IPWAVE Working Group
Internet-Draft
Intended status: Informational
Expires: September 25, 2019

J. Jeong, Ed.
Sungkyunkwan University

March 24, 2019

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

draft-ietf-ipwave-vehicular-networking-08

Abstract

This document discusses the problem statement and use cases of IP-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document surveys use cases using V2V, V2I, and V2X networking. Second, it analyzes proposed protocols for IP-based vehicular networking and highlights the limitations and difficulties found on those protocols. Third, it presents a problem exploration for key aspects in IP-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document discusses a problem statement to evaluate the gap between the state-of-the-art techniques and requirements in IP-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], service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850 - 5.925 GHz band (5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. Also, the European Union (EU) passed a decision to allocate radio spectrum for safety-related and non-safety-related applications of ITS with the frequency band of 5.875 - 5.905 GHz, which is called 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 the DSRC in terms of standards 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. Note that IEEE 802.11p was a separate standard, but was later enrolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set in 2012 [IEEE-802.11-OCB].

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC5944], MIPv6 [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213][RFC5844]) can be applied (or easily modified) to vehicular networks. In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. Note that a GN protocol is useful to route an event or notification message to vehicles around a geographic position, such as an acciendent area in a roadway. 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 discusses problem statements and use cases related to IP-based vehicular networking for Intelligent Transportation Systems (ITS), which is denoted as IP Wireless Access in Vehicular Environments (IPWAVE). First, it surveys the use cases for using V2V, V2I, and V2X networking in the ITS. Second, for literature review, it analyzes proposed protocols for IP-based vehicular networking and highlights the limitations and difficulties found on those protocols. Third, for problem statement, it presents a problem exploration with key aspects in IPWAVE, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect of the problem statement, it analyzes the gap between the state-of-the-art techniques and the requirements in IP-based vehicular networking. It also discusses potential topics relevant to IPWAVE Working Group (WG), such as Vehicle Identities Management, Multihop V2X Communications, Multicast, DNS Naming Services, Service Discovery, and IPv6 over Cellular Networks. Therefore, with the problem statement, this document will open a door to develop key protocols for IPWAVE that will be essential to IP-based vehicular networks.

2. Terminology

This document uses the following definitions:

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

- o LiDAR: Acronym for "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.

- o Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support their address autoconfiguration and mobility management with a binding table. It has end-to-end connections with RSUs under its control.

- o On-Board Unit (OBU): A node that has (e.g., IEEE 802.11-OCB and Cellular V2X (C-V2X) [TS-23.285-3GPP]) for wireless communications with other OBUs and RSUs, and may be connected to in-vehicle devices or networks. An OBU is mounted on a vehicle. It is assumed that a radio navigation receiver (e.g., Global Positioning System (GPS)) is included in a vehicle with an OBU for efficient navigation.

- o OCB: Acronym for "Outside the Context of a Basic Service Set" [IEEE-802.11-OCB].

- Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in car parking area.

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

- Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network nodes.

- Vehicle Detection Loop (or Loop Detector): An inductive device used for detecting vehicles passing or arriving at a certain point, for instance approaching a traffic light or in motorway traffic. The relatively crude nature of the loop's structure means that only metal masses above a certain size are capable of triggering the detection.

- V2I2P: Acronym for "Vehicle to Infrastructure to Pedestrian".

- V2I2V: Acronym for "Vehicle to Infrastructure to Vehicle".

- WAVE: Acronym for "Wireless Access in Vehicular Environments" [WAVE-1609.0].

3. Use Cases

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

3.1. V2V

The use cases of V2V networking discussed in this section include

- Context-aware navigation for driving safety and collision avoidance;

- Cooperative adaptive cruise control in an urban roadway;

- Platooning in a highway;

- Cooperative environment sensing.

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

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely by letting the drivers recognize dangerous obstacles and situations. That is, CASD navigator displays obstables 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, such as the Line-of-Sight unsafe, Non-Line-of-Sight unsafe and safe situations. This action plan can be performed among vehicles through 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 move together with a very short inter-distance. 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). This 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. Data generated by those sensors can be substantially large, and these data shall 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 context.

3.2. V2I

The use cases of V2I networking discussed in this section include

- Navigation service;

- Energy-efficient speed recommendation service;

- Accident notification service.

A navigation service, such as the Self-Adaptive Interactive Navigation Tool (called 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 the fast moving paths to emergency vehicles (e.g., ambulance and fire engine) to let them reach accident spots while providing other vehicles with efficient detour paths.

A TCC can recommend an energy-efficient speed to a vehicle driving in different traffic environments. [Fuel-Efficient] studies fuel-efficient route and speed plans for platooned trucks.

The emergency communication between accident vehicles (or emergency vehicles) and TCC can be performed via either RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, such as 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 FirstNet's network core. The current RAN is mainly constructed by 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Report], but it is expected that DSRC-based vehicular networks [DSRC] will be available for V2I and V2V in near future.

3.3. V2X

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

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with the access technology with an RSU (e.g., WiFi). Vehicles and pedestrians can also communicate with each other via an RSU that delivers scheduling information for wireless communication in order to save the smartphones' battery through sleeping mode.

For Vehicle-to-Pedestrian (V2P), a vehicle and a pedestrian's smartphone can directly communicate with each other via V2X without the relaying of an RSU as in a V2V scenario such that the pedestrian's smartphone is regarded as a vehicle with a wireless media interface to be able to communicate with another vehicle. In Vehicle-to-Device (V2D), a device can be a mobile node such as bicycle and motorcycle, and can communicate directly with a vehicle for collision avoidance.

