

IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement
and Use Cases
[draft-ietf-ipwave-vehicular-networking-12](#)

Abstract

This document discusses the problem statement and use cases of IP-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, it makes a problem statement about key aspects in IP-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document specifies requirements in IP-based vehicular networking, and suggests the direction of solutions satisfying those requirements.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 5, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents

(<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	3
3.	Use Cases	5
3.1.	V2V	5
3.2.	V2I	6
3.3.	V2X	7
4.	Vehicular Networks	8
4.1.	Vehicular Network Architecture	9
4.2.	V2I-based Internetworking	11
4.3.	V2V-based Internetworking	13
5.	Problem Statement	14
5.1.	Neighbor Discovery	15
5.1.1.	Link Model	16
5.1.2.	MAC Address Pseudonym	17
5.1.3.	Routing	18
5.2.	Mobility Management	19
6.	Security Considerations	20
7.	Informative References	21
Appendix A.	Changes from draft-ietf-ipwave-vehicular-networking-11	27
Appendix B.	Acknowledgments	28
Appendix C.	Contributors	28
	Author's Address	30

[1.](#) Introduction

Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks. 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). 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](#)].

For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety 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 of the DSRC, while IEEE 1609.2 [[WAVE-1609.2](#)] covers security aspects, IEEE 1609.3 [[WAVE-1609.3](#)] defines related services at network and transport layers, and IEEE 1609.4 [[WAVE-1609.4](#)] specifies the multi-channel operation. IEEE 802.11p was first a separate amendment, but was later rolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) in 2012 [[IEEE-802.11-OCB](#)].

Along with these WAVE standards, IPv6 [[RFC8200](#)] and Mobile IP protocols (e.g., MIPv4 [[RFC5944](#)], MIPv6 [[RFC6275](#)], and Proxy MIPv6 (PMIPv6) [[RFC5213](#)][[RFC5844](#)]) can be applied to vehicular networks. 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](#)].

This document describes use cases and a problem statement about IP-based vehicular networking for ITS, which is named IP Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, it makes a problem statement about key aspects in IPWAVE, namely, IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect of the problem statement, this document specifies requirements in IP-based vehicular networking, and proposes the direction of solutions fulfilling those requirements. This document is intended to motivate development of key protocols for IPWAVE.

2. Terminology

This document uses the following definitions:

- o Class-Based Safety Plan: A vehicle can make safety plan by classifying the surrounding vehicles into different groups for safety purposes according to the geometrical relationship among them. The vehicle groups can be classified as Line-of-Sight Unsafe, Non-Line-of-Sight Unsafe, and Safe groups [[CASD](#)].
- o 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](#)].

- o LiDAR: "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.
- o Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support their address autoconfiguration and mobility management with a binding table. An MA has end-to-end connections with RSUs under its control.
- o On-Board Unit (OBU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and Cellular V2X (C-V2X) [[TS-23.285-3GPP](#)]) for wireless communications with other OBUs and RSUs, and may be connected to in-vehicle devices or networks. An OBU is mounted on a vehicle.
- o OCB: "Outside the Context of a Basic Service Set". It is differentiated from the Basic Service Set (BSS) mode in IEEE 802.11 standard. A node in OCB mode can directly transmit packets to other nodes in its wireless range without the authentication or association process defined in BSS mode [[IEEE-802.11-OCB](#)].
- o Platooning: Moving vehicles can be grouped together to reduce air-resistance for energy efficiency and reduce the number of drivers such that only the leading vehicle has a driver and the other vehicles are autonomous vehicles without a driver and closely following the leading vehicle [[Truck-Platooning](#)].
- o Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) for wireless communications with vehicles and is also connected to the Internet through a router or switch for packet forwarding. An RSU can accommodate multiple routers (or switches) and servers (e.g., DNS server and edge computing server) in its internal network as an edge computing system. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in a car parking area.
- o Traffic Control Center (TCC): A node that maintains road infrastructure information (e.g., RSUs, traffic signals, and loop detectors), 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 included in a vehicular cloud for vehicular networks.
- o Vehicle: A Vehicle in this document is a node that has an OBU for wireless communication with other vehicles and RSUs. It has a

radio navigation receiver of Global Positioning System (GPS) for efficient navigation.

- o Vehicular Ad Hoc Network (VANET): 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.
- o Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network forwarding elements (e.g., switch and router).
- o Vehicle Detection Loop (i.e., Loop Detector): An inductive device used for detecting vehicles passing or arriving at a certain point, for instance, at an intersection with traffic lights or at a ramp toward a highway. The relatively crude nature of the loop's structure means that only metal masses above a certain size are capable of triggering the detection.
- o V2I2P: "Vehicle to Infrastructure to Pedestrian".
- o V2I2V: "Vehicle to Infrastructure to Vehicle".
- o WAVE: "Wireless Access in Vehicular Environments" [[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).

3.1. V2V

The use cases of V2V networking discussed in this section include

- o Context-aware navigation for driving safety and collision avoidance;
- o Cooperative adaptive cruise control in an urban roadway;
- o Platooning in a highway;
- o Cooperative environment sensing.

These four techniques will be important elements for self-driving vehicles.

Context-Aware Safety Driving (CASD) navigator [[CASD](#)] can help drivers to drive safely by alerting the drivers about dangerous obstacles and situations. That is, 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, which 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.

Cooperative Adaptive Cruise Control (CACC) [[CA-Cruise-Control](#)] helps vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles in 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 collision.

