             IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem
                            Statement and Use Cases
                 draft-ietf-ipwave-vehicular-networking-16

Abstract

   This document discusses the problem statement and use cases of
   IPv6-based vehicular networking for Intelligent Transportation
   Systems (ITS). The main scenarios of vehicular communications are
   vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and
   vehicle-to-everything (V2X) communications. First, this document
   explains use cases using V2V, V2I, and V2X networking. Next, for
   IPv6-based vehicular networks, it makes a gap analysis of current
   IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management,
   and Security & Privacy), and then lists up requirements for the
   extensions of those IPv6 protocols for IPv6-based vehicular
   networking.

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 standard 802.11 (commonly known as Wi-Fi) to enable safe driving services based on DSRC for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC 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].

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

Along with these WAVE standards and C-V2X standards, regardless of a wireless access technology under the IP stack of a vehicle, vehicular networks can operate IP mobility with IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Locator/ ID Separation Protocol (LISP) [RFC6830BIS], and Asymmetric Extended Route Optimization (AERO) [RFC6706BIS]). In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6] [ISO-ITS-IPv6-AMD1].

This document describes use cases and a problem statement about IPv6-based vehicular networking for ITS, which is named IPv6 Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, for IPv6-based vehicular networks, it makes a gap analysis of current

IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then lists up requirements for the extensions of those IPv6 protocols, which are tailored to IPv6-based vehicular networking. Thus, this document is intended to motivate development of key protocols for IPWAVE.

2. Terminology

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

   o Class-Based Safety Plan: A vehicle can make a 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 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): It 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 Global Positioning
      System (GPS) radio receiver 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 (e.g., car, bicycle, autobike,

motor cycle, and a similar one) and a device (e.g., smartphone and
IoT device). It has at least one IP interface that runs in IEEE
802.11-OCB and has an "OBU" transceiver. Also, it may have an IP
interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP]
[TR-22.886-3GPP][TS-23.287-3GPP]. 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
      follow the leading vehicle [Truck-Platooning].

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

   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 GPS radio navigation receiver for efficient navigation. Any
      device having an IP-OBU and a GPS receiver (e.g., smartphone and
      table PC) can be regarded as a vehicle in this document.

   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 V2D: "Vehicle to Device". It is the wireless communication
      between a vehicle and a device (e.g., smartphone and IoT device).

   o V2I2D: "Vehicle to Infrastructure to Device". It is the wireless
      communication between a vehicle and a device (e.g., smartphone and
      IoT device) 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 V2I2X: "Vehicle to Infrastructure to Everything". It is the
      wireless communication between a vehicle and another entity (e.g.,
      vehicle, smartphone, and IoT device) via an infrastructure node
      (e.g., IP-RSU).

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

   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).

   IP is widely used among popular end-user devices (e.g., smartphone
   and tablet) in the Internet. Applications (e.g., navigator
   application) for those devices can be extended such that the V2V use

   cases in this section can work with IPv6 as a network layer protocol
   and IEEE 802.11-OCB as a link layer protocol. In addition, IPv6
   security needs to be extended to support those V2V use cases in a
   safe, secure, privacy-preserving way.

   The use cases presented in this section serve as the description and
   motivation for the need to extend IPv6 and its protocols to
   facilitate "Vehicular IPv6". Section 5 summarizes the overall

problem statement and IPv6 requirements. Note that the adjective
"Vehicular" in this document is used to represent extensions of
existing protocols such as IPv6 Neighbor Discovery, IPv6 Mobility
Management (e.g., PMIPv6 [RFC5213] and DMM [RFC7429]), and IPv6
Security and Privacy Mechanisms rather than new "vehicular-specific"
functions. Refer to Section 5 for the problem statement of the
requirements of vehicular IPv6.

3.1. V2V

The use cases of V2V networking discussed in this section include

o Context-aware navigation for safe driving and collision avoidance;

o Cooperative adaptive cruise control in a roadway;

o Platooning in a highway;

o Cooperative environment sensing;

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

These five techniques will be important elements for autonomous
vehicles, which may be either terrestrial vehicles or UAM end
systems.

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers
to drive safely by alerting them to dangerous obstacles and
situations. That is, a CASD navigator displays obstacles or
neighboring vehicles relevant to possible collisions in real-time
through V2V networking. CASD provides vehicles with a class-based
automatic safety action plan, 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
individual 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
a collision.

Platooning [Truck-Platooning] allows a series (or group) 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 (e.g., air pollution, hazards/
obstacles, slippery areas by snow or rain, road accidents, traffic
congestion, and driving behaviors of neighboring vehicles) from
various vehicle-mounted sensors, such as radars, LiDARs, and cameras,
with other vehicles and pedestrians. [Automotive-Sensing] introduces
millimeter-wave vehicular communication for massive automotive
sensing. A lot of data can be generated by those sensors, and these
data typically need to be routed to different destinations. In
addition, from the perspective of driverless vehicles, it is expected
that driverless vehicles can be mixed with driver-operated vehicles.
Through cooperative environment sensing, driver-operated vehicles can
use environmental information sensed by driverless vehicles for
better interaction with the other vehicles and environment. Vehicles
can also share their intended maneuvering information (e.g., lane
change, speed change, ramp in-and-out, cut-in, and abrupt braking)
with neighboring vehicles. Thus, this information sharing can help
the vehicles behave as more efficient traffic flows and minimize
unnecessary acceleration and deceleration to achieve the best ride
comfort.

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

To encourage more vehicles to participate in this cooperative
environmental sensing, a reward system will be needed. Sensing
activities of each vehicle need to be logged in either a central way
through a logging server (e.g., TCC) in the vehicular cloud or a
distributed way (e.g., blockchain [Bitcoin]) through other vehicles
or infrastructure. In the case of a blockchain, each sensing message
from a vehicle can be treated as a transaction and the neighboring
vehicles can play the role of peers in a consensus method of a
blockchain [Bitcoin][Vehicular-BlockChain].