4. Analysis for Existing Protocols

4.1. Existing Protocols for Vehicular Networking

We describe some currently existing protocols and proposed solutions with respect to the following aspects that are relevant and essential for vehicular networking:

o IP address autoconfiguration;

o Routing protocol;

o Mobility management;

o DNS naming service;

o Service discovery;

o Security and privacy.

4.1.1. IP Address Autoconfiguration

For IP address autoconfiguration, Fazio et al. proposed a vehicular address configuration (VAC) scheme using DHCP where elected leader-vehicles provide unique identifiers for IP address configurations in vehicles [Address-Autoconf]. Kato et al. proposed an IPv6 address assignment scheme using lane and position information [Address-Assignment]. Baldessari et al. proposed an IPv6 scalable address autoconfiguration scheme called GeoSAC for vehicular networks [GeoSAC]. Wetterwald et al. conducted for heterogeneous vehicular networks (i.e., employing multiple access technologies) a comprehensive study of the cross-layer identity management, which constitutes a fundamental element of the ITS architecture [Identity-Management].

A server-based address autoconfiguration such as VAC [Address-Autoconf] takes some delay for a vehicle to join a new cluster (i.e., a connected VANET) and communicate with neighboring vehicles. This delay may prevent vehicles from exchaning safety

messages with each other in a prompty way. It will be good for a vehicle to maintain its IP address even when it joins another cluster. A geographical-position-based address autoconfiguration, such as a prefix allocation per lane [Address-Assignment] and a prefix allocation per geographic region [GeoSAC], causes the frequent change of a vehicle's IP address and requires the DAD for the uniqueness test of a new IP address. This is significant overhead for high-speed moving vehicles. It will be efficient for a vehicle to be able to use its IP address while moving across the clusters and geographical regions. For the cross-layer identity management with multiple wireless interfaces [Identity-Management], it will be necessary to maintain an upper-layer session (e.g., TCP session) of a vehicle with multiple IP addresses corresponing to the multiple wireless interfaces.

4.1.2. Routing Protocol

For vehicular routing, Abboud et al. proposed a cluster-based routing [Cluster-Based-Routing]. Vehicles construct clusters along with their location and speed information for fast data dissemination among the clusters. They consist of cluster headers, cluster gateways and cluster members for intra-cluster and inter-cluster communications. Tsukada et al. presented a work that aims at combining IPv6 networking and a Car-to-Car Network (called C2CNet) routing protocol proposed by the Car-to-Car Communication Consortium (C2C-CC). Note that C2CNet is the network layer of the C2C-CC communication system and uses a geographic routing protocol for vehicular networks [VANET-Geo-Routing]. Abrougui et al. presented a gateway discovery scheme for vehicles to access the Internet via a gateway, called Location-Aided Gateway Advertisement and Discovery (LAGAD) mechanism [LAGAD]. A vehicle (as a packet source) multihop away from a gateway can discover the gateway and deliver its packets to the gateway through the packet forwarding of intermediate vehicles (as relay vehicles) in a connected VANET. Those intermediate vehicles are located between the packet source vehicle and the gateway.

For data packet routing in vehicular networks, multihop V2V and multihop V2I communications are required. For multihop V2V communications within a connected VANET, a cluster-based routing like [Cluster-Based-Routing] can play a role of efficient data forwarding through a virtual backbone of cluster headers and cluster gateways. For this, an efficient cluster formation is performed through sharing the mobility information (e.g., position, direction, and speed) of vehicles. But the pure VANET-based clustering will cause significant control messages and need some delay for cluster formation, so vehicles can perform clustering through infrastructure nodes (e.g.,

RSUs and base stations) via cellular links, which guarantees always-network-connection.

For multihop V2I communications, a gateway discovery scheme like LAGAD [LAGAD] can be used through a connected VANET having a connection with an Internet gateway. However, this reactive gateway discovery causes much control messages for the discovery and need some delay until a packet source vehicle can transmit its packets toward the gateway. Thus, a proactive gateway discovery is required over a connected VANET where vehicles share routes towards gateways (e.g., distance vector information to gateways) in a proactive manner.

4.1.3. Mobility Management

For mobility management, Chen et al. tackled the issue of network fragmentation in VANET environments [IP-Passing-Protocol] by proposing a protocol that can postpone the time to release IP addresses to the DHCP server and select a faster way to get the vehicle's new IP address, when the vehicle density is low or the speeds of vehicles are highly variable. Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support the mobility of high-speed mobile vehicles, which is based on both DMM and PMIPv6 [H-DMM]. They also proposed a hybrid centralized-distributed mobility management for network mobility called H-NEMO to support the efficient mobility of mobile nodes and mobile routers between different subnets, which is based on both DMM and PMIPv6 [H-NEMO].