Platooning [[Truck-Platooning](#)] allows a series of vehicles (e.g., trucks) to follow each other very closely. Trucks 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 meters to 10 meters). Platooning can maximize the throughput of vehicular traffic in a highway and reduce the gas consumption because the leading vehicle can help the following vehicles to experience less air resistance.

Cooperative-environment-sensing use cases suggest that vehicles can share environmental information from various vehicle-mounted sensors, such as radars, LiDARs, and cameras with other vehicles and pedestrians. [[Automotive-Sensing](#)] introduces a 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 the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment.

[3.2.](#) V2I

The use cases of V2I networking discussed in this section include

- o Navigation service;
- o Energy-efficient speed recommendation service;
- o Accident notification service.

A navigation service, for example, the Self-Adaptive Interactive Navigation Tool (SAINT) [[SAINT](#)], using V2I networking interacts with TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles for 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.

A TCC can recommend an energy-efficient speed to a vehicle that depends on its traffic environment. [[Fuel-Efficient](#)] studies fuel-efficient route and speed plans for platooned trucks.

The emergency communication between accident vehicles (or emergency vehicles) and TCC can be performed via either RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [[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 by 4G-LTE for the 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 near future.

[3.3.](#) V2X

The use case of V2X networking discussed in this section is pedestrian protection service.

A pedestrian protection service, such as Safety-Aware Navigation Application (SANA) [[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., WiFi) with an RSU. Vehicles and pedestrians can also communicate with each other via an RSU that delivers scheduling information for wireless communication in order to save the smartphones' battery through sleeping mode.

For Vehicle-to-Pedestrian (V2P), a vehicle can directly communicate with a pedestrian's smartphone by V2X without RSU relaying. Light-weight mobile nodes such as bicycles may also communicate directly with a vehicle for collision avoidance using V2V.

4. Vehicular Networks

This section describes a vehicular network architecture supporting V2V, V2I, and V2X communications in vehicular networks. Also, it describes an internal network within a vehicle or RSU, and the internetworking between the internal networks via DSRC links.

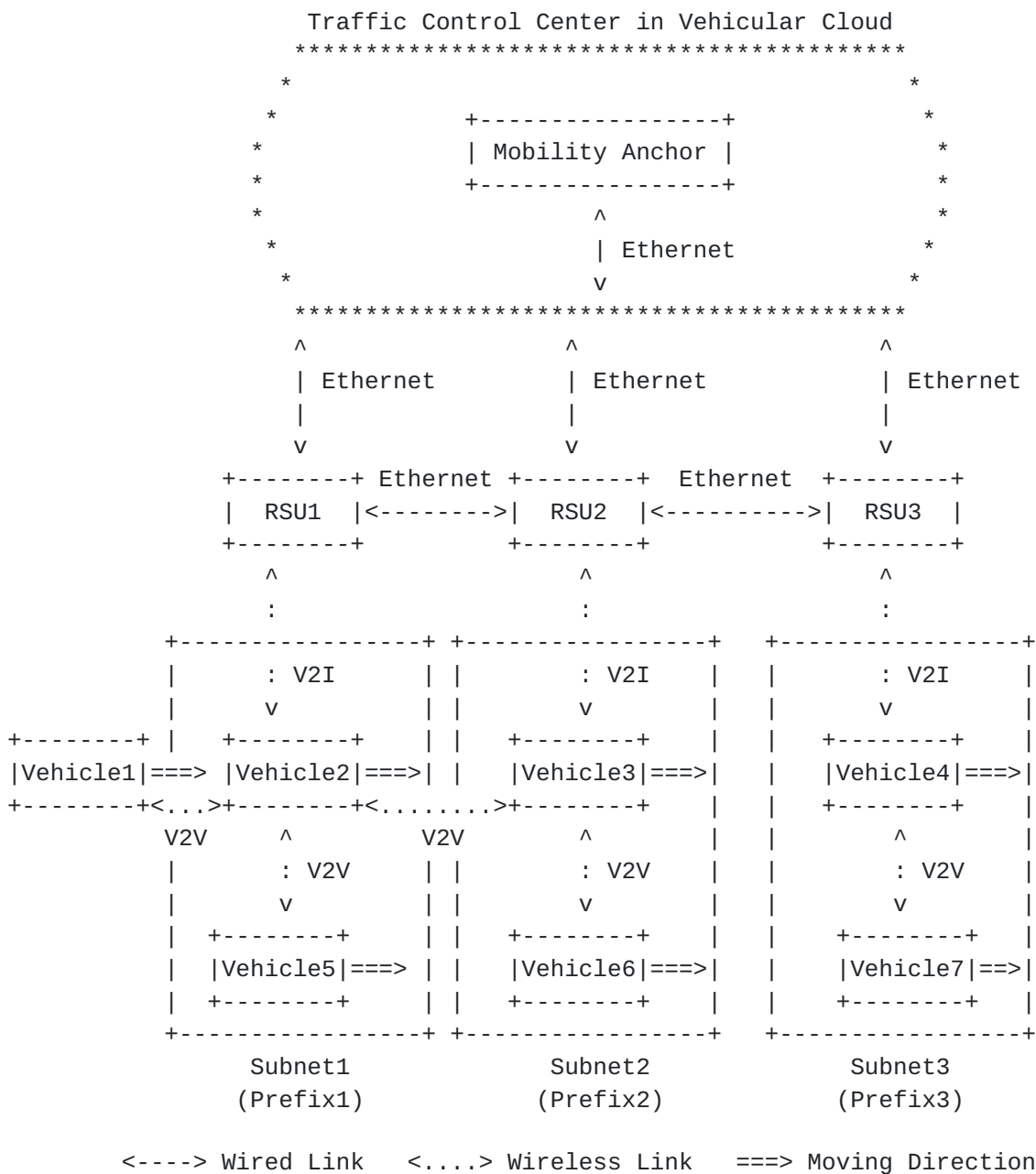


Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

4.1.1. Vehicular Network Architecture

Figure 1 shows an architecture for V2I and V2V networking in a road network. The vehicular network architecture contains vehicles, RSUs, Vehicular Cloud, Traffic Control Center, and Mobility Anchor as components. However, some components in the vehicular network architecture may not be needed for vehicular networking, such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor.

