IPWAVE Working Group
Internet-Draft
Intended status: Informational
Expires: January 3, 2019

J. Jeong, Ed.
Sungkyunkwan University

July 2, 2018

IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-03

Abstract

This document discusses problem statement and use cases on IP-based vehicular networks, which are considered a key component of Intelligent Transportation Systems (ITS). The main topics of vehicular networking are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. First, this document surveys use cases using V2V, V2I, and V2X networking. Second, this document analyzes current protocols for vehicular networking and general problems on those current protocols. Third, this document does problem exploration for key aspects in IP-based vehicular networking, such as IPv6 over IEEE 802.11-OCB, IPv6 Neighbor Discovery, Mobility Management, Vehicle Identities Management, Multihop V2X Communications, Multicast, DNS Naming Services, Service Discovery, IPv6 over Cellular Networks, Security and Privacy. For each key aspect, this document discusses problem statement to analyze the gap between the state-of-the-art techniques and requirements in IP-based vehicular networking.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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

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

This Internet-Draft will expire on January 3, 2019.

Table of Contents

1. Introduction

Vehicular networks have been focused on the driving safety, driving efficiency, and entertainment in road 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.

For driving safety services based on the DSRC, IEEE has standardized Wireless Access in Vehicular Environments (WAVE) standards, such as IEEE 802.11p [IEEE-802.11p], IEEE 1609.2 [WAVE-1609.2], IEEE 1609.3 [WAVE-1609.3], and IEEE 1609.4 [WAVE-1609.4]. Note that IEEE 802.11p has been published as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012. Along with these WAVE standards, IPv6 and Mobile IP protocols (e.g., MIPv4 and MIPv6) can be extended to vehicular networks [RFC2460][RFC5944][RFC6275]. Also, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. In addition, ISO has standardized a standard specifying the IPv6 network protocols and services 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). This document first surveys the use cases for using V2V and V2I networking in the ITS. Second, for problem statement, this document deals with critical aspects in vehicular networking, such as IPv6 over IEEE 802.11-OCB, IPv6 Neighbor Discovery, Mobility Management, Vehicle Identities Management, Multihop V2X Communications, Multicast, DNS Naming Services, Service Discovery, IPv6 over Cellular Networks, Security and Privacy. For each key aspect, this document discusses problem statement to analyze the gap

between the state-of-the-art techniques and requirements in IP-based vehicular networking. Finally, with the problem statement, this document suggests demanding key standardization items for the deployment of IPWAVE in road environments. As a consequence, this will make it possible to design a network architecture and protocols for vehicular networking.

2. Terminology

This document uses the following definitions:

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

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

- Road-Side Unit (RSU): A node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, LTE-V2X, etc.) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is deployed either at an intersection or in a road segment.

- On-Board Unit (OBU): A node that has a DSRC device for wireless communications with other OBUs and RSUs. 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.

- 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.

- 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.

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-Cuise-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. CACC can help adjacent vehicles to efficiently adjust their speed in a cascade way through V2V networking.

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 environment information from various sensors, such as radars, LiDARs and cameras, mounted on them 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 vehicles. Through cooperative enivronment sensing, driver vehicles can use enivronment information sensed by driverless vehicles for better interaction with environments.

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 global road traffic optimization and can guide individual vehicles for appropriate navigation paths in real time. The enhanced SAINT (called SAINT+) [SAINTplus] can give the fast moving paths for emergency vehicles (e.g., ambulance and fire engine) toward 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] studys 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-Annual-Report-2017], but DSRC-based vehicular networks can be used for V2I in near future [DSRC].

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 pedestrian and a vehicle, which have a smartphone, in a road network. Vehicles and pedestrians can communicate with each other via an RSU that delivers scheduling information for wireless communication to save the smartphones' battery.