The existing IPv6 protocol does not support wireless single-hop V2V
communications as well as wireless multihop V2V communications.
Thus, the IPv6 needs to support both single-hop and multihop
communications in a wireless medium so that vehicles can communicate
with each other by V2V communications to share either an emergency
situation or road hazard in a highway.

To support applications of these V2V use cases, the functions of IPv6
such as VND and VSP are prerequisites for IPv6-based packet exchange
and 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;

o Electric vehicle (EV) charging service;

o UAM navigation service with efficient battery charging.

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

Either a TCC or an ECD can recommend an energy-efficient speed to a
vehicle that depends on its traffic environment and traffic signal

scheduling [SignalGuru]. For example, when a vehicle approaches an
intersection area and a red traffic light for the vehicle becomes

turned on, it needs to reduce its speed to save fuel consumption. In
this case, either a TCC or an ECD, which has the up-to-date
trajectory of the vehicle and the traffic light schedule, can notify
the vehicle of an appropriate speed for fuel efficiency.
[Fuel-Efficient] studies fuel-efficient route and speed plans for
platooned trucks.

The emergency communication between accident vehicles (or emergency
vehicles) and a 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
using 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 the near future.

An EV charging service with V2I can facilitates the efficient battery
charging of EVs. In the case where an EV charging station is
connected to an IP-RSU, an EV can be guided toward the deck of the EV
charging station through a battery charging server connected to the
IP-RSU. In addition to this EV charging service, other value-added
services (e.g., air firmware/software update and media streaming) can
be provided to an EV while it is charging its battery at the EV
charging station.

A UAM navigation service with efficient battery charging can make the
battery charging schedule of UAM end systems (e.g., drone) for long-
distance flying [CBDN]. For this battery charging schedule, a UAM
end system can communicate with an infrastructure node (e.g., IP-RSU)
toward a cloud server via V2I communications. This cloud server can
coordinate the battery charging schedules of multiple UAM end systems
for their efficient navigation path, considering flight time from
their current position to a battery charging station, waiting time in
a waiting queue at the station, and battery charging time at the

station.

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

To support applications of these V2I use cases, the functions of IPv6 such as VND, VMM, and VSP are prerequisites for IPv6-based packet exchange, transport-layer session continuity, and 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 for a 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., Wi-Fi) 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.

The existing IPv6 protocol does not support wireless multihop 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 multihop data forwarding of intermediate vehicles (or pedestrians'

smartphones). Thus, IPv6 needs to be extended for multihop V2X (or
    V2I2X) communications.

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

4. Vehicular Networks

    This section describes an example 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

Jeong, Ed.   Expires January 8, 2021   [Page 11]

    the internetworking between the internal networks of two vehicles via
    wireless links.

```
                    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 Example Vehicular Network Architecture for V2I and V2V
```

4.1. Vehicular Network Architecture

   Figure 1 shows an example vehicular network architecture for V2I and
   V2V in a road network [OMNI-Interface]. The vehicular network
   architecture contains vehicles (including IP-OBU), IP-RSUs, Mobility
   Anchor, Traffic Control Center, and Vehicular Cloud as components.

   Note that the components of the vehicular network architecture can be
   mapped to those of an IP-based aeronautical network architecture in
   [OMNI-Interface], as shown in Figure 2.

```
        +------------------+------------------------------------+
        | Vehicular Network | Aeronautical Network              |
        +==================+====================================+
        | IP-RSU            | Access Router (AR)                 |
        +------------------+------------------------------------+
        | Vehicle (IP-OBU) | Mobile Node (MN)                   |
        +------------------+------------------------------------+
        | Moving Network    | End User Network (EUN)            |
        +------------------+------------------------------------+
        | Mobility Anchor   | Mobility Service Endpoint (MSE)   |
        +------------------+------------------------------------+
        | Vehicular Cloud   | Internetwork (INET) Routing System |
        +------------------+------------------------------------+
```
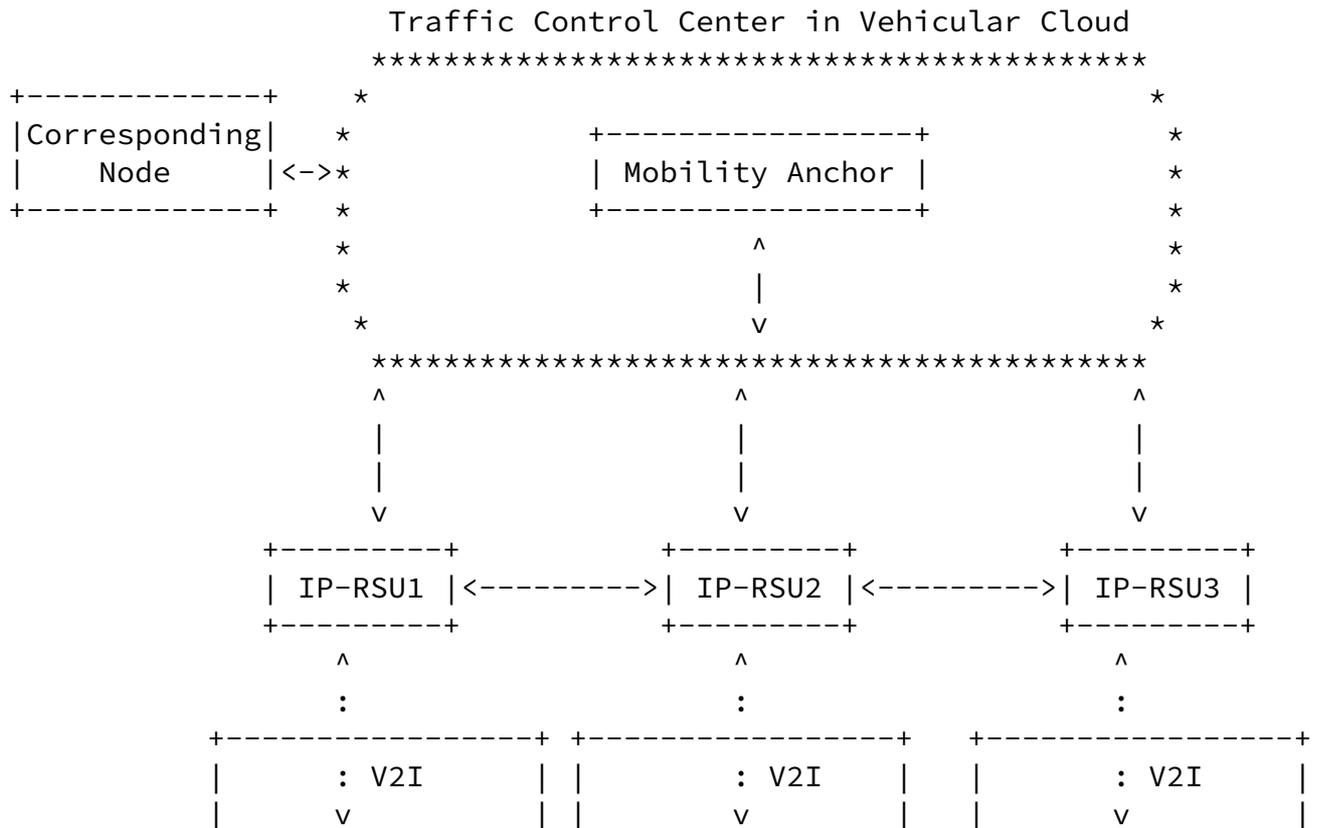
Figure 2: Mapping between Vehicular Network Components and
Aeronautical Network Components

