IPWAVE Working Group J. Jeong, Ed.
Internet-Draft Sungkyunkwan University
Intended status: Informational March 9, 2020
Expires: September 10, 2020

IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-14

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, it makes a problem statement about key aspects in IPv6-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document specifies requirements for IPv6-based vehicular networking.

Status of This Memo

Copyright Notice

Table of Contents

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 IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213]) 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 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, it makes a problem statement about key aspects in IPWAVE, namely, IPv6 Neighbor Discovery (ND), Mobility Management (MM), and Security & Privacy (SP). For each key aspect of the problem statement, this document specifies requirements for IPv6-based vehicular networking. 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:

- 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].

- 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].

- DMM: "Distributed Mobility Management" [RFC7333][RFC7429].

o Edge Computing (EC): It is the local computing near an access network (i.e., edge network) for the sake of vehicles and pedestrians.

o Edge Computing Device (ECD): It is a computing device (or server) for edge computing for the sake of vehicles and pedestrians.

o Edge Network (EN): In is an access network that has an IP-RSU for wireless communication with other vehicles having an IP-OBU and wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and MA). It may have a radio receiver of Global Positioning System (GPS) for its position recognition and the localization service for the sake of vehicles.

o IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle such as a car, bicycle, or similar. It has at least one IP interface that runs in mode OCB of 802.11 and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP]. See the definition of the term "OBU" in [RFC8691].

o IP-RSU: "IP Roadside Unit": 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. An IP-RSU communicates with the IP-OBU over an 802.11 wireless link operating in OCB mode. Also, it may have an IP interface that runs in C-V2X along with an "RSU" transceiver. 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 "RSU" in [RFC8691].

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 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 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.

o OCB: "Outside the Context of a Basic Service Set - BSS". It is a mode of operation in which a Station (STA) is not a member of a

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

o 802.11-OCB: It refers to the mode specified in IEEE Std 802.11-2016 [IEEE-802.11-OCB] when the MIB attribute dot11OCBActivited is 'true'.

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 Traffic Control Center (TCC): A node that maintains road infrastructure information (e.g., IP-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 IP-OBU for wireless communication with other vehicles and IP-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 V2D: "Vehicle to Device". It is the wireless communication between a vehicle and a device (e.g., IoT device).

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

o V2I2P: "Vehicle to Infrastructure to Pedestrian". It is the wireless communication between a vehicle and a pedestrian's mobile device (e.g., smartphone) via an infrastructure node (e.g., IP-RSU).

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

o VIP: "Vehicular Internet Protocol". It is an IPv6 extension for vehicular networks including V2V, V2I, and V2X.

o VMM: "Vehicular Mobility Management". It is an IPv6-based mobility management for vehicular networks.

o VND: "Vehicular Neighbor Discovery". It is an IPv6 ND extension for vehicular networks.

o VSP: "Vehicular Security and Privacy". It is an IPv6-based security and privacy for vehicular networks.

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).

Since IP is widely used among various computing devices in the Internet, it is expected that the use cases in this section need to work on top of IPv6 as the network layer protocol. Thus, the IPv6 for these use cases should be extended for vehicular IPv6 such that the IPv6 can support the functions of the network layer protocol such as Vehicular Neighbor Discovery (VND), Vehicular Mobility Management (VMM), and Vehicular Security and Privacy (VSP) in vehicular networks. 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. Refer to Section 5 for the problem statement of the requirements of the vehicular IPv6.

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.

The existing IPv6 protocol does not support wireless single-hop V2V communications as well as wireless multi-hop V2V communications. Thus, the IPv6 needs to be extended for both single-hop V2V communications and multi-hop V2V communications.

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.

To support the applications of these V2V use cases, the functions of IPv6 such as VND and VSP are prerequisite for the IPv6-based packet exchange and the secure, safe communication between two vehicles.

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.

The existing IPv6 protocol does not support wireless multi-hop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multi-hop data forwarding of intermediate vehicles. Thus, the IPv6 needs to be extended for multi-hop V2I communications.

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 IP-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.

To support the applications of these V2I use cases, the functions of IPv6 such as VND, VMM, and VSP are prerequisite for the IPv6-based packet exchange, the transport-layer session continuity, and the secure, safe communication between a vehicle and a server in the vehicular cloud.

3.3. V2X

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

The existing IPv6 protocol does not support wireless multi-hop V2X (or V2I2X) communications in an urban road network where RSUs are deployed at intersections, so a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an RSU through the multi-hop data forwarding of intermediate vehicles (or pedestrians' smartphones). Thus, the IPv6 needs to be extended for multi-hop V2X (or V2I2X) communications.