As shown in this figure, RSUs as routers and vehicles with OBU have wireless media interfaces for VANET. Furthermore, the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking. Note that 2001:DB8::/32 is a documentation prefix [RFC3849] for example prefixes in this document, and also that any routable IPv6 address needs to be routable in a VANET and a vehicular network including RSUs.

For IPv6 packets transported over IEEE 802.11-OCB, [IPv6-over-802.11-OCB] 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 Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC layer and IPv6 network layer, which is located between IEEE 802.11-OCB's logical link control layer and IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IP-based vehicular networks.

In Figure 1, three RSUs (RSU1, RSU2, and RSU3) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of RSUs and vehicles in the road network. A Mobility Anchor (MA) can be located in the TCC as its key component for the mobility management of vehicles. Vehicle2, Vehicle3, and Vehicle4 are wirelessly connected to RSU1, RSU2, and RSU3, respectively. The three wireless networks of RSU1, RSU2, and 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).

A single subnet prefix can span multiple vehicles in VANET. For example, in Figure 1, for Prefix 1, three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle5) can construct a connected VANET. Also, for Prefix 2, two vehicles (i.e., Vehicle3 and Vehicle6) can construct another connected VANET, and for Prefix 3, two vehicles (i.e., Vehicle4 and Vehicle7) can construct another connected VANET.

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 for each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., RSU2 and RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range for each other.

In vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications. In vehicular networks, the control plane can be separated from the data plane for efficient mobility management and data forwarding. The mobility information of a GPS receiver mounted in its vehicle (e.g., position, speed, and direction) can be used to accommodate mobility-aware proactive protocols. Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [[RFC6275](#)] and PMIPv6 [[RFC5213](#)], so the TCC maintains the mobility information of vehicles for location management. IP tunneling over the wireless link should be avoided for performance efficiency.