These components are not mandatory, and they can be deployed into
vehicular networks in various ways. Some of them (e.g., Mobility
Anchor, Traffic Control Center, and Vehicular Cloud) may not be
needed for the vehicular networks according to target use cases in
Section 3.

An existing network architecture (e.g., an IP-based aeronautical
network architecture [OMNI-Interface][UAM-ITS], a network
architecture of PMIPv6 [RFC5213], and a low-power and lossy network
architecture [RFC6550]) can be extended to a vehicular network
architecture for multihop V2V, V2I, and V2X, as shown in Figure 1.
In a highway scenario, a vehicle may not access an RSU directly
because of the distance of the DSRC coverage (up to 1 km). For
example, RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks)
[RFC6550] can be extended to support a multihop V2I since a vehicle
can take advantage of other vehicles as relay nodes to reach the RSU.
Also, RPL can be extended to support both multihop V2V and V2X in the
similar way.

Wireless communications needs to be considered for end systems for
Urban Air Mobility (UAM) such as flying cars and taxis [UAM-ITS].
These UAM end systems may have multiple wireless transmission media
interfaces (e.g., cellular, communications satellite (SATCOM), short-
range omni-directional interfaces), which are offered by different
data link service providers. To support not only the mobility
management of the UAM end systems, but also the multihop and
multilink communications of the UAM interfaces, the UAM end systems

can employ an Overlay Multilink Network (OMNI) interface
[OMNI-Interface] as a virtual Non-Broadcast Multiple Access (NBMA)
connection to a serving ground domain infrastructure. This
infrastructure can be configured over the underlying data links. The
OMNI interface and its link model provide a means of multilink,
multihop and mobility coordination to the legacy IPv6 ND messaging
[RFC4861] according to the NBMA principle. Thus, the OMNI link model
can support efficient UAM internetworking services without additional
mobility messaging, and without any modification to the IPv6 ND
messaging services or link model.

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.

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). A Traffic Control
Center (TCC) is connected to the Vehicular Cloud for the management
of IP-RSUs and vehicles in the road network. A Mobility Anchor (MA)
may be located in the TCC as a mobility management controller.
Vehicle2, Vehicle3, and Vehicle4 are wirelessly connected to IP-RSU1,
IP-RSU2, and IP-RSU3, respectively. The three wireless networks of
IP-RSU1, IP-RSU2, and IP-RSU3 can belong to three different subnets
(i.e., Subnet1, Subnet2, and Subnet3), respectively. Those three
subnets use three different prefixes (i.e., Prefix1, Prefix2, and
Prefix3).

Multiple vehicles under the coverage of an RSU share a prefix such
that mobile nodes share a prefix of a Wi-Fi access point in a
wireless LAN. This is a natural characteristic in infrastructure-
based wireless networks. For example, in Figure 1, two vehicles
(i.e., Vehicle2, and Vehicle5) can use 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 of each other. On the other hand, Vehicle3 can communicate
with Vehicle4 via the vehicular infrastructure (i.e., IP-RSU2 and IP-
RSU3) by employing V2I (i.e., V2I2V) communication because they are
not within the wireless communication range of each other.

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 the IEEE 802.11 MAC layer and the IPv6 network
layer, which is located between the IEEE 802.11-OCB's logical link
control layer and the IPv6 network layer. This IPv6 over 802.11-OCB
can be used for both V2V and V2I in IPv6-based vehicular networks.

An IPv6 mobility solution is needed for the guarantee of
communication continuity in vehicular networks so that a vehicle's
TCP session can be continued, or UDP packets can be delivered to a
vehicle as a destination without loss while it moves from an IP-RSU's
wireless coverage to another IP-RSU's wireless coverage. In
Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session)
with a 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 (e.g., MIPv6), an IP-RSU plays a
role of a home agent. On the other hand, in the network-based
mobility scheme (e.g., PMIPv6, an MA plays a role of a mobility
management controller such as a Local Mobility Anchor (LMA) in
PMIPv6, which also serves vehicles as a home agent, and an IP-RSU
plays a role of an access router such as a Mobile Access Gateway
(MAG) in PMIPv6 [RFC5213]. The host-based mobility scheme needs
client functionality in IPv6 stack of a vehicle as a mobile node for
mobility signaling message exchange between the vehicle and home
agent. On the other hand, the network-based mobility scheme does not
need such a client functionality for a vehicle because the network
infrastructure node (e.g., MAG in PMIPv6) as a proxy mobility agent
handles the mobility signaling message exchange with the home agent
(e.g., LMA in PMIPv6) for the sake of the vehicle.

