Revision Letter

Editor: Jaehoon (Paul) Jeong
Date: June 29, 2020

OLD: draft-ietf-ipwave-vehicular-networking-14
NEW: draft-ietf-ipwave-vehicular-networking-15

Dear IPWAVE WG,
In this revision letter, I show how I revised our IPWAVE Problem Statement (PS) Draft with the following eight reviewers:

1. Nancy Cam-Winget (Cisco)
2. Fred L. Templin (The Boeing Company)
3. Jung-Soo Park (ETRI)
4. Zeungil (Ben) Kim (Hyundai Motors)
5. Kyoungjae Sun (Soongsil University)
6. Zhiwei Yan (CNNIC)
7. Yong-Joon Joe (LSware)
8. Peter E. Yee (Akayla)

I sincerely appreciate their in-depth review, feedback and suggestions to improve our WG draft.

The reviewers' comments use bold font and my responses use regular font.

Reviewer 1. Nancy Cam-Winget (Cisco)

Hi,
I have reviewed https://tools.ietf.org/html/draft-ietf-ipwave-vehicular-networking-14 and have quite a few comments.

Most of them relate to whether this document is meant to lay out challenges of using current IPv6 standards+extensions

In vehicular networks only, or if requirements are to be listed. The abstract and intro elude to requirements, but I didn't

see these listed out or if they did, they were not placed in any consistent way….

=> This version includes the requirements in both the abstract and introduction.

Abstract (Page 1): The 1st Paragraph

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

Section 1. Introduction (Page 1): The 1st Paragraph

OLD	NEW
Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC] in the Intelligent Transportation Systems (ITS) with the frequency band of 5.850 - 5.925 GHz (i.e., 5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. The European Union (EU) allocated radio spectrum for safety-related and non-safety-related applications of ITS with the frequency band of 5.875 - 5.905 GHz, as part of the Commission Decision 2008/671/EC [EU-2008-671-EC].	Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC] in the Intelligent Transportation Systems (ITS) with the frequency band of 5.850 - 5.925 GHz (i.e., 5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. The European Union (EU) allocated radio spectrum for safety-related and non-safety-related applications of ITS with the frequency band of 5.875 - 5.905 GHz, as part of the Commission Decision 2008/671/EC [EU-2008-671-EC].

For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety services based on DSRC for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC of the DSRC, while IEEE 1609.2 [WAVE-1609.2] covers security aspects, IEEE 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE 1609.4 [WAVE-1609.4] specifies the multi-channel operation. IEEE 802.11p was first a separate amendment, but was later rolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) in 2012 [IEEE-802.11-OCB]. Along with these WAVE standards, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213]) can be applied to vehicular networks. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6]. This document describes use cases and a problem statement about IPv6-based vehicular networking for ITS, which is named IPv6 Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, it makes a problem statement about key aspects in IPWAVE, namely, IPv6 Neighbor Discovery (ND), Mobility Management (MM), and Security & Privacy (SP). For each key aspect of the problem statement, this document specifies requirements for IPv6-based vehicular networking. This document is intended to	For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety services based on DSRC for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC of the DSRC, while IEEE 1609.2 [WAVE-1609.2] covers security aspects, IEEE 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE 1609.4 [WAVE-1609.4] specifies the multi-channel operation. IEEE 802.11p was first a separate amendment, but was later rolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) in 2012 [IEEE-802.11-OCB]. 3GPP has standardized Cellular Vehicle-to-Everything (C-V2X) communications to support V2X in LTE mobile networks (called LTE V2X) and V2X in 5G mobile networks (called 5G V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. With C-V2X, vehicles can directly communicate with each other without relay nodes (e.g., eNodeB in LTE and gNodeB in 5G). Along with these WAVE standards, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213]) can be applied to vehicular networks. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6][ISO-ITS-IPv6-AMD1]. This document describes use cases and a problem statement about IPv6-based vehicular networking for ITS, which is named IPv6 Wireless Access in Vehicular

motivate development of key protocols for IPWAVE.	Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then lists up requirements for the extensions of those IPv6 protocols, which are tailored to IPv6-based vehicular networking. Thus, this document is intended to motivate development of key protocols for IPWAVE.