4. Analysis for Current Protocols

4.1. Current Protocols for Vehicular Networking

We analyze the current protocols from the follow aspects:

- IP address autoconfiguration;
- Routing;
- Mobility management;
- DNS naming service;
- Service discovery;
- 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 [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 a comprehensive study of the cross-layer identities management in vehicular networks using multiple access network technologies, which constitutes a fundamental element of the ITS architecture [Identity-Management].

4.1.2. Routing

For routing, Tsukada et al. presented a work that aims at combining IPv6 networking and a Car-to-Car Network routing protocol (called C2CNet) proposed by the Car2Car Communication Consortium (C2C-CC), which is an architecture using a geographic routing protocol [VANET-Geo-Routing]. Abrougui et al. presented a gateway discovery scheme for VANET, called Location-Aided Gateway Advertisement and Discovery (LAGAD) mechanism [LAGAD].

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 varied. Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support highly mobile vehicles [H-DMM]. [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]. Nguyen et al. extended their previous works on a vehicular adapted DMM considering a Software-Defined Networking (SDN) architecture [SDN-DMM].

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.

4.1.5. Service Discovery

For service discovery, as a popular existing service discovery protocol, DNS-based Service Discovery (DNS-SD) [RFC6763] with mDNS [RFC6762] provides service discovery. Vehicular ND [ID-Vehicular-ND] proposes an extension of IPv6 ND for the prefix and service discovery.

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) [Securing-VCOMM]. Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks [VNET-AAA].

4.2. General Problems

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

4.2.1. Vehicular Network Architecture

Figure 1 shows an architecture for V2I and V2V networking in a road network. The two RSUs (RSU1 and RSU2) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. TCC is connected to the Vehicular Cloud and the two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and the last vehicle (Vehicle3) is wirelessly connected to RSU2. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication. Vehicle1 can communicate with Vehicle3 via RSU1 and RSU2 via V2I communication.

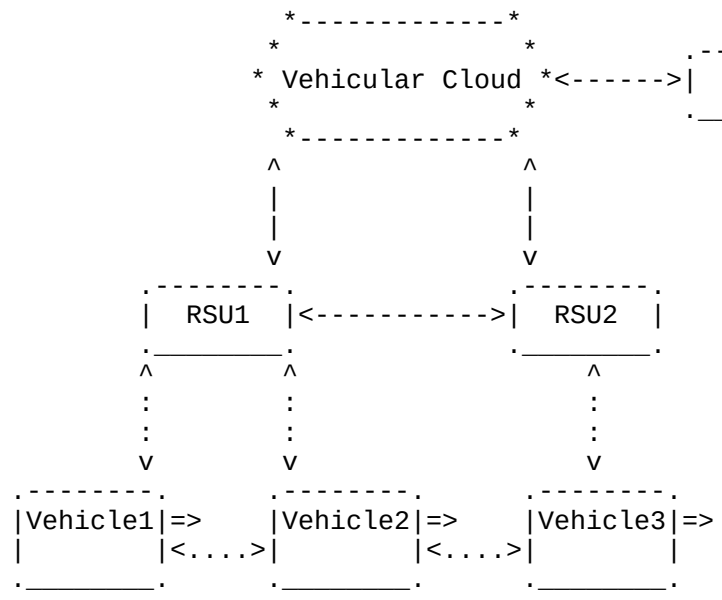

Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

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. ID/Pseudonym change for privacy requires a lightweight DAD. IP tunneling should be avoided for performance efficiency. The mobility information of a mobile device (e.g., vehicle), such as trajectory, position, speed, and direction, can be used by the mobile device and infrastructure nodes (e.g., TCC and RSU) for the accommodation of proactive protocols because it is usually equipped with a GPS receiver. Vehicles can use the TCC as its Home Network, so the TCC maintains the mobility information of vehicles for location management.

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: (i) an efficient mechanism for the IPv6 address assignment and DAD, (ii) on-demand IP mobility based on Proxy Mobile IPv6

(PMIPv6), and (iii) one-hop and two-hop communications for I2V and V2I networking.

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 recommebs that the IPv6 addressing assignment should follow considerations for ad-hoc link models, defined in [RFC5889] for nodes' mobility and link variability.