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

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

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 (or an MA inside 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.
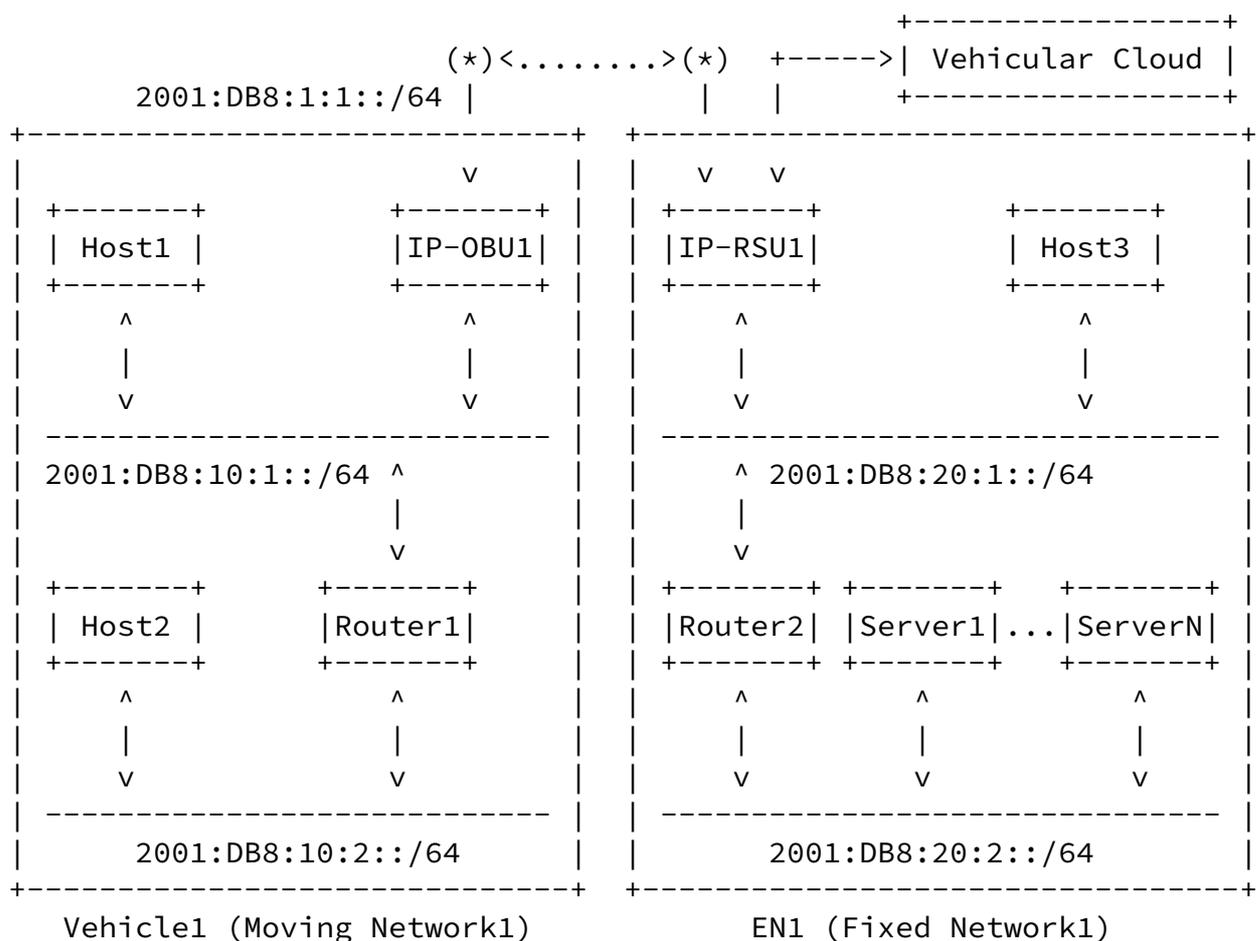
4.2. V2I-based Internetworking