Terminology:

V2D vs. V2P: it would be good to better classify the "device" as IoT device types are many similarly for "person". Of interest here, especially for security and privacy considerations, is a device a M2M device or is it one where one can expect to be driven by a human (e.g. mobile phone). I am presuming it is the former as you have V2P and I'm not sure the intent is that the vehicle communicates directly to a human but rather to a device that is being controlled by a human.

=> V2D replaces V2P since V2D means the communication between a vehicle and a pedestrian's smartphone (or an IoT device). Also, V2I2P is replaced with V2I2D.

Section 2. Terminology (Page 6): The 2nd Paragraph

OLD	NEW
o V2D: "Vehicle to Device". It is the wireless communication between a vehicle and a device (e.g., IoT device). o V2P: "Vehicle to Pedestrian". It is the wireless communication between a vehicle and a pedestrian's mobile device (e.g., smartphone). o V2I2P: "Vehicle to Infrastructure to Pedestrian". It is the wireless communication between a vehicle and a pedestrian's mobile device (e.g., smartphone) via an infrastructure node (e.g., IP-RSU).	o V2D: "Vehicle to Device". It is the wireless communication between a vehicle and a device (e.g., smartphone and IoT device). o V2I2D: "Vehicle to Infrastructure to Device". It is the wireless communication between a vehicle and a device (e.g., smartphone and IoT device) via an infrastructure node (e.g., IP-RSU).

There is a typo in “Edge Network (EN) : In” the “In” should be EN.
=> “In” is replaced with ”It” to represent “EN”.

Section 3:

This sentence is awkward:

“Thus, the IPv6

for these use cases should be extended for vehicular IPv6 such that

the IPv6 can support the functions of the network layer protocol such

as Vehicular Neighbor Discovery (VND), Vehicular Mobility Management

(VMM), and Vehicular Security and Privacy (VSP) in vehicular

networks.”

I think the intent is for this document to describe the motivation for why IPv6 and its protocols need to be extended in order to support “vehicular networks”. I would suggest reworking this paragraph and the next to something like:

“The use cases presented in this section serve as the description and motivation for the need to extend IPv6 and its protocols to facilitate ‘vehicular IPv6’. Section 5 summarizes the overall problem statement and IPv6 requirements.”
=> The suggested text looks good, so the following change is performed.

Section 3. Use Cases (Page 6): The 3rd Paragraph

OLD	NEW
Since IP is widely used among various computing devices in the Internet, it is expected that the use cases in this section need to work on top of IPv6 as the network layer protocol. Thus, the IPv6 for these use cases should be extended for vehicular IPv6 such that the IPv6 can support the functions of the network layer protocol such as Vehicular Neighbor Discovery (VND), Vehicular Mobility Management (VMM), and Vehicular Security and Privacy (VSP) in vehicular networks. Note	IP is widely used among popular end-user devices (e.g., smartphone and tablet) in the Internet. Applications (e.g., navigator application) for those devices can be extended such that the V2V use cases in this section can work with IPv6 as a network layer protocol and IEEE 802.11-OCB as a link layer protocol. The use cases presented in this section serve as the description and motivation for the need to extend IPv6 and its protocols to facilitate

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

Section 3.1

· “ navigation for driving safety” : should that be “safely” or “for providing driving safety plans”?
=> “driving safety” is replaced with “safe driving” in the draft.

The 2nd paragraph of this section doesn’t provide a rationale for why IPv6 needs to support single-hop or multi-hop in a wireless medium. The wireless hops are controlled at the link not MAC layer (e.g. IPv6). There is more clarification or description that better highlights why IPv6 (as a dependency with the link layer?) is relevant.
=> We address why the IPv6 needs to support both single-hop and multi-hop communications in a wireless medium as follows.