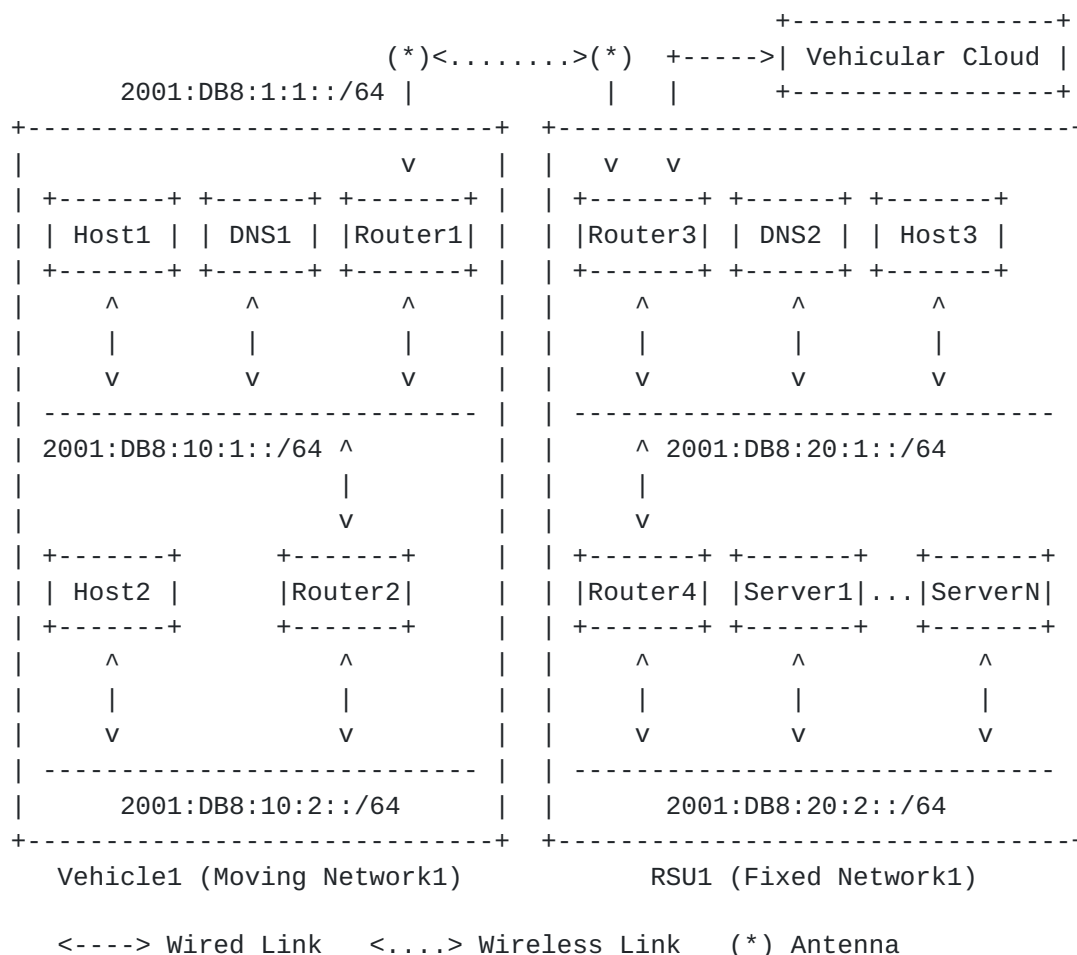


Figure 2: Internetworking between Vehicle Network and RSU Network

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle's internal network (i.e., moving network) and an RSU's internal network (i.e., fixed network) via V2I communication. Note that an RSU can accommodate multiple routers (or switches) and servers (e.g., DNS server and edge computing server) in its internal network as an edge computing system.

A vehicle's internal network often uses Ethernet to interconnect control units in the vehicle. The internal network also supports WiFi and Bluetooth to accommodate a driver's and passenger's mobile devices (e.g., smartphone or tablet). It is reasonable to consider the interaction between the internal network and an external network within another vehicle or RSU.

As shown in Figure 2, the vehicle's moving network and the RSU's fixed network are self-contained networks having multiple subnets and

having an edge router for the communication with another vehicle or RSU. Internetworking between two internal networks via V2I communication requires an exchange of network prefix and other parameters through a prefix discovery mechanism, such as ND-based prefix discovery [[ID-Vehicular-ND](#)]. For ND-based prefix discovery, network prefixes and parameters should be registered with a vehicle's router and an RSU router with an external network interface in advance.

For an IP communication between a vehicle and an RSU or between two neighboring vehicles, the network parameter discovery collects information relevant to the link layer, MAC layer, and IP layer. The link layer information includes wireless link layer parameters and transmission power level. The MAC layer information includes the MAC address of an external network interface for the internetworking with another vehicle or RSU. The IP layer information includes the IP address and prefix of an external network interface for the internetworking with another vehicle or RSU.

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle's moving network and the RSU's fixed network. A DNS service should be supported for the DNS name resolution of in-vehicle devices within a vehicle's internal network as well as for the DNS name resolution of those devices from a remote host in the Internet (e.g., a customer's web browser and an automotive service center system). The DNS names of in-vehicle devices and their service names can be registered with a DNS server in a vehicle or an RSU, as shown in Figure 2.

Figure 2 also shows internetworking between the vehicle's moving network and the RSU's fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Fixed Network1) inside RSU1. RSU1 has the DNS Server (DNS2), one host (Host3), the two routers (Router3 and Router4), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1's Router1 (a mobile router) and RSU1's Router3 (a fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2I networking. Thus, one host (Host1) in Vehicle1 can communicate with one server (Server1) in RSU1 for a vehicular service through Vehicle1's moving network, a wireless link between Vehicle1 and RSU1, and RSU1's fixed network.