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 Wi-Fi and Bluetooth to accommodate a driver's and
passenger's mobile devices (e.g., smartphone or tablet). The network
topology and subnetting depend on each vendor's network configuration
for a vehicle and an EN. It is reasonable to consider the
interaction between the internal network and an external network
within another vehicle or an EN.

```
                                                   +----------------+
                             (*)<........>(*)  +----->| 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 3: Internetworking between Vehicle and Edge Network

    As shown in Figure 3, 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. The

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

    Figure 3 also shows the 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-
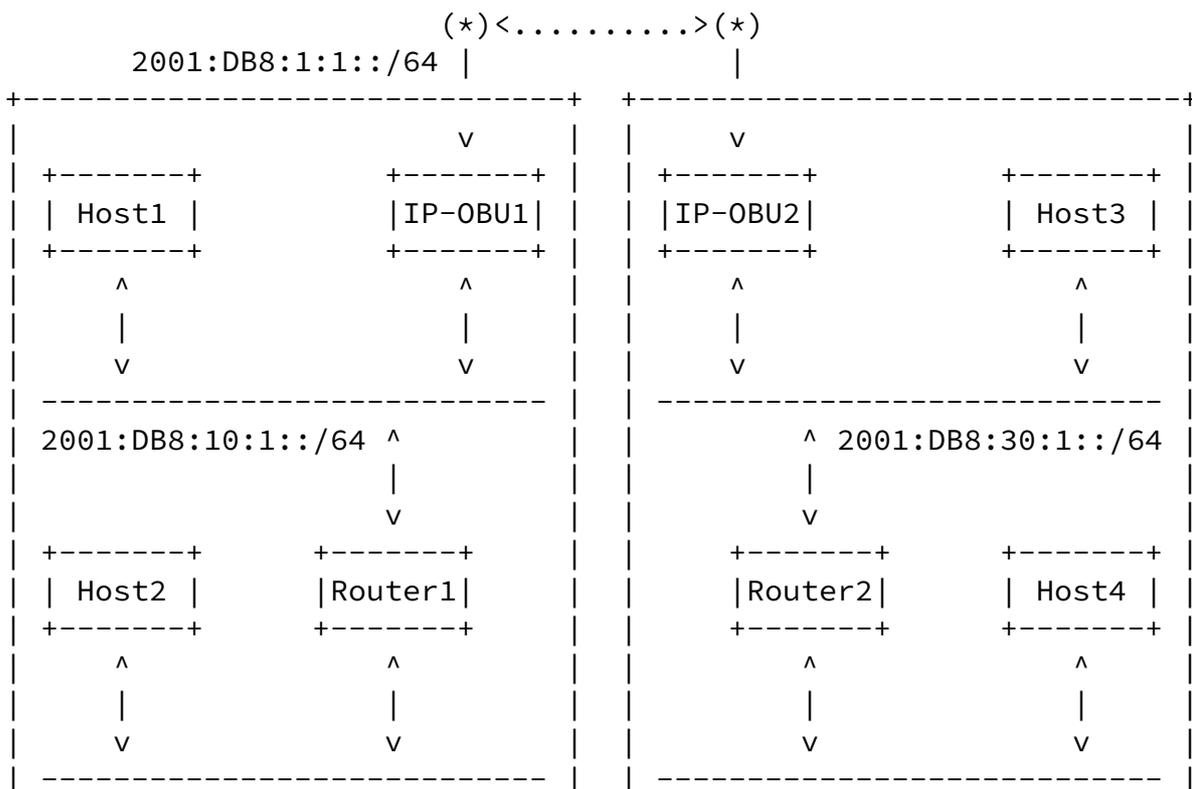   RSU1, and EN1's fixed network.

    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, and the MAC address of an external network interface for
    the internetworking with another IP-OBU or IP-RSU. The IPv6 layer
    information includes the IPv6 address and network prefix of an
    external network interface for the internetworking with another IP-
    OBU or IP-RSU.

Through the mutual knowledge of the network parameters of internal
networks, packets can be transmitted between the vehicle's moving
network and the EN's fixed network. Thus, V2I requires an efficient
protocol for the mutual knowledge of network parameters.

As shown in Figure 3, global IPv6 addresses are used for the wireless
link interfaces for IP-OBU and IP-RSU, but IPv6 Unique Local
Addresses (ULAs) [RFC4193] can also be used for those wireless link
interfaces as long as IPv6 packets can be routed to them in the
vehicular networks [OMNI-Interface]. For the guarantee of the
uniqueness of an IPv6 address, the configuration and control overhead
of the DAD of the wireless link interfaces should be minimized to
support the V2I and V2X communications of vehicles moving fast along
roadways.

4.3. V2V-based Internetworking

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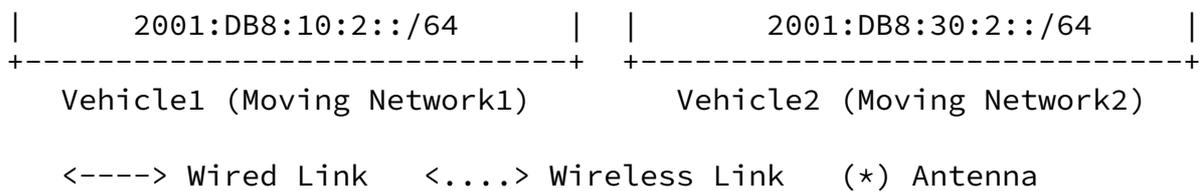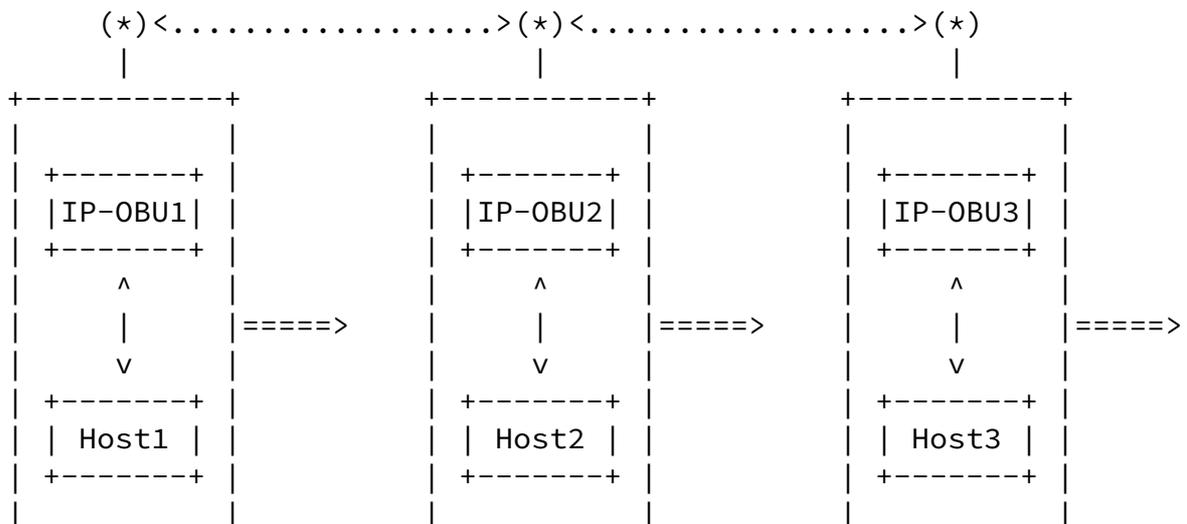   networks of two neighboring vehicles via V2V communication.

```
                            (*)<..........>(*)
           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 4: Internetworking between Two Vehicles
```

Figure 4 shows the 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.

As a V2V use case in Section 3.1, Figure 5 shows the linear network
topology of platooning vehicles for V2V communications where Vehicle3
is the leading vehicle with a driver, and Vehicle2 and Vehicle1 are
the following vehicles without drivers.