Section 3.1. V2V (Page 8): The 7th Paragraph

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

While these use cases are relevant, the descriptions merely describe the uses for the application layer signaling. I presume that for efficiency and expediency (e.g. to deal with minimal latency), the services for establishing neighbors in a V2V topology it is best done

at the IPv6 layer, vs. the 802.11p layer? But that is not really well described or clarified other than “Since IP is widely used among various computing devices in the Internet, it is expected that the use cases in this section need to work on top of IPv6 as the network layer protocol.” In the beginning of this full section. More motivation at the beginning of the section for why it has to be at IPv6 layer should help to address the neighbor discovery, but also a better description for why the security scope for these scenarios will help provide the reasoning for why security extensions in IPv6 are needed.

=> Popular end-user devices (e.g., smartphone and tablet) use IP for the Internet connectivity. The applications (e.g., navigator application) for those devices can be extended easily to support the V2V use cased in this section using IPv6 and IEEE 802.11-OCB as a network layer and a link layer, respectively as follows.

Section 3. Use Cases (Page 6): The 2nd Paragraph

OLD	NEW
Since IP is widely used among various computing devices in the Internet, it is expected that the use cases in this section need to work on top of IPv6 as the network layer protocol.	IP is widely used among popular end-user devices (e.g., smartphone and tablet) in the Internet. Applications (e.g., navigator application) for those devices can be extended such that the V2V use cases in this section can work with IPv6 as a network layer protocol and IEEE 802.11-OCB as a link layer protocol. In addition, IPv6 security needs to be extended to support those V2V use cases in a safe, secure, privacy-preserving way.

=> The necessity of IPv6 security for V2V is addressed as follows.

Section 3. Use Cases (Page 6): The 2nd Paragraph

OLD	NEW
Since IP is widely used among various computing devices in the Internet, it is expected that the use cases in this section need to work on top of IPv6 as the network layer protocol.	IP is widely used among popular end-user devices (e.g., smartphone and tablet) in the Internet. Applications (e.g., navigator application) for those devices can be extended such that the V2V use cases in this section can work with IPv6 as a network layer protocol and IEEE 802.11-OCB as a link layer protocol. In addition, IPv6 security needs to be extended to support those V2V use cases in a safe, secure, privacy-preserving way.

Section 3.2 and 3.3

· Similar to Section 3.1 a better explanation for why the “multi-hop” is required at IPv6 vs. at the link layer. Some mesh networks establish the hops at the link layer….then there’s RPL (RFC 6550) that speaks to constrained connected entities needing to establish connectivity. Their motivation is clear, while I’m not sure RPL can be used “as is”, their motivations seem similar so would expect to see some rationale for why the vehicular space is different than those listed in RFC6550 to help motivate the need for further work.
=> In a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). In this case, a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Even though RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks in RFC6550) supports a multihop routing, the network of RPL is assumed to either be a static topology or make a slow topology change, so it is hard to use RPL for a frequently changing network topology of Vehicular Ad Hoc Networks (VANET) as it is.

Section 4.1. Vehicular Network Architecture (Page 13): The 3rd Paragraph

OLD	NEW
The existing, well-known architecture such as PMIPv6 [RFC5213] can be extended to a vehicular network architecture (as shown in Figure 1) such that it can support wireless multi-hop V2I, multi-hop V2V, and multi-hop V2X (or V2I2X).	An existing network architecture (e.g., an IP-based aeronautical network architecture [OMNI-Interface], a network architecture of PMIPv6 [RFC5213], and a low-power and lossy network architecture [RFC6550]) can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. In a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). For example, RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

Section 4.1

Is the Traffic Control Center “all of the Vehicular Cloud” or is it meant to be 1 application or service in the cloud? They way it is depicted, it equated TCC = Vehicle cloud but the description in this section “…(TCC) is connected to the Vehicular Cloud for the management of IP-RSUs and vehicles in the road network” infers that it is an application in the cloud used to manage the connections between IP-RSUs and vehicles, is that correct?