Petrescu et al. proposed the joint IP networking and radio architecture for V2V and V2I communication in [Joint-IP-Networking]. 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.

4.2.1.1. V2I-based Internetworking

This section discusses the internetworking between a vehicle's moving network and an RSU's fixed 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. The method of prefix assignment for each subnet inside the vehicle's mobile network and the RSU's fixed network is out of scope for this document. Internetworking between two internal networks via either V2I or V2V communication requires an exchange of network prefix and other parameters.

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, LTE D2D, Bluetooth, and LiFi) 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.

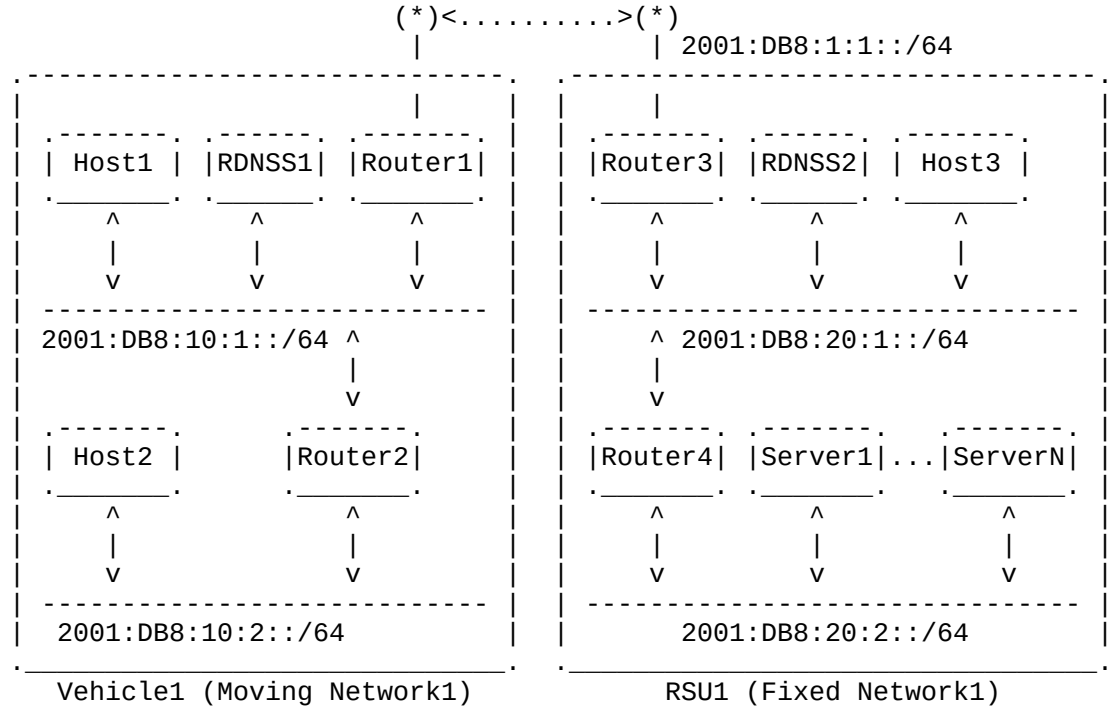

Figure 2: Internetworking between Vehicle Network and RSU Network

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 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.

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 (RDNSS1), 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 (RDNSS2), 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 in Figure 3.