[NEMO-LMS] proposed an architecture to enable IP mobility for moving networks using a network-based mobility scheme based on PMIPv6. Chen et al. proposed a network mobility protocol to reduce handoff delay and maintain Internet connectivity to moving vehicles in a highway [NEMO-VANET]. Lee et al. proposed P-NEMO, which is a PMIPv6-based IP mobility management scheme to maintain the Internet connectivity at the vehicle as a mobile network, and provides a make-before-break mechanism when vehicles switch to a new access network [PMIP-NEMO-Analysis]. Peng et al. proposed a novel mobility management scheme for integration of VANET and fixed IP networks [VNET-MM]. This scheme uses both a road network layout and the wireless coverage of multiple base stations in order to improve the connectivity of vehicles to the Internet and decrease the overhead of mobility management. Nguyen et al. extended their previous works (i.e., H-DMM [H-DMM] and H-NEMO [H-NEMO]) on a vehicular DMM by using a Software-Defined Networking (SDN) architecture, which separates the control plane and the data plane in network functionality [SDN-DMM].

A vehicle can have an internal network for its in-vehicle devices and passengers' mobile devices. In this case, vehicular networks need to support not only the host mobility for the vehicle, but also the network mobility of such an internet network within the vehicle. The current mobility management schemes, such as [H-DMM] and [H-NEMO], are not enough to support both the host mobility and network mobility in an efficient way. An efficient mobility management scheme can take advantage of a vehicle's mobility information (e.g., position, direction, and speed) and partial or full trajectory (i.e., a navigation path in a road network) in order to perform operations for mobility management proactively. For this proactive mobility management, an SDN-based mobility management scheme like [SDN-DMM] will be promising because SDN controllers can proactively set up forwarding tables for traffic flows of vehicles with their mobility and trajectory information.

4.1.4. DNS Naming Service

For DNS naming service, Multicast DNS (mDNS) [RFC6762] allows devices in one-hop communication range to resolve each other's DNS name into the corresponding IP address in multicast. DNS Name Autoconfiguration (DNSNA) [ID-DNSNA] proposes a DNS naming service for Internet-of-Things (IoT) devices in a large-scale network.

A DNS name resolution service needs to support DNS name resolution for in-vehicle devices and passengers' mobile devices within a vehicle's internal network, which can be called intra-vehicle DNS name resolution. Also, it needs to support DNS name resolution between devices (e.g., cooperative cruise control device) existing in different vehicles, which can be called inter-vehicle DNS name resolution. In addition, it need to support DNS name resolution in hosts or servers as corresponding nodes in the Internet, which can be called global DNS name resolution.

For the intra-vehicle DNS name resolution and inter-vehicle DNS name resolution, both mDNS [RFC6762] and DNSNA [ID-DNSNA] can be used, but they perform DNS name resolution in a reactive way. That is, when a DNS query is given by a querier, it will be multicasted to devices through mDNS or be unicasted to a dedicated DNS server through DNSNA, respectively.

For the inter-vehicle DNS name resolution in fast-moving vehicles, a proactive DNS resolution can be performed by the help of an RSU that collects the DNS information of vehicles and disseminate it to vehicles under its coverage.

For the global DNS name resolution, a vehicle can use an RSU's DNS server (or a DNS server close to an RSU in the wired network) to

perform a DNS resolution for the sake of the vehicle's device during its travel. When the DNS resolution is finished by the RSU's DNS server, the DNS server can forward the DNS resolution result to the vehicle through the current RSU providing the vehicle with the Internet connectivity.

4.1.5. Service Discovery

To discover instances of a demanded service in vehicular networks, DNS-based Service Discovery (DNS-SD) [RFC6763] with either DNSNA [ID-DNSNA] or mDNS [RFC6762] provides vehicles with service discovery by using standard DNS queries. Vehicular ND [ID-Vehicular-ND] proposes an extension of IPv6 ND for the prefix and service discovery with new ND options.

For vehicular networks, DNSNA can use a dedicated DNS server residing in an RSU or close to an RSU in the wired network [ID-DNSNA]. In this case, in-vehicle devices can register their services (e.g., cooperative cruise control service and navigation service) into the DNS server. When the DNS server can receive a service discovery query from vehicles via an RSU, it can resolve it quickly for them. In DNSNA, these DNS query and response messages are delivered in unicast rather than multicast, so the wireless channel will be utilized efficiently for DNS resolution including service discovery. Thus, DNSNA will provide a more efficient service discovery to vehicles in a high-vehicle-density environment than mDNS [RFC6762] and Vehicular ND [ID-Vehicular-ND]. This is because a DNS query for service discovery is unicasted by DNSNA, but it is multicasted by both mDNS and Vehicular ND.

In a V2V scenario such as the case where a dedicated DNS server in an RSU is not available for the registration and sharing of service information, Vehicular ND can provide vehicles with rapid service discovery by letting vehicles proactively advertise their service information with Neighbor Advertisement (NA) messages. Thus, considering both V2I and V2V scenarios, an efficient service discovery scheme can be designed.

4.1.6. Security and Privacy

For security and privacy, Fernandez et al. proposed a secure vehicular IPv6 communication scheme using Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) for vehiculer networks. This scheme provides the secure communication channel between a home agent and a mobile router to support the network mobility of a vehicle's internal network [Securing-VCOMM]. Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks

[VNET-AAA]. The vehicular networks consist of VANETs as a front end and an access network as a back end via an access point. The security scheme provides vehicles with an efficient AAA service for the network connectivity during their movement in the road network.

Security services in vehicular networks need to support an efficient AAA for the accommodation of only valid vehicles and a secure communication with IKEv2 and IPsec between vehicles or between a vehicle and the corresponding node in the Internet. For the efficiency, these security services need to take advantage of a vehicular network architecture having a TCC and RSUs as well as a vehicle's mobility and trajectory information.