```
        (*)<..................>(*)<..................>(*)
         |                      |                      |
   +----------+           +----------+           +----------+
   |          |           |          |           |          |
   | +------+ |           | +------+ |           | +------+ |
   | |IP-OBU1| |          | |IP-OBU2| |          | |IP-OBU3| |
   | +------+ |           | +------+ |           | +------+ |
   |    ^     |           |    ^     |           |    ^     |
   |    |     |=====>     |    |     |=====>     |    |     |=====>
   |    v     |           |    v     |           |    v     |
   | +------+ |           | +------+ |           | +------+ |
   | | Host1 | |          | | Host2 | |          | | Host3 | |
   | +------+ |           | +------+ |           | +------+ |
   |          |           |          |           |          |
```

```
+----------+          +----------+          +----------+
   Vehicle1              Vehicle2              Vehicle3

 <----> Wired Link   <....> Wireless Link   ===> Moving Direction
 (*) Antenna
```
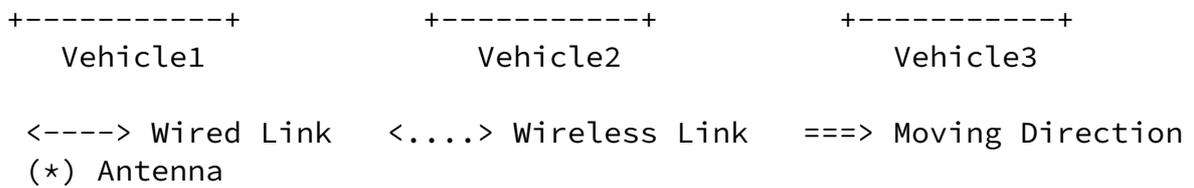
   Figure 5: Multihop Internetworking between Two Vehicle Networks

   As shown in Figure 5, multihop internetworking is feasible among the
   moving networks of three vehicles in the same VANET. For example,
   Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1
   in Vehicle1, IP-OBU2 in Vehicle2, and IP-OBU3 in Vehicle3 in the
   linear network, as shown in the figure.

5. Problem Statement

   In order to specify protocols using the architecture mentioned in
   [Section 4.1](), IPv6 core protocols have to be adapted to overcome
   certain challenging aspects of vehicular networking. Since the
   vehicles are likely to be moving at great speed, protocol exchanges
   need to be completed in a time relatively short compared to the
   lifetime of a link between a vehicle and an IP-RSU, or between two
   vehicles.

   Note that if two vehicles are moving in the opposite directions in a
   roadway, the relative speed of this case is two times the relative
   speed of a vehicle passing through an RSU. The time constraint of a
   wireless link between two nodes needs to be considered because it may
   affect the lifetime of a session involving the link.

   The lifetime of a session varies depending on the session's type such
   as a web surfing, voice call over IP, and DNS query. Regardless of a
   session's type, to guide all the IPv6 packets to their destination
   host, IP mobility should be supported for the session.

   Thus, the time constraint of a wireless link has a major impact on
   IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also
   vulnerable to disconnections that occur before the completion of
   identity verification and tunnel management. This is especially true
   given the unreliable nature of wireless communication. This section
   presents key topics such as neighbor discovery and mobility
   management.

. 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 the efficient and reliable support of
   multicast and unicast from the link layer for various network
   operations such as MAC Address Resolution (AR), Duplicate Address
   Detection (DAD), and Neighbor Unreachability Detection (NUD).

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

   The legacy DAD assumes that a node with an IPv6 address can reach any
   other node with the scope of its address at the time it claims its
   address, and can hear any future claim for that address by another
   party within the scope of its address for the duration of the address
   ownership. However, the partitioning and merging of VANETs makes
   this assumption frequently invalid in vehicular networks. The
   merging and partitioning of VANETs frequently occurs 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 as the

destination vehicle.

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

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. IPv6 ND needs to work to
support those IPv6-based safety applications efficiently.

Thus, in IPv6-based vehicular networking, IPv6 ND should have minimum
changes for the interoperability with the legacy IPv6 ND used in the
Internet, including the DAD and NUD operations.

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. Note that the OMNI link model
supports these multihop V2V and V2I through an OMNI multilink service
[OMNI-Interface].

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 a single link between each vehicle pair within wireless communication range, as shown in Figure 5. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Suppose that a global-scope IPv6 prefix (or an IPv6 ULA prefix) is assigned to VANETs in vehicular networks. 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 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, when they are Vehicle1 and Vehicle3, as shown in Figure 5.

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 from each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable from each other in one hop due to either the multihop topology in the VANET or multiple partitions, the prefix should be off-link.

The vehicular link model needs to support multihop routing in a
connected VANET where the vehicles with the same global-scope IPv6
prefix (or the same IPv6 ULA prefix) are connected in one hop or
multiple hops. It also needs to support the multihop routing in
multiple connected VANETs through infrastructure nodes (e.g., IP-RSU)
where they are connected to the infrastructure. For example, in
Figure 1, suppose that Vehicle1, Vehicle2, and Vehicle3 are
configured with their IPv6 addresses based on the same global-scope
IPv6 prefix. Vehicle1 and Vehicle3 can also communicate with each
other via either multihop V2V or multihop V2I2V. When Vehicle1 and
Vehicle3 are connected in a VANET, it will be more efficient for them
to communicate with each other directly via VANET rather than
indirectly via IP-RSUs. On the other hand, when Vehicle1 and
Vehicle3 are far away from direct 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 the role of a relay node for those VANETs.

Thus, in IPv6-based vehicular networking, the vehicular link model
should have minimum changes for the interoperability with the legacy
IPv6 link model in an efficient fashion to support the IPv6 DAD and
NUD operations.

5.1.2. MAC Address Pseudonym

For the protection of drivers' privacy, a pseudonym of a MAC address
of a vehicle's network interface should be used, so that the MAC
address can be changed periodically. However, although such a
pseudonym of a MAC address can protect to some extent the privacy of
a vehicle, it may not be able to resist attacks on vehicle
identification by other fingerprint information, for example, the
scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack].
The pseudonym of a MAC address affects an IPv6 address based on the