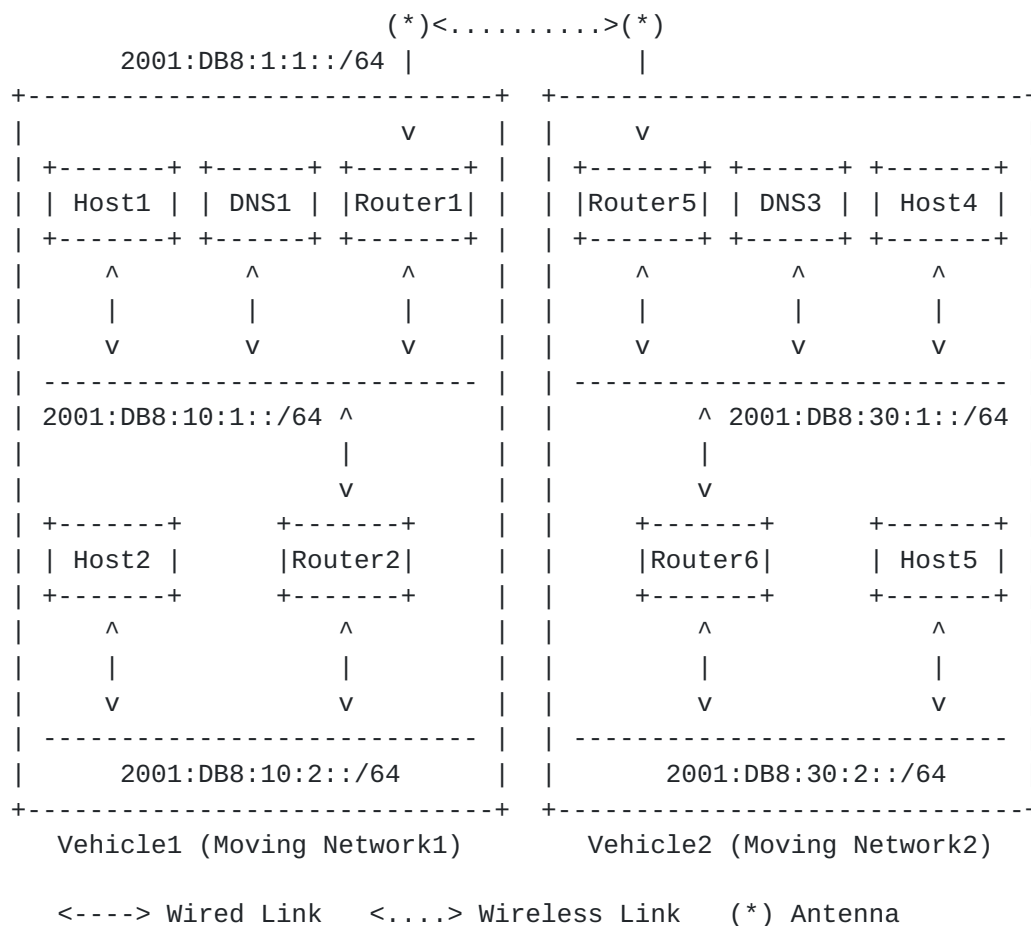


Figure 3: Internetworking between Two Vehicle Networks

4.3. V2V-based Internetworking

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

Figure 3 shows internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (DNS3), the two hosts (Host4 and Host5), and the two routers (Router5 and Router6). Vehicle1's Router1 (a mobile router) and Vehicle2's Router5 (a mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. Thus, one host (Host1) in Vehicle1 can communicate with one host (Host4) in Vehicle1 for a vehicular service through Vehicle1's moving network, a wireless link between Vehicle1 and Vehicle2, and Vehicle2's moving network.

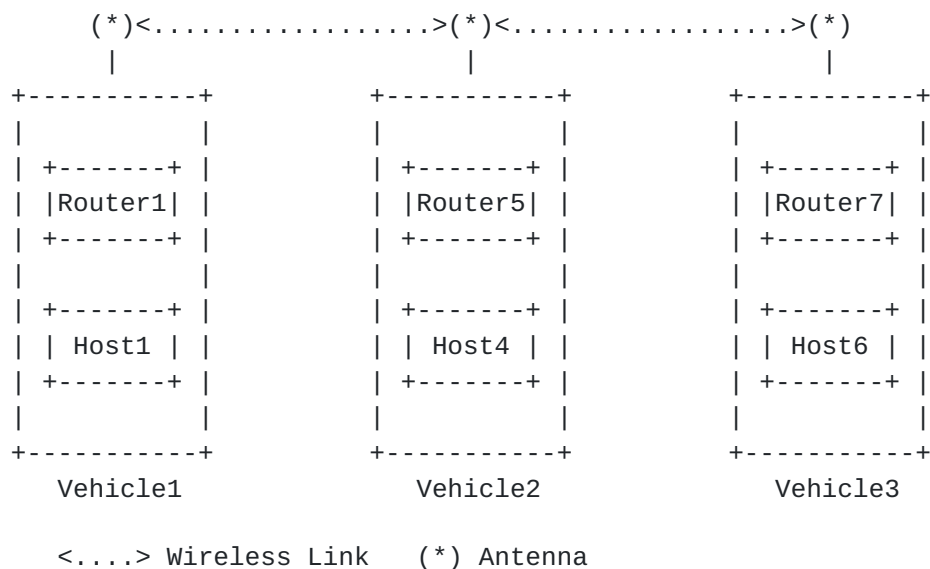


Figure 4: Multihop Internetworking between Two Vehicle Networks

Figure 4 shows multihop internetworking between the moving networks of two vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host6 in Vehicle3 via Router 5 in Vehicle2 that is an intermediate vehicle being connected to Vehicle1 and Vehicle3 in a linear topology as shown in the figure.

5. Problem Statement

In order to specify protocols using the abovementioned architecture for VANETs, 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 time relatively small compared to the lifetime of a link between a vehicle and an RSU, or between two vehicles. This has a major impact on IPv6 neighbor discovery. Mobility management 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 communications. Finally, and perhaps most importantly, proper authorization for vehicular protocol messages must be assured in order to prevent false reports of accidents or other mishaps on the road, which would cause horrific misery in modern urban environments. This section presents key topics such as neighbor discovery and mobility management.

5.1. Neighbor Discovery

IPv6 Neighbor Discovery (IPv6 ND) [[RFC4861](#)][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for point-to-point links and transit links (e.g., Ethernet). It assumes an efficient and reliable support of multicast from the link layer for various network operations such as MAC Address Resolution (AR) and Duplicate Address Detection (DAD).

DAD and ND-related parameters (e.g., Router Lifetime) need to be extended to vehicular networking (e.g., V2V, V2I, and V2X). Vehicles move quickly within the communication coverage of any particular vehicle or RSU. Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and run IPv6 ND.

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 frequently invalid in vehicular networks. The merging and partitioning of VANETs occurs frequently in vehicular networks. This merging and partitioning should be considered for the IPv6 Neighbor Discovery (e.g., SLAAC). Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. Also, SLAAC should be extended to prevent IPv6 address duplication due to the merging of VANETs. According to the merging and partitioning, a destination vehicle (as an IP host) should be distinguished as either an on-link host or off-link host even though the source vehicle uses the same prefix with the destination vehicle.

The vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD, and two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and 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. A vehicular infrastructure having RSUs and an MA can participate in the vehicular-network-wide DAD for the sake of vehicles [[RFC6775](#)]. For the vehicle as an IPv6 node, deriving a unique IPv6 address from a globally unique MAC address creates a privacy issue. Refer to [Section 6](#) for the discussion about such a privacy issue.

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval should be adjusted for high-speed vehicles and vehicle density. As vehicles move faster, the NA interval should decrease (e.g., from 1 sec to 0.5 sec) for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase (e.g., from 0.5 sec to 1 sec) for the NA messages to reduce collision probability with other NA messages.