4.2. General Problems

This section describes a possible vehicular network architecture for V2V, V2I, and V2X communications. Then it analyzes the limitations of the current protocols for vehicular networking.

```
                     Traffic Control Center in Vehicular Cloud
                    *-----------------------------------------*
                   *                                           *
                  *             +----------------+              *
                 *              | Mobility Anchor|               *
                 *              +----------------+               *
                  *                      ^                      *
                   *                     |                     *
                    *--------------------v--------------------*
                    ^               ^                        ^
                    |               |                        |
                    |               |                        |
                    v               v                        v
               +--------+ Ethernet +--------+            +--------+
               |  RSU1  |<-------->|  RSU2  |<---------->|  RSU3  |
               +--------+          +--------+            +--------+
                  ^                     ^                    ^
                  :                     :                    :
           +--------------------------------------+ +------------------+
           |      : V2I             V2I :         | |    V2I :         |
           |      v                     v         | |        v         |
+--------+ |   +--------+          +--------+     | |    +--------+    |
|Vehicle1|===> |Vehicle2|===>      |Vehicle3|===> | |    |Vehicle4|===>|
|        |<...>|        |<........>|        |     | |    |        |    |
+--------+ V2V +--------+    V2V   +--------+     | |    +--------+    |
           |                                      | |                  |
           +--------------------------------------+ +------------------+
                           Subnet1                         Subnet2

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

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

4.2.1. Vehicular Network Architecture

Figure 1 shows an architecture for V2I and V2V networking in a road network. As shown in this figure, RSUs as routers and vehicles with OBU have wireless media interfaces for VANET. Also, it is assumed that such 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.

Especially, for IPv6 packets transporting over IEEE 802.11-OCB, [IPv6-over-802.11-OCB] specifies several details, such as Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. Especially, an Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC

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

In Figure 1, three RSUs (RSU1, RSU2, and RSU3) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of RSUs and vehicles in the road network. A Mobility Anchor (MA) is located in the TCC as its key component for the mobility management of vehicles. Two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and one vehicle (Vehicle3) is wirelessly connected to RSU2. The wireless networks of RSU1 and RSU2 belong to a multi-link subnet (denoted as Subnet1) with the same network prefix. Thus, these three vehicles are within the same subnet. On the other hand, another vehicle (Vehicle4) is wireless connected to RSU4, belonging to another subnet (denoted as Subnet2). That is, the first three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle3) and the last vehicle (i.e., Vehicle4) are located in the two different subnets.

In wireless subnets in vehicular networks (e.g., Subnet 1 and Subnet 2 in Figure 1), vehicles can construct a connected VANET (as 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 same subnet along their IPv6 addresses, which are based on the same prefix. On the other hand, Vehicle3 can communicate with Vehicle4 via RSU2 and RSU3 employing V2I (i.e., V2I2V) communication because they are within the two different subnets along with their IPv6 addresses, which are based on the two different prefixes.

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

Cespedes et al. proposed a vehicular IP in WAVE called VIP-WAVE for I2V and V2I networking [VIP-WAVE]. The standard WAVE does not

support both seamless communications for Internet services and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU), either. To overcome these limitations of the standard WAVE, VIP-WAVE enhances the standard WAVE by the following three schemes:

1. An efficient mechanism for the IPv6 address assignment and DAD

2. An on-demand IP mobility management based on PMIPv6 [RFC5213]

3. One-hop and two-hop communication scheme for V2I networking

Note that VIP-WAVE supports at most two-hop V2I communication for simple forwarding operations in VANET. This is because the multi-hop V2I communication with more than two hops requires an additional VANET routing protocol. Such a multi-hop V2I communication will be required for vehicles in a highway with sparsely deployed RSUs in order to provide them with the Internet connectivity via V2I.

Baccelli et al. provided an analysis of the operation of IPv6 as it has been described by the IEEE WAVE standards 1609 [IPv6-WAVE]. This analysis confirms that the use of the standard IPv6 protocol stack in WAVE is not sufficient. It recommends that the IPv6 addressing assignment should follow considerations for ad-hoc link models, defined in [RFC5889] for nodes' mobility and link variability. However, this ad-hoc link model is not clearly defined to support the efficient V2V and V2I for vehicles with a wireless interface configured with an IPv6 address.

Petrescu et al. proposed the joint IP networking and radio architecture for V2V and V2I communication in [Joint-IP-Networking]. The radio architecture uses Wi-Fi for wireless link rather than IEEE 802.11-OCB. The proposed architecture considers an IP topology in a similar way as a radio link topology, in the sense that an IP subnet would correspond to the range of 1-hop vehicular communication. This architecture defines three types of vehicles: Leaf Vehicle, Range Extending Vehicle, and Internet Vehicle. Leaf Vehicle is like a vehicle with OBU and has one external WiFi interface along with an MR. This MR supports the network mobility of a user's mobile device and in-vehicle devices in the vehicle's internal network. Range Extending Vehicles has two external Wi-Fi interfaces to connect two Wi-Fi subnets of cars in a train. Internet Vehicle has one Wi-Fi interface for a car's subnet and one Wireless Metropolitan Area Network (WMAN) interface for the Internet connectivity. However, this architecture is not suitable for vehicles with a small size and with a wireless interface for V2V and V2I in vehicular links.

4.2.1.1. V2I-based Internetworking

This section discusses the internetworking between a vehicle's moving network and an RSU's fixed network via V2I communication.