Perhaps just use one of the terms (e.g. TCC) and define it as “TCC is a cloud application used to manage connections….”
=> TCC is part of a vehicular cloud for vehicular networks, and manages road network infrastructure nodes such as IP-RSUs and MAs as follows.

Section 2. Terminology (Page 5): The 15th Paragraph

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

Section 5

· There should be a space between “abovementioned”
=> “abovementioned” becomes “mentioned in Section 4.1” as follows.

Section 5. Problem Statement (Page 20): The 1st Paragraph

OLD	NEW
In order to specify protocols using the abovementioned architecture for VANETs, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking.	In order to specify protocols using the architecture mentioned in Section 4.1, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking.

· I might argue that timing constraints for a session between 2 vehicles or a moving vehicle to an IP-RSU would be in the same order of magnitude. The presumption made, which should be made explicit, is that IP-RSU’s are geographically fixed and are not expected to move, where are vehicles are highly mobile.
=> You are right for the same order of magnitude at those timing constraints, but if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU.

Section 5. Problem Statement (Page 20): The 2nd Paragraph

OLD	NEW
In order to specify protocols using the abovementioned architecture for VANETs, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively small compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles. This has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communications. Thus, this section presents key topics such as neighbor discovery and mobility management.	In order to specify protocols using the architecture mentioned in Section 4, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively small compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles. Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU. The time constraint of a wireless link between two nodes needs to be considered because it may affect the lifetime of a session involving the link. The lifetime of a session varies depending on the session's type such as a web surfing, voice call over IP, and DNS query. Regardless of a session's type, to guide all the IPv6 packets to their destination host, IP mobility should be supported for the session. Thus, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. This section presents key topics such as neighbor discovery and mobility management.

· I also believe the lifetime (or time-to-live) of a session should vary depending on the types of sessions being established, are there no considerations for these?

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

Section 5. Problem Statement (Page 20): The 3rd Paragraph

OLD	NEW
In order to specify protocols using the abovementioned architecture for VANETs, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively small compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles. This has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communications. Thus, this section presents key topics such as neighbor discovery and mobility management.	In order to specify protocols using the architecture mentioned in Section 4, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively small compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles. Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU. The time constraint of a wireless link between two nodes needs to be considered because it may affect the lifetime of a session involving the link. The lifetime of a session varies depending on the session's type such as a web surfing, voice call over IP, and DNS query. Regardless of a session's type, to guide all the IPv6 packets to their destination host, IP mobility should be supported for the session. Thus, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. This section presents key topics such as neighbor discovery and mobility

	management.

· From the descriptions, I would tease out that the problem and challenges arise from: (1) highly mobile environments, to differentiate this from voice calls or cellular mobility, there are considerations to the packet delivery and to the session establishment (2) the "units" (whether OBU or RSU) are highly constrained in cpu and memory (3) both the mobility and constrained environments should also bring in the considerations of the session lifetimes and key management used for these sessions. If this is the case, I would prefer to see these requirements made more explicit.
=> The hardware specifications of OBU and RSU are similar to those of laptop computers and routers, which are different from IoT devices. Thus, I think we do not need additional requirements for the OBU and RSU.

· But I am not seeing how these challenges provide a set of requirements. A section that summarizes or turns these challenges to requirements would help; the alternative is to make these subsections crisper into the requirements needed to address the challenges or gaps presented in IPv6 of each section.
=> I try to address the requirements in the subsections according to your comments in each subsection.