According to a report from the National Highway Traffic Safety Administration (NHTSA) [[NHTSA-ACAS-Report](#)], an extra 0.5 second of warning time can prevent about 60% of the collisions of vehicles moving closely in a roadway. A warning message should be exchanged every 0.5 second. Thus, if the ND messages (e.g., NS and NA) are used as warning messages, they should be exchanged every 0.5 second.

For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. Implementations for such applications are not available yet. ND needs work to support IP-based safety applications.

5.1.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in a vehicular wireless link [[VIP-WAVE](#)] [[RFC5889](#)]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces [[RFC6250](#)]. However, interference and different levels of transmission power may cause asymmetric links to appear in vehicular wireless links. As a result, a new vehicular link model should 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 and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IP 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 multiple links between pairs of vehicles within 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 is assigned to VANETs in vehicular networks. Even though two vehicles in the same VANET

configure their IPv6 addresses with the same IPv6 prefix, they may not communicate with each other not in a one hop in the same VANET because of the multihop network connectivity. 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. When these two VANETs converge to one VANET, the two vehicles can communicate with each other in a multihop fashion.

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 an on-link prefix and off-link prefix according to the one-hop reachability among the vehicles in an appropriate way. If the vehicles with the same prefix are reachable with 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 with each other in one hop due to either the multi-hop topology in the VANET or multiple partitions, the prefix should be off-link.

The vehicular link model needs to support the multihop routing in a connected VANET where the vehicles with the same global-scope IPv6 prefix are connected in one hop or multiple hops. It also needs to support the multihop routing in multiple connected VANETs via an RSU that has the wireless connectivity with each VANET. 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 multi-hop V2V or multi-hop V2I2V. When two vehicles of Vehicle1 and Vehicle3 are connected in a VANET, it will be more efficient for them to communicate with each other via VANET rather than RSUs. On the other hand, when the two vehicles of Vehicle1 and Vehicle3 are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V. Thus, two separate VANETs can merge into one network via RSU(s). Also, newly arriving vehicles can merge two separate VANETs into one VANET if they can play a role of a relay node for those VANETs.

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 some extent of 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](#)]. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP) session with an IPv6 address pair. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

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 should be updated, and the uniqueness of the address should be performed through the DAD procedure. For vehicular networks with high mobility and density, this DAD should be performed efficiently with minimum overhead so that the vehicles can exchange warning messages with each other every 0.5 second [[NHTSA-ACAS-Report](#)].

For the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, with a mobility management scheme (e.g., MIPv6 and PMIPv6), the new IP address for the transport-layer session can be notified to an appropriate end point, and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address. This mobility management overhead for pseudonyms should be minimized for efficient operations in vehicular networks having lots of vehicles.

[5.1.3.](#) Routing

For multihop V2V communications in either a VANET or VANETs via RSUs, a vehicular ad hoc routing protocol (e.g., AODV and OLSRV2) 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 [[ID-Multicast-Problems](#)].

The merging of the IPv6 Neighbor Discovery and a VANET routing protocol allows the efficient wireless channel utilization. A routing protocol for VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in VANET with a dynamic network topology if the IPv6 ND is used to check the neighborhood of each vehicle, and can be extended to compute each vehicle's routing table in VANET.

Vehicular ND can be extended to accommodate routing functionality with a prefix discovery option. The ND extension can allow vehicles to exchange their prefixes in a multihop fashion [[ID-Vehicular-ND](#)]. With the exchanged prefixes, they can compute their routing table (or

IPv6 ND's neighbor cache) for the VANETs with a distance-vector algorithm [[Intro-to-Algorithms](#)].

5.2. Mobility Management

The seamless connectivity and timely data exchange between two end points requires an efficient mobility management including location management and handover. Most of vehicles are equipped with a GPS receiver as part of a dedicated navigation system or a corresponding smartphone App. The GPS receiver may not provide vehicles with accurate location information in adverse, local environments such as building area and tunnel. The location precision can be improved by the assistance from the RSUs or a cellular system with a GPS receiver for location information.

With a GPS navigator, an efficient mobility management will be possible by vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having RSUs and an MA in TCC) [[ID-Vehicular-MM](#)]. This vehicular infrastructure can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the 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 RSUs along with mobility information.

By predicting a vehicle's mobility, the vehicular infrastructure can better support RSUs to perform efficient DAD, data packet routing, 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 [[ID-Vehicular-MM](#)]. For example, when a vehicle is moving into the wireless link under another RSU belonging to a different subnet, the RSU can proactively perform the DAD for the sake of the vehicle, reducing IPv6 control traffic overhead in the wireless link. To prevent a hacker from impersonating RSUs as bogus RSUs, RSUs and MA in the vehicular infrastructure need to have secure channels via IPsec.

Therefore, with a proactive handover and a multihop DAD in vehicular networks, RSUs needs to efficiently forward data packets from the wired network (or the wireless network) to a moving destination vehicle along its trajectory.

6. Security Considerations

This section discusses security and privacy for IP-based vehicular networking. The security and privacy are one of key components in IP-based vehicular networking, such as neighbor discovery and mobility management, so they need to be analyzed in depth.

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe. Sybil attack, which tries to confuse a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. This sybil attack should be prevented through the cooperation between good vehicles and RSUs. Note that good vehicles are ones with valid certificates that are determined by the authentication process with an authentication server in the vehicular network. Applications on IP-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way. Even a perfectly authorized and legitimate vehicle may be hacked to run malicious applications to track and collect other vehicles' information. For this case, an attack mitigation process may be required to reduce the aftermath of the malicious behaviors.