```
                                                    +-----------------+
                           (*)<........>(*)  +----->| Vehicular Cloud |
          2001:DB8:1:1::/64 |            |   |      +-----------------+
   +------------------------------+  +---------------------------------+
   |                        v     |  |   v   v                         |
   | +-------+ +------+ +-------+ |  | +-------+ +------+ +-------+    |
   | | Host1 | | DNS1 | |Router1| |  | |Router3| | DNS2 | | Host3 |    |
   | +-------+ +------+ +-------+ |  | +-------+ +------+ +-------+    |
   |     ^        ^         ^     |  |     ^         ^        ^        |
   |     |        |         |     |  |     |         |        |        |
   |     v        v         v     |  |     v         v        v        |
   | ---------------------------- |  | ------------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |     ^ 2001:DB8:20:1::/64        |
   |                    |         |  |     |                           |
   |                    v         |  |     v                           |
   | +-------+      +-------+     |  | +-------+ +-------+   +-------+ |
   | | Host2 |      |Router2|     |  | |Router4| |Server1|...|ServerN| |
   | +-------+      +-------+     |  | +-------+ +-------+   +-------+ |
   |     ^              ^         |  |     ^         ^           ^     |
   |     |              |         |  |     |         |           |     |
   |     v              v         |  |     v         v           v     |
   | ---------------------------- |  | ------------------------------- |
   |      2001:DB8:10:2::/64      |  |       2001:DB8:20:2::/64        |
   +------------------------------+  +---------------------------------+
      Vehicle1 (Moving Network1)            RSU1 (Fixed Network1)

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

Figure 2: Internetworking between Vehicle Network and RSU Network

As shown in Figure 2, the vehicle's moving network and the RSU's fixed network are self-contained networks having multiple subnets and having an edge router for the communication with another vehicle or RSU. Internetworking between two internal networks via V2I communication requires an exchange of network prefix and other parameters through a prefix discovery mechanism, such as ND-based prefix discovery [ID-Vehicular-ND]. For the ND-based prefix discovery, network prefixs and parameters should be registered into a vehicle's router and an RSU router with an external network interface in advance.

The network parameter discovery collects networking information for an IP communication between a vehicle and an RSU or between two

neighboring vehicles, such as link layer, MAC layer, and IP layer information. The link layer information includes wireless link layer parameters, such as wireless media (e.g., IEEE 802.11-OCB and LTE-V2X) and a transmission power level. The MAC layer information includes the MAC address of an external network interface for the internetworking with another vehicle or RSU. The IP layer information includes the IP address and prefix of an external network interface for the internetworking with another vehicle or RSU.

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle's moving network and the RSU's fixed network. DNS services should be supported to enable name resolution for hosts or servers residing either in the vehicle's moving network or the RSU's fixed network. It is assumed that the DNS names of in-vehicle devices and their service names are registered into a DNS server in a vehicle or an RSU, as shown in Figure 2. For service discovery, those DNS names and service names can be advertised to neighboring vehicles through either DNS-based service discovery mechanisms [RFC6762][RFC6763][ID-DNSNA] and ND-based service discovery [ID-Vehicular-ND]. For the ND-based service discovery, service names should be registered into a vehicle's router and an RSU router with an external network interface in advance. For this service discovery, each vehicle and each RSU should have its dedicated DNS server within its internal network, respectively, as shown in Figure 2.

Figure 2 shows internetworking between the vehicle's moving network and the RSU's fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Fixed Network1) inside RSU1. RSU1 has the DNS Server (DNS2), one host (Host3), the two routers (Router3 and Router4), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1's Router1 (called mobile router) and RSU1's Router3 (called fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for I2V networking.

4.2.1.2. 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 | | DNS1 | |Router1| |  | |Router5| | DNS3 | | Host4 | |
   | +-------+ +------+ +-------+ |  | +-------+ +------+ +-------+ |
   |     ^        ^         ^     |  |     ^         ^        ^     |
   |     |        |         |     |  |     |         |        |     |
   |     v        v         v     |  |     v         v        v     |
   | ---------------------------- |  | ---------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |         ^ 2001:DB8:30:1::/64 |
   |                    |         |  |         |                    |
   |                    v         |  |         v                    |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   | | Host2 |      |Router2|     |  |     |Router6|      | Host5 | |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   |     ^              ^         |  |         ^              ^     |
   |     |              |         |  |         |              |     |
   |     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 Vehicle Networks

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

4.2.2. Latency

The communication delay (i.e., latency) between two vehicles should be bounded to a certain threshold (e.g., 500 ms) for collision-avoidance message exchange [CASD]. For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. The real implementations for such applications are not

available yet. Thus, the feasibility of IP-based safety applications is not tested yet in the real world.

4.2.3. Security

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

4.2.4. Pseudonym Handling

For the protection of drivers' privacy, the pseudonym of a MAC address of a vehicle's network interface should be used, with the help of which the MAC address can be changed periodically. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP) session with an IPv6 address pair. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

5. Problem Exploration

This section discusses key topics for IPWAVE WG, such as neighbor discovery, mobility management, and security & privacy.

5.1. Neighbor Discovery

Neighbor Discovery (ND) [RFC4861] is a core part of the IPv6 protocol suite. This section discusses the need for modifying ND for use with vehicular networking (e.g., V2V, V2I, and V2X). The vehicles are moving fast within the communication coverage of a vehicular node (e.g., vehicle and RSU). The external wireless link between two vehicular nodes can be used for vehicular networking, as shown in Figure 2 and Figure 3.