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 IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU. An edge computing device behind the IP-RSU can collect the mobility information from vehicles and pedestrians, 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 the communication with vehicles, considering their mobility.

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.

To support the applications of these V2X use cases, the functions of IPv6 such as VND, VMM, and VSP are prerequisite for the IPv6-based packet exchange, the transport-layer session continuity, and the secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU.

```
                     Traffic Control Center in Vehicular Cloud
                    *******************************************
+-------------+    *                                           *
|Corresponding|   *             +-----------------+             *
|    Node     |<->*             | Mobility Anchor |             *
+-------------+   *             +-----------------+             *
                  *                      ^                      *
                  *                      |                      *
                   *                     v                     *
                    *******************************************
                    ^                   ^                     ^
                    |                   |                     |
                    |                   |                     |
                    v                   v                     v
              +---------+           +---------+           +---------+
              | IP-RSU1 |<--------->| IP-RSU2 |<--------->| IP-RSU3 |
              +---------+           +---------+           +---------+
                  ^                     ^                    ^
                  :                     :                    :
           +-----------------+ +-----------------+   +-----------------+
           |      : V2I      | |        : V2I    |   |       : V2I     |
           |      v          | |        v        |   |       v         |
+--------+ |   +--------+    | |   +--------+    |   |   +--------+    |
|Vehicle1|===> |Vehicle2|===>| |   |Vehicle3|===>|   |   |Vehicle4|===>|
+--------+<...>+--------+<........>+--------+    |   |   +--------+    |
           V2V     ^         V2V        ^        |   |        ^        |
           |       : V2V     | |        : V2V    |   |        : V2V    |
           |       v         | |        v        |   |        v        |
           |  +--------+     | |   +--------+    |   |    +--------+   |
           |  |Vehicle5|===> | |   |Vehicle6|===>|   |    |Vehicle7|==>|
           |  +--------+     | |   +--------+    |   |    +--------+   |
           +-----------------+ +-----------------+   +-----------------+
                 Subnet1              Subnet2              Subnet3
                (Prefix1)            (Prefix2)            (Prefix3)

        <----> Wired Link   <....> Wireless Link   ===> Moving Direction
```

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

4. Vehicular Networks

This section describes an exemplary vehicular network architecture supporting V2V, V2I, and V2X communications in vehicular networks. It describes an internal network within a vehicle or an edge network (called EN). It 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.

4.1. Vehicular Network Architecture

Figure 1 shows an exemplary vehicular network architecture for V2I and V2V in a road network. The vehicular network architecture contains vehicles, IP-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 networks, such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor.

The existing, well-known architecture such as PMIPv6 [RFC5213] can be extended to a vehicular network architecture (as shown in Figure 1) such that it can support wireless multi-hop V2I, multi-hop V2V, and multi-hop V2X (or V2I2X).

As shown in this figure, IP-RSUs as routers and vehicles with IP-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 IP-RSUs.

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 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 IPv6-based vehicular networks.

In Figure 1, 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), which are part of a Vehicular Cloud. 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, which is a controller for the mobility management of vehicles. 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 RSU share a prefix such that mobile nodes share a prefix of a WiFi 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 Prefix 1 to configure their IPv6 global addresses for V2I communication.

A single subnet prefix announced by an RSU 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., IP-RSU2 and IP-RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range for each other.

An IPv6 mobility solution is needed in vehicular networks so that a vehicle's TCP session can be continued 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 with a corresponding 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]). In the host-based mobility scheme, an IP-RSU plays a role of a home agent in a visited network. On the other hand, in the network-based mobility scheme, an MA plays a role of a mobility management

controller such as a Local Mobility Anchor (LMA) in PMIPv6, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213].

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]. 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 can configure and monitor its IP-RSUs and vehicles for mobility management, location management, and security services as an SDN controller.

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 handover schemes, which can perform the handover of a vehicle according to its mobility and the wireless signal strength of a vehicle and an IP-RSU in a proactive way.