A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., RSU) connected to an authentication server in TCC. Also, Transport Layer Security (TLS) certificates can be used for secure E2E vehicle communications.

For secure V2I communication, a secure channel between a mobile router in a vehicle and a fixed router in an RSU should be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym should be provided to the

vehicle; that is, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an RSU) in terms of transport layer for a long-living higher-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IP addresses, because an adversary can see the change of the MAC and IP addresses and track the vehicle with those addresses.

For the IPv6 ND, the vehicular-network-wide DAD is required for the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that makes the DAD-related ND packets are disseminated over the VANET and vehicular network including the RSUs and the MA. The vehicles and RSUs need to filter out suspicious ND traffic in advance.

For the mobility management, a malicious vehicle can construct multiple virtual bogus vehicles, and register them with the RSU and the MA. This registration makes the RSU and MA waste their resources. The RSU and MA need to determine whether a vehicle is genuine or bogus in the mobility management.

7. Informative References

[Automotive-Sensing]

Choi, J., Va, V., Gonzalez-Prelcic, N., Daniels, R., R. Bhat, C., and R. W. Heath, "Millimeter-Wave Vehicular Communication to Support Massive Automotive Sensing", IEEE Communications Magazine, December 2016.

[CA-Cruise-Control]

California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", [Online] Available: <http://www.path.berkeley.edu/research/automated-and-connected-vehicles/cooperative-adaptive-cruise-control>, 2017.

[CASD]

Shen, Y., Jeong, J., Oh, T., and S. Son, "CASD: A Framework of Context-Awareness Safety Driving in Vehicular Networks", International Workshop on Device Centric Cloud (DC2), March 2016.

- [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), October 2010.
- [EU-2008-671-EC] European Union, "Commission Decision of 5 August 2008 on the Harmonised Use of Radio Spectrum in the 5875 - 5905 MHz Frequency Band for Safety-related Applications of Intelligent Transport Systems (ITS)", EU 2008/671/EC, August 2008.
- [FirstNet] U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", [Online]
Available: <https://www.firstnet.gov/>, 2012.
- [FirstNet-Report] First Responder Network Authority, "FY 2017: ANNUAL REPORT TO CONGRESS, Advancing Public Safety Broadband Communications", FirstNet FY 2017, December 2017.
- [Fuel-Efficient] van de Hoef, S., H. Johansson, K., and D. V. Dimarogonas, "Fuel-Efficient En Route Formation of Truck Platoons", IEEE Transactions on Intelligent Transportation Systems, January 2018.
- [ID-Multicast-Problems] Perkins, C., McBride, M., Stanley, D., Kumari, W., and JC. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", [draft-ietf-mboned-ieee802-mcast-problems-06](#) (work in progress), July 2019.
- [ID-Vehicular-MM] Jeong, J., Ed., Shen, Y., and Z. Xiang, "Vehicular Mobility Management for IP-Based Vehicular Networks", [draft-jeong-ipwave-vehicular-mobility-management-01](#) (work in progress), July 2019.
- [ID-Vehicular-ND] Jeong, J., Ed., Shen, Y., and Z. Xiang, "Vehicular Neighbor Discovery for IP-Based Vehicular Networks", [draft-jeong-ipwave-vehicular-neighbor-discovery-07](#) (work in progress), July 2019.

[Identity-Management]

Wetterwald, M., Hrizi, F., and P. Cataldi, "Cross-layer Identities Management in ITS Stations", The 10th International Conference on ITS Telecommunications, November 2010.

[IEEE-802.11-OCB]

"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, December 2016.

[IEEE-802.11p]

"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 6: Wireless Access in Vehicular Environments", IEEE Std 802.11p-2010, June 2010.

[Intro-to-Algorithms]

H. Cormen, T., E. Leiserson, C., L. Rivest, R., and C. Stein, "Introduction to Algorithms, 3rd ed.", The MIT Press, July 2009.

[IPv6-over-802.11-OCB]

Benamar, N., Haerri, J., Lee, J., and T. Ernst, "Basic Support for IPv6 over IEEE Std 802.11 Networks Operating Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)", [draft-ietf-ipwave-ipv6-over-80211ocb-49](#) (work in progress), July 2019.

[ISO-ITS-IPv6]

ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012.

[NHTSA-ACAS-Report]

National Highway Traffic Safety Administration (NHTSA), "Final Report of Automotive Collision Avoidance Systems (ACAS) Program", DOT HS 809 080, August 2000.

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", [RFC 3561](#), July 2003.

[RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", [RFC 3849](#), July 2004.

- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", [RFC 4086](#), June 2005.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), September 2007.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](#), September 2007.
- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", [RFC 5213](#), August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", [RFC 5844](#), May 2010.
- [RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", [RFC 5889](#), September 2010.
- [RFC5944] Perkins, C., Ed., "IP Mobility Support in IPv4, Revised", [RFC 5944](#), November 2010.
- [RFC6250] Thaler, D., "Evolution of the IP Model", [RFC 6250](#), May 2011.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", [RFC 6275](#), July 2011.
- [RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 6775](#), November 2012.
- [RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", [RFC 7181](#), April 2014.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 8200](#), July 2017.