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

from 0.5 sec to 1 sec) for the NA messages to reduce collision probability with other NA messages.

5.1.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in a vehicular wireless link [VIP-WAVE]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces. However, interference and different levels of transmission power may cause unidirectional links to appear in vehicular wireless links. As a result, a new vehicular link model is required for a dynamically changing vehicular wireless link.

There is a relationship between a link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IP link or extended IP links via ND proxy. Note that a subnet prefix can be used by spanning multiple links into a multi-link subnet with an extended subnet concept [RFC6775]. Also, note that IPv6 Stateless Address Autoconfiguration (SLAAC) can be performed in the multiple links where each of them is not assigned with a unique subnet prefix, that is, all of them are configured with the same subnet prefix [RFC4861][RFC4862].

A vehicular link model needs to consider a multi-hop V2V (or V2I) over a multi-link subnet as shown in Figure 1. In this figure, vehicles in Subnet1 having RSU1 and RSU2 construct a multi-link subnet called Subnet1 with VANETs and RSUs. Vehicle1 and Vehicle3 can communicate with each other via multi-hop V2V or multi-hop V2I2V. When two vehicles (e.g., Vehicle1 and Vehicle3 in Figure 1) are connected in a VANET, they can communicate with each other via VANET rather than RSUs. On the other hand, when two vehicles (e.g., Vehicle1 and Vehicle3) are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V.

Thus, IPv6 ND should be extended into a Vehicular Neighbor Discovey (VND) [ID-Vehicular-ND] to support the concept of an IPv6 link corresponding to an IPv6 prefix even in a multi-link subnet consisting of multiple vehicles and RSUs that are interconnected with wireless communication range in IP-based vehicular networks.

5.1.2. MAC Address Pseudonym

In the ETSI standards, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities (e.g., MAC address) and the corresponding IPv6 addresses [Identity-Management]. Whenever the network interface identifier changes, the IPv6 address based on the network interface identifier should be updated, and the uniqueness of the address should be performed through the DAD procedure. For vehicular networks with high-mobility, this DAD should be performed efficiently with minimum overhead.

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

5.1.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes in within the internal networks of two vehicular nodes (e.g., vehicle and RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is required. It is assumed that a vehicular node has an external network interface and its internal network, as shown in Figure 2 and Figure 3. The vehicular ND (VND) [ID-Vehicular-ND] can support the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) of vehicular nodes with a vehicular prefix information option. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without a vehicular ad hoc routing protocol (e.g., AODV [RFC3561] and OLSRv2 [RFC7181]).

5.1.4. Routing

For multihop V2V communications in a multi-link subnet (as a connected VANET), 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. Instead of the vehicular ad hoc routing protocol, Vehicular ND along with a prefix discovery option can be used to let vehicles exchange their prefixes in a multihop fashion [ID-Vehicular-ND]. With the exchanged prefixes, they can compute their routing table (or IPv6 ND's neighbor

cache) for the multi-link subnet with a distance-vector algorithm [Intro-to-Algorithms].

Also, an efficient, rapid DAD should be supported in a multi-link subnet to prevent or reduce IPv6 address conflicts in such a subnet by using a multi-hop DAD optimization [ID-Vehicular-ND][RFC6775] or an IPv6 geographic-routing-based address autoconfiguration [GeoSAC].

5.2. Mobility Management

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

With this GPS navigator, an efficient mobility management is possible by vehicles periodically reporting their current position and trajectory (i.e., navigation path) to RSUs and a Mobility Anchor (MA) in TCC. The RSUs and MA can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the efficient mobility management (e.g., proactive handover). For a better proactive handover, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]), can be used to determine the moment of a handover between RSUs along with mobility information [ID-Vehicular-ND].

With the prediction of the vehicle mobility, MA can support RSUs to perform DAD, data packet routing, horizontal handover (i.e., handover in wireless links using a homogeneous radio technology), and vertical handover (i.e., handover in wireless links using heterogeneous radio technologies) in a proactive manner. Even though a vehicle moves into the wireless link under another RSU belonging to a different subnet, the RSU can proactively perform the DAD for the sake of the vehicle, reducing IPv6 control traffic overhead in the wireless link [ID-Vehicular-ND]. To prevent a hacker from impersonating RSUs as bogus RSUs, RSUs and MA should have secure channels via IPsec.

Therefore, with a proactive handover and a multihop DAD in vehicular networks [ID-Vehicular-ND], RSUs can efficiently forward data packets from the wired network (or the wireless network) to a moving destination vehicle along its trajectory along with the MA. Thus, a moving vehicle can communicate with its corresponding vehicle in the

vehicular network or a host/server in the Internet along its trajectory.

5.3. Security and Privacy

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

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

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

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

6. Security Considerations

This document discussed security and privacy for IP-based vehicular networking.

The security and privacy for key components in IP-based vehicular networking, such as neighbor discovery and mobility management, need to be analyzed in depth.

7. Informative References

[Address-Assignment]
Kato, T., Kadowaki, K., Koita, T., and K. Sato, "Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network", IEEE Asia-Pacific Services Computing Conference, December 2008.

[Address-Autoconf]
Fazio, M., Palazzi, C., Das, S., and M. Gerla, "Automatic IP Address Configuration in VANETs", ACM International Workshop on Vehicular Inter-Networking, September 2016.