MAC address, and a transport-layer (e.g., TCP 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 or 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 a VANET may cause redundant wireless frames in
the air to check the neighborhood of each vehicle and compute the
routing information in a VANET with a dynamic network topology
because 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 efficient mobility management including location
management and handover. Most 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 or a tunnel. The location precision can be improved
with assistance of the IP-RSUs or a cellular system with a GPS
receiver for location information.

With a GPS navigator, efficient mobility management can be performed
with the help of vehicles periodically reporting their current

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

By predicting a vehicle's mobility, the vehicular infrastructure
needs to better support IP-RSUs to perform efficient SLAAC, data

forwarding, horizontal handover (i.e., handover in wireless links
using a homogeneous radio technology), and vertical handover (i.e.,
handover in wireless links using heterogeneous radio technologies) in
advance along with the movement of the vehicle.

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

For a mobility management scheme in a shared link, where the wireless
subnets of multiple IP-RSUs share the same prefix, an efficient
vehicular-network-wide DAD is required. If DHCPv6 is used to assign
a unique IPv6 address to each vehicle in this shared link, the DAD is
not required. On the other hand, for a mobility management scheme
with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213] and OMNI
[OMNI-Interface]), DAD is not required because the IPv6 address of a
vehicle's external wireless interface is guaranteed to be unique.
There is a tradeoff between the prefix usage efficiency and DAD
overhead. Thus, the IPv6 address autoconfiguration for vehicular
networks needs to consider this tradeoff to support efficient
mobility management.

Therefore, for the proactive and seamless IPv6 mobility of vehicles,
the vehicular infrastructure (including IP-RSUs and MA) needs to
efficiently perform the mobility management of the vehicles with

their mobility information and link-layer information. Also, in
IPv6-based vehicular networking, IPv6 mobility management should have
minimum changes for the interoperability with the legacy IPv6
mobility management schemes such as PMIPv6, DMM, LISP, and AERO.

6. Security Considerations

   This section discusses security and privacy for IPv6-based vehicular
   networking. Security and privacy are key components of IPv6-based
   vehicular networking along with neighbor discovery and mobility
   management.

   Security and privacy are paramount in V2I, V2V, and V2X networking.
   Vehicles and infrastructure must be authenticated in order to
   participate in vehicular networking. Also, in-vehicle devices (e.g.,
   ECU) and a driver/passenger's mobile devices (e.g., smartphone and
   tablet PC) in a vehicle need to communicate with other in-vehicle
   devices and another driver/passenger's mobile devices in another
   vehicle, or other servers behind an IP-RSU in a secure way. Even
   though a vehicle is perfectly authenticated and legitimate, it may be

   hacked for running malicious applications to track and collect its
   and other vehicles' information. In this case, an attack mitigation
   process may be required to reduce the aftermath of malicious
   behaviors.

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

   Even though vehicles can be authenticated with valid certificates by
   an authentication server in the vehicular cloud, the authenticated
   vehicles may harm other vehicles, so their communication activities
   need to be logged in either a central way through a logging server
   (e.g., TCC) in the vehicular cloud or a distributed way (e.g.,

blockchain [Bitcoin]) along with other vehicles or infrastructure.
For the non-repudiation of the harmful activities of malicious nodes,
a blockchain technology can be used [Bitcoin]. Each message from a
vehicle can be treated as a transaction and the neighboring vehicles
can play the role of peers in a consensus method of a blockchain
[Bitcoin][Vehicular-BlockChain]. For a blockchain's efficient
consensus in vehicular networks having fast moving vehicles, a new
consensus algorithm needs to be developed or an existing consensus
algorithm needs to be enhanced.

To identify malicious vehicles among vehicles, an authentication
method is required. A Vehicle Identification Number (VIN) and a user
certificate (e.g., X.509 certificate [RFC5280]) along with an in-
vehicle device's identifier generation can be used to efficiently
authenticate a vehicle or its driver (having a user certificate)
through a road infrastructure node (e.g., IP-RSU) connected to an
authentication server in the vehicular cloud. This authentication
can be used to identify the vehicle that will communicate with an
infrastructure node or another vehicle. In the case where a vehicle
has an internal network (called Moving Network) and elements in the
network (e.g., in-vehicle devices and a user's mobile devices), as
shown in Figure 3, the elements in the network need to be
authenticated individually for safe authentication. Also, Transport
Layer Security (TLS) certificates [RFC8446][RFC5280] can be used for
an element's authentication to allow secure E2E vehicular
communications between an element in a vehicle and another element in

a server in a vehicular cloud, or between an element in a vehicle and
another element in another vehicle.

For secure V2I communication, a secure channel (e.g., IPsec) between
a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e.,
IP-RSU) in an EN needs to be established, as shown in Figure 3
[RFC4301][RFC4302][RFC4303][RFC4308][RFC7296]. Also, for secure V2V
communication, a secure channel (e.g., IPsec) between a mobile router
(i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in
another vehicle needs to be established, as shown in Figure 4. For
secure communication, an element in a vehicle (e.g., an in-vehicle
device and a driver/passenger's mobile device) needs to establish a
secure connection (e.g., TLS) with another element in another vehicle
or another element in a vehicular cloud (e.g., a server). Even

though IEEE 1609.2 [WAVE-1609.2] specifies security services for
applications and management messages. This WAVE specification is
optional, so if WAVE does not support the security of a WAVE frame,
either the network layer or the transport layer needs to support
security services for the WAVE frames.

For the setup of a secure channel over IPsec or TLS, the multihop V2I
communications over DSRC is required in a highway for the
authentication by involving multiple intermediate vehicles as relay
nodes toward an IP-RSU connected to an authentication server in the
vehicular cloud. The V2I communications over 5G V2X (or LTE V2X) is