Section 5.1

· I am not sure what requirements or challenges the use cases are faced with to warrant IPv6 neighbor discovery. Given the requirements/challenges I listed in a previous bullet, by the time you get a IPv6 ND packet and process it, that particular entity may be out of reach. So, I think the problem or challenge faced here is that for these use cases, what is required is for a mechanism/protocol that allows for these nodes to securely advertise themselves (at the IP layer) with globally unique IPv6 addresses. I might counter that vehicle speed and density may be irrelevant if the goal for this requirement is to be able to get enough of the identity of the node you may want to connect to. Having the long prose description of the problems is OK (although much of this I believe is also already in RFC 8691), but it is hard to determine what is actually needed to fulfil these use cases.
=> I clarify the requirements of IPv6 ND for vehicular networks as follows. The requirements for IPv6 ND for vehicular networks are efficient DAD (Duplicate Address Detection) and NUD (Neighbor Unreachability Detection) operations. An efficient DAD is required to reduce the overhead of the DAD packets during a vehicle's travel in a road network, which guaranteeing the uniqueness of a vehicle's global IPv6 address. An efficient NUD is required to reduce the overhead of the NUD packets during a vehicle's travel in a road network, which guaranteeing the accurate neighborhood information of a vehicle in terms of adjacent vehicles and RSUs.

Section 5.1. Neighbor Discovery (Page 21): The 1st Paragraph and the 3rd Paragraph

OLD	NEW
IPv6 ND [RFC4861][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for point-to-point links and transit links (e.g., Ethernet). It assumes an efficient and reliable support of multicast from the link layer for various network operations such as MAC Address Resolution (AR) and Duplicate Address Detection (DAD). Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and run IPv6 ND.	IPv6 ND [RFC4861][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for point-to-point links and transit links (e.g., Ethernet). It assumes an efficient and reliable support of multicast and unicast from the link layer for various network operations such as MAC Address Resolution (AR), Duplicate Address Detection (DAD), and Neighbor Unreachability Detection (NUD). Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and run IPv6 ND. The requirements for IPv6 ND for vehicular networks are efficient DAD and NUD operations. An efficient DAD is required to reduce the overhead of the DAD packets during a vehicle's travel in a road network, which guaranteeing the uniqueness of a vehicle's global IPv6 address. An efficient NUD is required to reduce the overhead of the NUD packets during a vehicle's travel in a road network, which guaranteeing the accurate neighborhood information of a vehicle in terms of adjacent vehicles and RSUs.

Section 5.1.1

· **“wheh” should be “when”**
=> This typo is fixed by replacing “wheh” by “when”.

· **Perhaps I’m being too literal, “…can have multiple links between pairs of vehicles with wireless communication range, as shown in Figure 4.” I only see a single link between each vehicle pair?**
=> Yes, a single link is correct. I correct it as follows.

Section 5.1.1. Link Model (Page 23): The 4th Paragraph

OLD	NEW
A VANET can have multiple links between pairs of vehicles within wireless communication range, as shown in Figure 4.	A VANET can have a single link between each vehicle pair within wireless communication range, as shown in Figure 5.

Section 6

· Should this section follow the style of the "here are the requirements" that are not met in IPv6 security based on the challenges described? Or should this be more to provide the set of potential attacks that need to be addressed when considering the requirements (e.g. IPv6 "vehicular" deployment scenarios)? Neither come across strongly in this section.
=> Section 6 specifies possible attacks in vehicular networks, and the corresponding requirements for security. More potential attacks and countermeasures are explained in a separate I-D, draft-jeong-ipwave-security-privacy-01.
https://tools.ietf.org/html/draft-jeong-ipwave-security-privacy-01

· 2nd paragraph " Vehicles and infrastructure must be authorized in order to participate in vehicular networking." (e.g. must vs. need). Also, I see authorized, what about authenticated? The receiver must have assurances that the information is authentic, perhaps using privacy preserving techniques.
=> I agree with you that "authentication" is more appropriate than "authorization" for the admission control to vehicular networks. I reflect your comments on the text as follows.

Section 6. Security Considerations (Page 26): The 2nd Paragraph

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

· The last sentence of the paragraph needs to be qualified; that is, as this is the security considerations section, there needs to be at minimum examples (not necessarily exhaustive) of the types of attacks possible.
=> I shorten the description of a sybil attack as an example as follows.