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. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.

```
                                                    +-----------------+
                           (*)<........>(*)  +----->| Vehicular Cloud |
          2001:DB8:1:1::/64 |            |   |      +-----------------+
   +------------------------------+  +---------------------------------+
   |                        v     |  |   v   v                         |
   | +-------+          +-------+ |  | +-------+          +-------+    |
   | | Host1 |          |IP-OBU1| |  | |IP-RSU1|          | Host3 |    |
   | +-------+          +-------+ |  | +-------+          +-------+    |
   |     ^                  ^     |  |     ^                  ^        |
   |     |                  |     |  |     |                  |        |
   |     v                  v     |  |     v                  v        |
   | ---------------------------- |  | ------------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |     ^ 2001:DB8:20:1::/64        |
   |                    |         |  |     |                           |
   |                    v         |  |     v                           |
   | +-------+      +-------+     |  | +-------+ +-------+   +-------+ |
   | | Host2 |      |Router1|     |  | |Router2| |Server1|...|ServerN| |
   | +-------+      +-------+     |  | +-------+ +-------+   +-------+ |
   |     ^              ^         |  |     ^         ^           ^     |
   |     |              |         |  |     |         |           |     |
   |     v              v         |  |     v         v           v     |
   | ---------------------------- |  | ------------------------------- |
   |      2001:DB8:10:2::/64      |  |       2001:DB8:20:2::/64        |
   +------------------------------+  +---------------------------------+
      Vehicle1 (Moving Network1)            EN1 (Fixed Network1)

      <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 2: Internetworking between Vehicle and Edge Network

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle's internal network (i.e., moving 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 WiFi 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 the interaction between the internal network and an external network within another vehicle or an EN.

As shown in Figure 2, as internal networks, a vehicle's moving 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 the communication with another vehicle or another EN. Internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the network prefixes of the internal networks.

Figure 2 also shows internetworking between the vehicle's moving network and the EN's fixed network. There exists an internal network (Moving 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 moving 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, 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 moving network and the EN's fixed network. Thus, V2I requires an efficient protocol for the mutual knowledge of network parameters.

```
                        (*)<..........>(*)
          2001:DB8:1:1::/64 |              |
   +------------------------------+  +------------------------------+
   |                        v     |  |     v                        |
   | +-------+          +-------+ |  | +-------+          +-------+ |
   | | Host1 |          |IP-OBU1| |  | |IP-OBU2|          | Host3 | |
   | +-------+          +-------+ |  | +-------+          +-------+ |
   |     ^                  ^     |  |     ^                  ^     |
   |     |                  |     |  |     |                  |     |
   |     v                  v     |  |     v                  v     |
   | ---------------------------- |  | ---------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |         ^ 2001:DB8:30:1::/64 |
   |                    |         |  |         |                    |
   |                    v         |  |         v                    |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   | | Host2 |      |Router1|     |  |     |Router2|      | Host4 | |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   |     ^              ^         |  |         ^              ^     |
   |     |              |         |  |         |              |     |
   |     v              v         |  |         v              v     |
   | ---------------------------- |  | ---------------------------- |
   |      2001:DB8:10:2::/64      |  |      2001:DB8:30:2::/64      |
   +------------------------------+  +------------------------------+
      Vehicle1 (Moving Network1)        Vehicle2 (Moving Network2)

      <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 3: Internetworking between Two Vehicles

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 two hosts (Host1 and Host2), and two routers (IP-OBU1 and Router1). There exists another internal network (Moving 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 moving network, a wireless link between IP-OBU1 and IP-OBU2, and Vehicle2's moving network.

```
        (*)<..................>(*)<..................>(*)
         |                      |                      |
   +-----------+          +-----------+          +-----------+
   |           |          |           |          |           |
   | +-------+ |          | +-------+ |          | +-------+ |
   | |IP-OBU1| |          | |IP-OBU2| |          | |IP-OBU3| |
   | +-------+ |          | +-------+ |          | +-------+ |
   |           |          |           |          |           |
   | +-------+ |          | +-------+ |          | +-------+ |
   | | Host1 | |          | | Host2 | |          | | Host3 | |
   | +-------+ |          | +-------+ |          | +-------+ |
   |           |          |           |          |           |
   +-----------+          +-----------+          +-----------+
      Vehicle1               Vehicle2               Vehicle3

      <....> Wireless Link   (*) Antenna
```

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 Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-OBU2 in Vehicle2, and IP-OBU3 in 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 IP-RSU, or between two vehicles. This 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 communications. Thus, this section presents key topics such as neighbor discovery and mobility management.

5.1. 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).

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 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 ND such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. 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 needs to prevent IPv6 address duplication due to the merging of VANETs. According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or an off-link host even though the source vehicle uses the same prefix with the destination vehicle.

To efficiently prevent the IPv6 address duplication due to the VANET partitioning and merging from happing 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.

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 neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles.

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. Implementations for such applications are not available yet. IPv6 ND needs to efficiently work to support IPv6-based safety applications.

5.1.1. Link Model

A prefix model for a vehicular network needs to facilitate the 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 prefix 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.