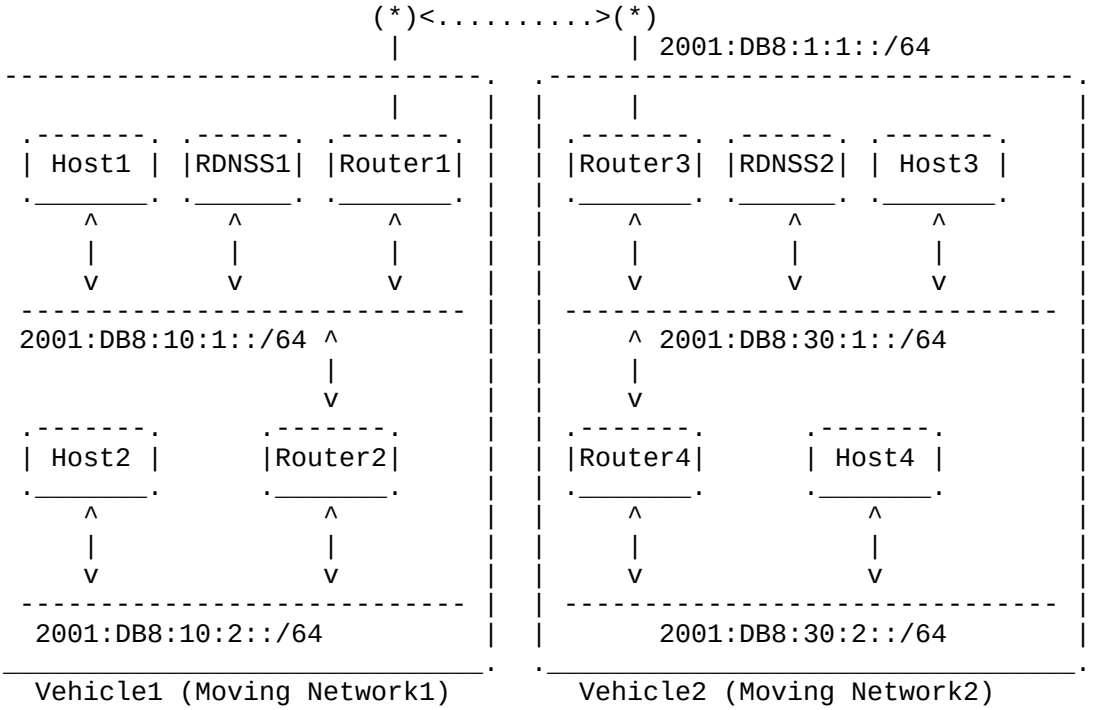

Figure 3: Internetworking between Two Vehicle Networks

In Figure 3, the prefix assignment for each subnet inside each vehicle's mobile network is done through a prefix delegation protocol.

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 (RDNSS1), 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 (RDNSS2), the two hosts (Host3 and Host4), and the two routers (Router3 and Router4). Vehicle1's Router1 (called mobile router) and Vehicle2's Router3 (called mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking.

The differences between IPWAVE (including Vehicular Ad Hoc Networks (VANET)) and Mobile Ad Hoc Networks (MANET) are as follows:

- IPWAVE is not power-constrained operation;
- Traffic can be sourced or sinked outside of IPWAVE;
- IPWAVE shall support both distributed and centralized operations;
- No "sleep" period operation is required for energy saving.

4.2.2. Latency

The communication delay (i.e., latency) between two vehicular nodes (vehicle and RSU) should be bounded to a certain threshold. 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, so the feasibility of IP-based safety applications is not tested yet.

4.2.3. Security

Security protects vehicles roaming in road networks from the attacks of malicious vehicular nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious vehicular 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. 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 privacy, pseudonym for a vehicle’s network interface is used, which the interface’s identifier is changed periodically. Such a pseudonym affects an IPv6 address based on the network interface’s identifier, and a transport-layer session with an IPv6 address pair. The pseudonym handling is not implemented and test yet for applications on IP-based vehicular networking.

5. Problem Exploration

5.1. IPv6 over IEEE 802.11-OCB

IPv6 over IEEE 802.11-OCB generally follows the standard IPv6 procedure. [IPv6-over-80211-OCB] specifies several details for IPv6 packets transporting over IEEE 802.11-OCB. Especially, an Ethernet Adaptation (EA) layer is suggested to be inserted between Logical Link Control layer and Network layer. The EA layer is mainly in charge of transforming some parameters between 802.11 MAC layer and IPv6 layer.