required to allow a vehicle to communicate directly with a gNodeB (or
eNodeB) connected to an authentication server in the vehicular cloud.

To prevent an adversary from tracking a vehicle with its MAC address
or IPv6 address, especially for a long-living transport-layer session
(e.g., voice call over IP and video streaming service), a MAC address
pseudonym needs to be provided to each vehicle; that is, each vehicle
periodically updates its MAC address and its IPv6 address needs to be
updated accordingly by the MAC address change [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 (using
either IPsec or TLS), there will be no privacy benefit from changing
MAC and IPv6 addresses, because an adversary can observe the change
of the MAC and IPv6 addresses and track the vehicle with those
addresses. Thus, the MAC address pseudonym and the IPv6 address
update should be performed with strong E2E confidentiality.

For the IPv6 ND, the DAD is required to ensure the uniqueness of the
IPv6 address of a vehicle's wireless interface. This DAD can be used
as a flooding attack that uses the DAD-related ND packets
disseminated over the VANET or vehicular networks. Thus, the

vehicles and IP-RSUs need to filter out suspicious ND traffic in
advance.

For 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 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 with the IPv6
mobility of vehicles, 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.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash
          System", URL: https://bitcoin.org/bitcoin.pdf, May 2009.

[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.

[CBDN]   Kim, J., Kim, S., Jeong, J., Kim, H., Park, J., and T.
          Kim, "CBDN: Cloud-Based Drone Navigation for Efficient
          Battery Charging in Drone Networks", IEEE Transactions on
          Intelligent Transportation Systems, November 2019.

[DMM-FPC] Matsushima, S., Bertz, L., Liebsch, M., Gundavelli, S.,
          Moses, D., and C. Perkins, "Protocol for Forwarding Policy
          Configuration (FPC) in DMM", draft-ietf-dmm-fpc-cpdp-13
          (work in progress), March 2020.

[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.

   [ISO-ITS-IPv6-AMD1]
             ISO/TC 204, "Intelligent Transport Systems -
             Communications Access for Land Mobiles (CALM) - IPv6
             Networking - Amendment 1", ISO 21210:2012/AMD 1:2017,
             September 2017.

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

   [OMNI-Interface]
             Templin, F. and A. Whyman, "Transmission of IPv6 Packets
             over Overlay Multilink Network (OMNI) Interfaces", draft-
             templin-6man-omni-interface-24 (work in progress), June
             2020.

   [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.

   [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast
              Addresses", RFC 4193, October 2005.

   [RFC4301] Kent, S. and K. Seo, "Security Architecture for the
              Internet Protocol", RFC 4301, December 2005.

   [RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December
              2005.

   [RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)",
              RFC 4303, December 2005.

   [RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308,
              December 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.

   [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S.,
              Housley, R., and W. Polk, "Internet X.509 Public Key
              Infrastructure Certificate and Certificate Revocation List
              (CRL) Profile", RFC 5280, May 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.

   [RFC6550]   Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R.,
                Levis, P., Pister, K., Struik, R., Vasseur, JP., and R.
                Alexander, "RPL: IPv6 Routing Protocol for Low-Power and
                Lossy Networks", RFC 6550, March 2012.

   [RFC6706BIS]
                Templin, F., "Asymmetric Extended Route Optimization
                (AERO)", draft-templin-intarea-6706bis-58 (work in
                progress), June 2020.

   [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.

   [RFC6830BIS]
                Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A.
                Cabellos, "The Locator/ID Separation Protocol (LISP)",
                draft-ietf-lisp-rfc6830bis-32 (work in progress), March
                2020.

   [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.

   [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T.
              Kivinen, "Internet Key Exchange Protocol Version 2
              (IKEv2)", RFC 7296, October 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.

[SignalGuru]
          Koukoumidis, E., Peh, L., and M. Martonosi, "SignalGuru:
          Leveraging Mobile Phones for Collaborative Traffic Signal
          Schedule Advisory", ACM MobiSys, June 2011.

[TR-22.886-3GPP]
          3GPP, "Study on Enhancement of 3GPP Support for 5G V2X
          Services", 3GPP TR 22.886/Version 16.2.0, December 2018.

[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/Version 16.2.0, December 2019.

[TS-23.287-3GPP]
          3GPP, "Architecture Enhancements for 5G System (5GS) to
          Support Vehicle-to-Everything (V2X) Services", 3GPP
          TS 23.287/Version 16.2.0, March 2020.

[UAM-ITS] Templin, F., "Urban Air Mobility Implications for
          Intelligent Transportation Systems", draft-templin-ipwave-
          uam-its-03 (work in progress), July 2020.

[Vehicular-BlockChain]
          Dorri, A., Steger, M., Kanhere, S., and R. Jurdak,
          "BlockChain: A Distributed Solution to Automotive Security
          and Privacy", IEEE Communications Magazine, Vol. 55, No.
          12, December 2017.

   [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-15

   The following changes are made from draft-ietf-ipwave-vehicular-
   networking-15:

   o This version is revised based on the further comments from the
      following reviewers: Fred L. Templin (The Boeing Company) and
      YongJoon Joe (LSware).

o According to the comments from Fred L. Templin, in [Section 3.1](#)
   and [Section 3.2](#), UAM (Urban Air Mobility) end systems are
   considered for new V2V and V2I use cases.

o According to the comments from YongJoon Joe, in [Section 3.1](#) and
   [Section 6](#), the text about a consensus method of a blockchain in
   vehicular networks is revised such that a consensus algorithm
   needs to be efficient for fast moving vehicles.

[Appendix B](#).   Acknowledgments

[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), Suresh Krishnan (Kaloom), Nancy Cam-Winget
(Cisco), Fred L. Templin (The Boeing Company), Jung-Soo Park (ETRI),
Zeungil (Ben) Kim (Hyundai Motors), Kyoungjae Sun (Soongsil

University), Zhiwei Yan (CNNIC), YongJoon Joe (LSware), and Peter E.

Yee (Akayla). 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