or smaller).

The AERO/OMNI service addresses the MTU issue by introducing a new layer in the Internet architecture known as the "OMNI Adaptation

Layer (OAL)". The OAL allows end systems that configure an OMNI interface to utilize a full 65535-octet MTU by leveraging the IPv6 fragmentation and reassembly service during encapsulation to produce fragment sizes that are assured of traversing the path without loss due to a size restriction. Thus, this allows end systems to send packets that are often much larger than the actual path MTU.

Performance studies over the course of many decades have proven that applications will see greater performance by sending smaller numbers of large packets (as opposed to larger numbers of small packets) even if fragmentation is needed. The OAL further supports even larger packet sizes through the IP Parcels construct [PARCELS], which provides "packets-in-packet" encapsulation for a total size up to 4 MB. Together, the OAL and IP Parcels will provide a revolutionary new capability for greater efficiency in both mobile and fixed networks. On the other hand, due to the highly dynamic nature of vehicular networks, a high packet loss may not be able to be avoided. The high packet loss on IP Parcels can simultaneously cause multiple TCP sessions to experience packet retransmissions, session time-out, or re-establishment of the sessions. Other protocols, such as MPTCP and QUIC, may also experience similar issues. A mechanism for mitigating this issue in OAL and IP Parcels should be considered.

Acknowledgments

This work was supported by a grant from the Institute of Information & Communications Technology Planning & Evaluation (IITP) funded by the Korea MSIT (Ministry of Science and ICT) (R-20160222-002755, Cloud-based Security Intelligence Technology Development for the Customized Security Service Provisioning).

This work was supported in part by the MSIT, Korea, under the ITRC (Information Technology Research Center) support program (IITP-2022-2017-0-01633) supervised by the IITP.

This work was supported in part by the IITP (2020-0-00395-003, Standard Development of Blockchain-based Network Management Automation Technology).

This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

This work was supported in part by the Cisco University Research Program Fund, Grant # 2019-199458 (3696), and by ANID Chile Basal Project FB0008.

Contributors

This document is a group work of the IPWAVE working group, greatly benefiting from inputs and texts by Rex Buddenberg (Naval Postgraduate School), Thierry Ernst (YoGoKo), Bokor Laszlo (Budapest University of Technology and Economics), Jose Santa Lozanoi (Universidad of Murcia), Richard Roy (MIT), Francois Simon (Pilot), Sri Gundavelli (Cisco), Erik Nordmark (Zededa), Dirk von Hugo (Deutsche Telekom), Pascal Thubert (Cisco), Carlos Bernardos (UC3M),

Russ Housley (Vigil Security), Suresh Krishnan (Cisco), Nancy Cam-Winget (Cisco), Fred L. Templin (The Boeing Company), Jung-Soo Park (ETRI), Zeungil (Ben) Kim (Hyundai Motors), Kyoungjae Sun (Soongsil University), Zhiwei Yan (CNNIC), YongJoon Joe (LSware), Peter E. Yee (Akayla), and Erik Kline (Aalyria). The authors sincerely appreciate their contributions.

The following are coauthors of this document:

Nabil Benamar
Department of Computer Sciences,
High School of Technology of Meknes
Moulay Ismail University
Morocco
Phone: +212 6 70 83 22 36
Email: benamar73@gmail.com

Sandra Cespedes
NIC Chile Research Labs
Universidad de Chile
Av. Blanco Encalada 1975
Santiago
Chile
Phone: +56 2 29784093
Email: scespede@niclabs.cl

Jérôme Härri
Communication Systems Department
EURECOM
Sophia-Antipolis
France
Phone: +33 4 93 00 81 34
Email: jerome.haerri@eurecom.fr

Dapeng Liu
Alibaba
Beijing
100022
China
Phone: +86 13911788933
Email: max.ldp@alibaba-inc.com

Tae (Tom) Oh
Department of Information Sciences and Technologies
Rochester Institute of Technology
One Lomb Memorial Drive
Rochester, NY 14623-5603
United States of America
Phone: +1 585 475 7642
Email: Tom.Oh@rit.edu

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway,
Santa Clara, CA 95050
United States of America
Phone: +1 408 330 4586,
Email: charliep@computer.org

Alexandre Petrescu
CEA, LIST, CEA Saclay
91190 Gif-sur-Yvette
France
Phone: +33169089223
Email: Alexandre.Petrescu@cea.fr

Yiwen Chris Shen
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4106
Email: chrisshen@skku.edu
URI: https://chrisshen.github.io

Michelle Wetterwald
FBConsulting
21, Route de Luxembourg,
L-L-6633, Wasserbillig,
Luxembourg
Email: Michelle.Wetterwald@gmail.com

Author's Address

Jaehoon Paul Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea
Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php