5.2. 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 and V2I). The vehicles are moving fast within the communication coverage of a vehicular node (e.g., vehicle and RSU). The external 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 for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase for the NA messages to collide with other NA messages with lower collision probability.

5.2.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in WAVE [IPv6-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 a WAVE link model.

Also, in an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix are on the same IP link. Hence, there is a relationship between link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. Such a relationship does not hold in a WAVE link model due to node mobility and highly dynamic topology.

Thus, IPv6 ND should be extended to support the concept of a link for an IPv6 prefix in terms of multicast in VANET.

5.2.2. MAC Address Pseudonym

As the ETSI GeoNetworking, 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. For the continuity of an end-to-end transport-layer (e.g., TCP, UDP, and SCTP) session, the IP addresses of the transport-layer session should be notified to both the end points and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address.

5.2.3. 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, the network prefix dissemination or exchange is required. It is assumed that a vehicular node has an external network interface and its internal network. The standard IPv6 ND needs to be extended for the communication between the internal-network vehicular nodes by letting each of them know the other side’s prefix with a new ND option [ID-Vehicular-ND].

5.2.4. Routing

For Neighbor Discovery in vehicular networks (called vehicular ND), Ad Hoc routing is required for either unicast or multicast in the links in a connected VANET with the same IPv6 prefix [GeoSAC]. Also, a rapid DAD should be supported to prevent or reduce IPv6 address conflicts in such links.

5.3. 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 navigator as a dedicated navigation system or a smartphone App. With this GPS navigator, vehicles can share their current position and trajectory (i.e., navigation path) with TCC. TCC can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory). With the prediction of the vehicle mobility, TCC supports RSUs to perform DAD, data packet routing, and handover in a proactive manner.

5.4. 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].

5.5. 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, which is a coordinator for the access to wireless channels.

5.6. 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-Considerations-802]. Since serveral procedures and functions based on IPv6 use multicast for control-plane messages, such as Neighbor Discovery (called ND) and Service Discovery, [Multicast-Considerations-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.

5.7. DNS Naming Services and Service Discovery

When two vehicular nodes communicate with each other with 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 recursive DNS server (RDNSS) 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].

5.8. IPv6 over Cellular Networks

IP has been supported in celluar networks since the time of General Packet Radio Service (GPRS) in the 2nd generation cellular networks of Global System for Mobile communications (2G-GSM) developed and maintained by the 3rd Generation Partnership Project (3GPP). The 2G and 3G-based radio accesses separate end-user data traffic (User Plane) from network transport traffic among network elements (Transport Plane). The two planes run independently in terms of addressing and the IP version. The Transport Plane forms tunnels to transport user data traffic [IPv6-3GPP-Survey].

The 4G-Long-Term-Evolution (4G-LTE) radio access simplifies the complex architecture of GPRS core network by introduing the Evolved Packet Core (EPC). Both 2G/3G and 4G-LTE system use Access Point Name (APN) to bridge user data and outside network. User traffic is transported via Packet Data Protocol (PDP) Contexts in GPRS, and Packet Data Network (PDN) Connections in EPC. Different traffics at a user equipment (UE) side need to connect to different APNs through multiple PDP Contexts or PDN Connections. Each of the context or the connection needs to have its own IP address.

IPv6 is partially supported in 2G/3G and 4G-LTE. In 2G/3G, a UE can be allocated an IPv6 address via two different ways, IPv6 and IPv4v6 PDP Contexts. By IPv4v6 PDP Context, both an IPv4 address and an /64 IPv6 prefix are allocated. In 4G-LTE, the IPv6 address allocation has a different process compared with that in 2G/3G networks. The major difference is that 4G-LTE builds the IP connectivity at the beginning of a UE attachment, whereas the IP connectivity of 2G/3G networks is created on demand. All 3GPP networks (i.e., 2G/3G and 4G-LTE) only support SLAAC address allocation, and do not suggest performing DAD. In addition, 3GPP networks remove link-layer address resolution, e.g., ND Protocol for IPv6, due to the assumption that the GGSN (Gateway GPRS Support Node) in 2G/3G networks or the P-GW (Packet Data Network Gateway) in 4G-LTE network is always the first-hop router for a UE.