[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.

[Broadcast-Storm]
Wisitpongphan, N., K. Tonguz, O., S. Parikh, J., Mudalige, P., Bai, F., and V. Sadekar, "Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks", IEEE Wireless Communications, December 2007.

[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.

[Cluster-Based-Routing]
Abboud, K. and W. Zhuang, "Impact of Microscopic Vehicle Mobility on Cluster-Based Routing Overhead in VANETs", IEEE Transactions on Vehicular Technology, Vol. 64, No. 12, December 2015.

[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.

[ETSI-GeoNetwork-IP]
ETSI Technical Committee Intelligent Transport Systems, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols", ETSI EN 302 636-6-1, October 2013.

[ETSI-GeoNetworking]
ETSI Technical Committee Intelligent Transport Systems, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality", ETSI EN 302 636-4-1, May 2014.

[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.

[GeoSAC] Baldessari, R., Bernardos, C., and M. Calderon, "GeoSAC - Scalable Address Autoconfiguration for VANET Using Geographic Networking Concepts", IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, September 2008.

[H-DMM] Nguyen, T. and C. Bonnet, "A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users", IEEE International Conference on Communications, June 2015.

[H-NEMO] Nguyen, T. and C. Bonnet, "A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility", IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks, June 2015.

[ID-DNSNA]
Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-04 (work in progress), October 2018.

[ID-Vehicular-ND]
Jeong, J., Ed., Shen, Y., and Z. Xiang, "IPv6 Neighbor Discovery for IP-Based Vehicular Networks", draft-jeong-ipwave-vehicular-neighbor-discovery-06 (work in progress), March 2019.

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

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

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

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

[IP-Passing-Protocol]
Chen, Y., Hsu, C., and W. Yi, "An IP Passing Protocol for Vehicular Ad Hoc Networks with Network Fragmentation", Elsevier Computers & Mathematics with Applications, January 2012.

[IPv6-over-802.11-OCB]
Petrescu, A., Benamar, N., Haerri, J., Lee, J., and T. Ernst, "Transmission of IPv6 Packets over IEEE 802.11 Networks operating in mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)", draft-ietf-ipwave-ipv6-over-80211ocb-34 (work in progress), December 2018.

[IPv6-WAVE]
Baccelli, E., Clausen, T., and R. Wakikawa, "IPv6 Operation for WAVE - Wireless Access in Vehicular Environments", IEEE Vehicular Networking Conference, December 2010.

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

[Joint-IP-Networking]
Petrescu, A., Boc, M., and C. Ibars, "Joint IP Networking and Radio Architecture for Vehicular Networks", 11th International Conference on ITS Telecommunications, August 2011.

[LAGAD] Abrougui, K., Boukerche, A., and R. Pazzi, "Location-Aided Gateway Advertisement and Discovery Protocol for VANets", IEEE Transactions on Vehicular Technology, Vol. 59, No. 8, October 2010.

[Multicast-802]
Perkins, C., Stanley, D., Kumari, W., and JC. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-perkins-intarea-multicast-ieee802-03 (work in progress), July 2017.

[Multicast-Alert]
Camara, D., Bonnet, C., Nikaein, N., and M. Wetterwald, "Multicast and Virtual Road Side Units for Multi Technology Alert Messages Dissemination", IEEE 8th International Conference on Mobile Ad-Hoc and Sensor Systems, October 2011.

[NEMO-LMS]
Soto, I., Bernardos, C., Calderon, M., Banchs, A., and A. Azcorra, "NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios", IEEE Communications Magazine, May 2009.

[NEMO-VANET]
Chen, Y., Hsu, C., and C. Cheng, "Network Mobility Protocol for Vehicular Ad Hoc Networks", Wiley International Journal of Communication Systems, November 2014.

[PMIP-NEMO-Analysis]
Lee, J., Ernst, T., and N. Chilamkurti, "Performance Analysis of PMIPv6-Based Network Mobility for Intelligent Transportation Systems", IEEE Transactions on Vehicular Technology, January 2012.

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

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", RFC 4086, June 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy Mobile IPv6", RFC 5844, May 2010.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

[RFC5944] Perkins, C., Ed., "IP Mobility Support in IPv4, Revised", RFC 5944, November 2010.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

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

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

[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.

[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.

[SDN-DMM] Nguyen, T., Bonnet, C., and J. Harri, "SDN-based Distributed Mobility Management for 5G Networks", IEEE Wireless Communications and Networking Conference, April 2016.

[Securing-VCOMM]
Fernandez, P., Santa, J., Bernal, F., and A. Skarmeta, "Securing Vehicular IPv6 Communications", IEEE Transactions on Dependable and Secure Computing, January 2016.

[TR-22.886-3GPP]
3GPP, "Study on Enhancement of 3GPP Support for 5G V2X Services", 3GPP TS 22.886, June 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, June 2018.

[VANET-Geo-Routing]
Tsukada, M., Jemaa, I., Menouar, H., Zhang, W., Goleva, M., and T. Ernst, "Experimental Evaluation for IPv6 over VANET Geographic Routing", IEEE International Wireless Communications and Mobile Computing Conference, June 2010.

[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.

[VMaSC-LTE]
Ucar, S., Ergen, S., and O. Ozkasap, "Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination", IEEE Transactions on Vehicular Technology, April 2016.