- [SAINT] Jeong, J., Jeong, H., Lee, E., Oh, T., and D. Du, "SAINT: Self-Adaptive Interactive Navigation Tool for Cloud-Based Vehicular Traffic Optimization", IEEE Transactions on Vehicular Technology, Vol. 65, No. 6, June 2016.
- [SAINTplus] Shen, Y., Lee, J., Jeong, H., Jeong, J., Lee, E., and D. Du, "SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization", IEEE Transactions on Intelligent Transportation Systems, June 2017.
- [SANA] Hwang, T. and J. Jeong, "SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks", Springer Lecture Notes in Computer Science (LNCS), Vol. 9502, December 2015.
- [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", IEEE 2015 International Conference on Computing, Networking and Communications (ICNC), February 2015.
- [Timing-Attack] Matte, C., Cunche, M., Rousseau, F., and M. Vanhoef, "Defeating MAC Address Randomization Through Timing Attacks", ACM the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '16), July 2016.
- [Truck-Platooning] California Partners for Advanced Transportation Technology (PATH), "Automated Truck Platooning", [Online] Available: <http://www.path.berkeley.edu/research/automated-and-connected-vehicles/truck-platooning>, 2017.
- [TS-23.285-3GPP] 3GPP, "Architecture Enhancements for V2X Services", 3GPP TS 23.285, June 2018.
- [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, vol. 14, no. 1, March 2013.

[WAVE-1609.0]

IEEE 1609 Working Group, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture", IEEE Std 1609.0-2013, March 2014.

[WAVE-1609.2]

IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", IEEE Std 1609.2-2016, March 2016.

[WAVE-1609.3]

IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services", IEEE Std 1609.3-2016, April 2016.

[WAVE-1609.4]

IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation", IEEE Std 1609.4-2016, March 2016.

Appendix A. Changes from [draft-ietf-ipwave-vehicular-networking-11](#)

The following changes are made from [draft-ietf-ipwave-vehicular-networking-11](#):

- o This version is revised based on the comments from Charlie Perkins and Sandra Cespedes.
- o In [Section 5](#), the problem statement is revised with easily identifiable problems.
- o In [Section 1](#), the description of GeoNetworking (GN) protocols (i.e., geographic routing) is removed because the GN protocols are not relevant to the IPWAVE's use cases.
- o In [Section 2](#), the terms of OCB, Context-Awareness, Platooning, and Class-Based Safety Plan are clarified.
- o In [Section 2](#), the definition of an RSU is revised so that it can accommodate multiple routers (or switches) and servers (including DNS server and edge computing server) as an edge computing system because the RSU is regularly a router or switch.
- o In [Section 4.1](#), a general vehicular network architecture is proposed for the problem statement along with Figure 1. This figure clarifies that a single subnet prefix can span multiple vehicles that construct a subnet. Also, some components in the vehicular network architecture may not be needed such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor.
- o In [Section 5.1.1](#), the motivation of a new link model as a vehicular link model is added. The "on-link" and "off-link" for prefixes are classified according to the subnet topology of VANET.
- o In [Section 5.1.1](#), the merging and partitioning of VANETs is described, and the requirements of the IPv6 ND are addressed for the merging and partitioning as a problem statement.
- o In [Section 5.1.2](#), a citation of [[Scrambler-Attack](#)], which uses the scrambler seed in the IEEE 802.11-OCB frames as fingerprint information, is added to show the insufficiency of the MAC address pseudonym for privacy.
- o In [Section 5.1](#), the subsection of Prefix Dissemination/Exchange is removed because the Prefix Dissemination/Exchange subsection discusses a solution rather than a problem or requirement.

- o In [Section 5.1.3](#), the motivation of merging the IPv6 ND and a VANET routing protocol is explained to improve wireless channel utilization by removing redundant neighbor information exchange.
- o The text of the problems and requirements of security and privacy in vehicular networks are moved to [Section 6](#).
- o In [Section 6](#), the compromise of a perfectly authorized and legitimate vehicle is described as a security problem to be considered.
- o In [Section 3.3](#), the description of Vehicle-to-Pedestrian (V2P) is concised to deliver the clear concept of the direct communication between a vehicle and a pedestrian.

[Appendix B](#). Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

This work was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2017-0-01633) supervised by the IITP (Institute for Information & communications Technology Promotion).

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).

[Appendix C](#). Contributors

This document is a group work of 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 Lozano (Universidad of Murcia), Richard Roy (MIT), Francois Simon (Pilot), Sri Gundavelli (Cisco), Erik Nordmark, Dirk von Hugo (Deutsche Telekom), and Pascal Thubert (Cisco). The authors sincerely appreciate their contributions.

The following are co-authors 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

Jerome Haerri
Communication Systems Department
EURECOM
Sophia-Antipolis
France

Phone: +33 4 93 00 81 34
EMail: jerome.haerri@eurecom.fr

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

Phone: +86 13911788933
EMail: max.ldap@alibaba-inc.com

Tae (Tom) Oh
Department of Information Sciences and Technologies
Rochester Institute of Technology
One Lomb Memorial Drive
Rochester, NY 14623-5603
USA

Phone: +1 585 475 7642
EMail: Tom.Oh@rit.edu

Charles E. Perkins
Futurewei Inc.

2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4586
EMail: charliep@computer.org

Alexandre Petrescu
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
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
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu
URI: <http://iotlab.skku.edu/people-chris-shen.php>

Michelle Wetterwald
FBConsulting
21, Route de Luxembourg
Wasserbillig, Luxembourg L-6633
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

Fax: +82 31 290 7996

EMail: pauljeong@skku.edu

URI: <http://iotlab.skku.edu/people-jaehoon-jeong.php>