Recently, 3GPP has announced a new technical specification, Release 14 (3GPP-R14), which proposes an architecture enhancements for vehicle-to-everything (V2X) services using the modified sidelink interface that originally is designed for the LTE Device-to-Device

(LTE-D2D) communications. 3GPP-R14 regulates 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.

5.8.1. 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 consider 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 [TS-23285-3GPP] states that both IP based and non-IP based V2X messages are supported, and only IPv6 is supported for IP based messages. Moreover, [TS-23285-3GPP] instructes that a UE autoconfigures a link- local IPv6 address by following [RFC4862], but without sending Neighbor Solicitation and Neighbor Advertisement messages for DAD.

5.8.2. Cellular V2X (C-V2X) Using 5G

The emerging services, functions and applications in automotive industry spurs ehhanced V2X (eV2X)-based services in the future 5G era. The 3GPP Technical Report [TS-22886-3GPP] is studying new use cases for V2X using 5G in the future.

5.9. Security and Privacy

Security and privacy are paramount in the V2I and V2V networking in vehicular networks. Only authorized vehicles should be allowed to use the V2I and V2V 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 authenticate a vehicle and the user through a road infrastructure node, such as an RSU connected to an authentication server in TCC. Transport Layer Security (TLS) certificates can also be used for secure vehicle communications.

For secure V2I communication, the 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, the secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

The security for vehicular networks should provide vehicles with AAA services in an efficient way. It should consider not only horizontal handover, but also vertical handover since vehicles have multiple wireless interfaces.

To prevent an adversary from tracking a vehicle by with its MAC address or IPv6 address, 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 communications between two vehicular nodes (e.g., vehicle and RSU).

6. Security Considerations

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

The security and privacy for key components in vehicular networking, such as IP address autoconfiguration, routing, mobility management, DNS naming service, and service discovery, needs 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-Cuise-Control]
California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", [Online] Available: http://www.path.berkeley.edu/research/automated-and-connected-vehicles/cooperative-adaptive-cruise-control, 2017.

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

[DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), October 2010.

[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.

[FirstNet]
U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", [Online] Available: https://www.firstnet.gov/, 2012.

[FirstNet-Annual-Report-2017]
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.

[ID-DNSNA]
Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-03 (work in progress), July 2018.

[ID-Vehicular-ND]
Jeong, J., Ed., Shen, Y., Jo, Y., Jeong, J., and J. Lee, "IPv6 Neighbor Discovery for Prefix and Service Discovery in Vehicular Networks", draft-jeong-ipwave-vehicular-neighbor-discovery-03 (work in progress), July 2018.

[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]
IEEE 802.11 Working Group, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2012, February 2012.

[IEEE-802.11p]
IEEE 802.11 Working Group, "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.

[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.

[IPv6-3GPP-Survey]
Soininen, J. and J. Korhonen, "Survey of IPv6 Support in 3GPP Specifications and Implementations", IEEE Communications Surveys & Tutorials, January 2015.

[IPv6-over-80211-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-25 (work in progress), June 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-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.

[Multicast-Considerations-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.

[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.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[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.

[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.

[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.

[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.

[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-22886-3GPP]
3GPP, "Study on Enhancement of 3GPP Support for 5G V2X Services", 3GPP TS 22.886, June 2018.

[TS-23285-3GPP]
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, 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. 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 B. 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), and Francois Simon (Pilot). 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
Department of Electrical Engineering
Universidad de Chile
Av. Tupper 2007, Of. 504
Santiago, 8370451
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

Appendix C. Changes from draft-ietf-ipwave-vehicular-networking-02

The following changes are made from draft-ietf-ipwave-vehicular-networking-02:

- The overall structure of the document is reorganized for the problem statement for IPWAVE.

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