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, radio 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 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 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 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 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 between them. 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, for example, wheh 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 an on-link prefix and off-link prefix 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 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 multihop 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 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 the two vehicles of Vehicle1 and Vehicle3 are connected in a VANET, it will be more efficient for them to directly communicate with each other via VANET rather than indirectly via IP-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 IP-RSUs, they can communicate with each other through the relay of IP-RSUs via V2I2V. Thus, two separate VANETs can merge into one network via IP-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 and and SCTP) 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 needs to be updated, and the uniqueness of the address needs to be checked through the DAD procedure. For vehicular networks with high mobility and density, this DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange application messages (e.g., collision avoidance and accident notification) with each other with a short interval (e.g., 0.5 second) [NHTSA-ACAS-Report].

5.1.3. Routing

For multihop V2V communications in either a VANET or VANETs via IP-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].

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 because the IPv6 ND is used to check the neighborhood of each vehicle. Thus, the vehicular routing needs to take advantage of the IPv6 ND to minimize its control overhead.

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. Note that The GPS receiver may not provide vehicles with accurate location information in adverse environments such as a building area and tunnel. The location precision can be improved by the assistance from the IP-RSUs or a cellular system with a GPS receiver for location information.

With a GPS navigator, an 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 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 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.

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.

6. Security Considerations

This section discusses security and privacy for IPv6-based vehicular networking. The security and privacy is one of key components in IPv6-based vehicular networking along with neighbor discovery and mobility management.

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

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. For example, Sybil attack, which tries to confuse a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. This sybil attack needs to be prevented through the

cooperation between good vehicles and IP-RSUs. Note that good vehicles are ones with valid certificates that are determined by the authentication process with an authentication server in the vehicular cloud. However, applications on IPv6-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.

To identify the genuineness of vehicles against malicious vehicles, an authentication method is required. 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., IP-RSU) connected to an authentication server in the vehicular cloud. Also, Transport Layer Security (TLS) certificates can be used for the vehicle authentication to allow secure E2E vehicle communications. To identify the genuineness of vehicles against malicious vehicles, an authentication method is required. For vehicle authentication, information available from a vehicle or a driver (e.g., Vehicle Identification Number (VIN) and Transport Layer Security (TLS) certificate [RFC8446]) needs to be used to efficiently authenticate a vehicle or a user with the help of a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the vehicular cloud.

For secure V2I communication, a secure channel 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. Also, for secure V2V communication, a secure channel 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.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym needs to be provided to the vehicle; that is, each vehicle periodically updates its MAC address and the corresponding IPv6 address [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 IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality, 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.

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

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-11 (work in progress), December 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.

[In-Car-Network]
Lim, H., Volker, L., and D. Herrscher, "Challenges in a Future IP/Ethernet-based In-Car Network for Real-Time Applications", ACM/EDAC/IEEE Design Automation Conference (DAC), June 2011.

[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.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[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.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 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.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, March 2014.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, April 2014.

[RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

[RFC7429] Liu, D., Zuniga, JC., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, January 2015.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 8200, July 2017.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018.

[RFC8691] Benamar, N., Haerri, 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, December 2019.

[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.

[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-13

The following changes are made from draft-ietf-ipwave-vehicular-networking-13:

- This version is revised based on the comments from Carlos Bernardos.

- The definition of Mobility Anchor (MA) is clarified with a reference to PMIPv6.

- In Vehicular Neighbor Discovery, Vehicular Mobility Management, and Vehicular Security and Privacy, the prefix of "Vehicular" is explained to represent extensions of the existing protocols rather than new "vehicular-specific" functions.

- In Section 4.1, an exemplary vehicular network architecture is explained as an extension of the existing network architecture of PMIPv6 for multi-hop V2V, V2I, and V2X (or V2I2X).

- For the IPv6 communication between an IP-OBU and an IP-RSU or between two neighboring IP-OBUs, the requirements of knowing the network parameters are addressed rather than the network parameter sharing as a solution.

- In Figure 1, the prefix sharing of multiple vehicles under an RSU is explained such that it is the same as the prefix sharing in a WiFi LAN.

- The separation of the control plane and data plane is explained by referring to the concept of SDN and the relationship between the SDN controller and forwarding elements.

- In Figure 2, the topology of a vehicle's internal network is justified with the reference to a real car network [In-Car-Network].

- The discussion on ND timers is modified, focusing on a problem rather than a solution.

Appendix B. Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant 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 (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 Lozanoi (Universidad of Murcia), Richard Roy (MIT), Francois Simon (Pilot), Sri Gundavelli (Cisco), Erik Nordmark, Dirk von Hugo (Deutsche Telekom), Pascal Thubert (Cisco), Carlos Bernardos (UC3M), Russ Housley (Vigil Security), and Suresh Krishnan (Kaloom). 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.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
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