[VNET-AAA]
Moustafa, H., Bourdon, G., and Y. Gourhant, "Providing Authentication and Access Control in Vehicular Network Environment", IFIP TC-11 International Information Security Conference, May 2006.

[VNET-MM] Peng, Y. and J. Chang, "A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks and Fixed IP Networks", Springer Mobile Networks and Applications, February 2010.

[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. Relevant Topics to IPWAVE Working Group

This section discusses topics relevant to IPWAVE WG: (i) vehicle identity management; (ii) multihop V2X; (iii) multicast; (iv) DNS naming services and service discovery; (v) IPv6 over cellular networks.

A.1. Vehicle Identity Management

A vehicle can have multiple network interfaces using different access network technologies [Identity-Management]. These multiple network interfaces mean multiple identities. To identify a vehicle with multiple indenties, a Vehicle Identification Number (VIN) can be used as a globally unique vehicle identifier.

To support the seamless connectivity over the multiple identities, a cross-layer network architecture is required with vertical handover functionality [Identity-Management]. Also, an AAA service for multiple identities should be provided to vehicles in an efficient way to allow horizontal handover as well as vertical handover; note that AAA stands for Authentication, Authorization, and Accounting.

A.2. Multihop V2X

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

A.3. Multicast

IP multicast in vehicular network environments is especially useful for various services. For instance, an automobile manufacturer can multicast a particular group/class/type of vehicles for service notification. As another example, a vehicle or an RSU can disseminate alert messages in a particular area [Multicast-Alert].

In general IEEE 802 wireless media, some performance issues about multicast are found in [Multicast-802]. Since several procedures and functions based on IPv6 use multicast for control-plane messages, such as Neighbor Discovery (ND) and Service Discovery, [Multicast-802] describes that the ND process may fail due to unreliable wireless link, causing failure of the DAD process. Also, the Router Advertisement messages can be lost in multicasting.

A.4. DNS Naming Services and Service Discovery

When two vehicular nodes communicate with each other using the DNS name of the partner node, DNS naming service (i.e., DNS name resolution) is required. As shown in Figure 2 and Figure 3, a DNS server within an internal network can perform such DNS name resolution for the sake of other vehicular nodes.

A service discovery service is required for an application in a vehicular node to search for another application or server in another vehicular node, which resides in either the same internal network or the other internal network. In V2I or V2V networking, as shown in Figure 2 and Figure 3, such a service discovery service can be provided by either DNS-based Service Discovery (DNS-SD) [RFC6763] with mDNS [RFC6762] or the vehicular ND with a new option for service discovery [ID-Vehicular-ND].

A.5. IPv6 over Cellular Networks

Recently, 3GPP has announced a set of new technical specifications, such as Release 14 (3GPP-R14) [TS-23.285-3GPP], which proposes an architecture enhancements for V2X services using the modified sidelink interface that originally is designed for the LTE-Device-to-Device (D2D) communications. 3GPP-R14 specifies that the V2X services only support IPv6 implementation. 3GPP is also investigating and discussing the evolved V2X services in the next generation cellular networks, i.e., 5G new radio (5G-NR), for advanced V2X communications and automated vehicles' applications.

A.5.1. Cellular V2X (C-V2X) Using 4G-LTE

Before 3GPP-R14, some researchers have studied the potential usage of C-V2X communications. For example, [VMaSC-LTE] explores a multihop cluster-based hybrid architecture using both DSRC and LTE for safety message dissemination. Most of the research considers a short message service for safety instead of IP datagram forwarding. In other C-V2X research, the standard IPv6 is assumed.

The 3GPP technical specification of [TS-23.285-3GPP] states that both IP based and non-IP based V2X messages are supported, and only IPv6 is supported for IP based messages. Moreover, [TS-23.285-3GPP] instructs that a UE autoconfigures a link-local IPv6 address by following SLAAC in [RFC4862], but without sending Neighbor Solicitation and Neighbor Advertisement messages for DAD. This is because a unique prefix is allocated to each node by the 3GPP network, so the IPv6 addresses cannot be duplicate.

A.5.2. Cellular V2X (C-V2X) Using 5G

The emerging services, functions, and applications, which are developped in automotive industry, demand reliable and efficient communication infrastructure for road networks. Correspondingly, enhanced V2X (eV2X)-based services can be supported by 5G systems. The 3GPP Technical Report of [TR-22.886-3GPP] is studying new use cases and the corresponding service requirements for V2X (including V2V and V2I) using 5G in both infrastructure mode and the sidelink variations in the future.

Appendix B. Changes from draft-ietf-ipwave-vehicular-networking-07

The following changes are made from draft-ietf-ipwave-vehicular-networking-07:

- This version is revised based on the comments from Charlie Perkins and Sri Gundavelli.

- In Section 4.1, the existing protocols relevant to IP vehicular networking are summarized and analyzed with pros and cons. This subsection addresses the requirements for IP vehicular networking.

- In Figure 1, a vehicular network architecture is modified to clarify a multi-link subnet consisting of vehicular wireless links, and to provide efficient vehicular communications for V2I & V2V to vehicles whose wireless interface is configured with a global IP address.

Appendix C. Acknowledgments

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

This work was supported in part by Global Research Laboratory Program through the NRF funded by the Ministry of Science and ICT (MSIT) (NRF-2013K1A1A2A02078326) and by the DGIST R&D Program of the MSIT (18-EE-01).

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 D. 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, and Dirk von Hugo (Deutsche Telekom). 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 Software
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