Section 6. Security Considerations (Page 27): The 3rd Paragraph

OLD	NEW
Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe. For example, Sybil attack, which tries to confuse a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. This sybil attack needs to be prevented through the cooperation between good vehicles and IP-RSUs. Note that good vehicles are ones with valid certificates that are determined by the authentication process with an authentication server in the vehicular cloud. However, applications on IPv6-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.	Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safe driving applications (e.g., context-aware navigation, cooperative adaptive cruise control, and platooning), as explained in Section 3.1, the cooperative action among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) for disturbing safe driving. For example, a Sybil attack, which tries to confuse a vehicle with multiple false identities, may disturb a vehicle from taking a safe maneuver.

· Do vehicular networks need to provide confidentiality? For privacy reasons, I think this is a hard requirement? But there are some IEEE 1609 messages that are not encrypted?
=> Yes. Even though IEEE 1609.2 specifies security services for applications and management messages. This WAVE specification is optional, so if WAVE does not support the security of a WAVE frame, either the network layer or the transport layer need to support security services for the WAVE frames.

Section 6. Security Considerations (Page 27): The 6th Paragraph

OLD	NEW
For secure V2I communication, a secure channel between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e., IP-	For secure V2I communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router

RSU) in an EN needs to be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router (i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in another vehicle needs to be established, as shown in Figure 3.	(i.e., IP-RSU) in an EN needs to be established, as shown in Figure 3 [RFC4301][RFC4302][RFC4303][RFC4308][RFC7296]. Also, for secure V2V communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in another vehicle needs to be established, as shown in Figure 4. For secure communication, an element in a vehicle (e.g., an in-vehicle device and a driver/passenger's mobile device) needs to establish a secure connection (e.g., TLS) with another element in another vehicle or another element in a vehicular cloud (e.g., a server). Even though IEEE 1609.2 [WAVE-1609.2] specifies security services for applications and management messages. This WAVE specification is optional, so if WAVE does not support the security of a WAVE frame, either the network layer or the transport layer needs to support security services for the WAVE frames.

· 3rd paragraph is somewhat confusing, I think it is trying to state: "Strong security measures against lying nodes are required. As nodes communicate information that can be used by safety applications, protections to ensure the communication is authentic, protected from forgery and originates from an authorized node." The "authorized node" will require special considerations given the nature of the highly transient connections. I would argue that just because it is a valid certificate, does not make a vehicle "good", but perhaps you are trying to state that the assessment of what makes a "good" or "trusted" vehicle is outside the scope of this charter? Or is this meant to be a segue to the next paragraph, though that paragraph refutes using "valid certs" only.
=> You are right in that an authenticated vehicle with a valid certificate may do harm to its neighboring vehicles. I address this observation as follows.

Section 6. Security Considerations (Page 27): The 4th Paragraph

OLD	NEW
	Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles, so their

	communication activities need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play a role of peers in a consensus method of a blockchain such as Proof of Work (PoW) and Proof of Stake (PoS) [Bitcoin][Vehicular-BlockChain].

· I disagree that an unauthenticated VIN number is not sufficient to identify a car (note that there are instances in which VINs have changed when a vehicle's engine, for instance, gets replaced). Tighter requirements should be imposed as to when it is a Vehicle vs. a user on a device. The draft describes a Vehicle as having its own network so it would seem that each element in that network should be authenticated….there needs to be a better description of this in the security section. When describing a "Vehicle" are you identifying that network? A particular component of that network? A particular application in the host of the vehicle? Authentication is strong requirement, both at the message, transport and entity level; these need to be distinctly called out.

=> You are right. For a safe authentication, the elements in the network need to be authenticated individually. I clarify the authentication of an entity level and the authentication of a transport layer, respectively. Your comments are addressed as follows.

Section 6. Security Considerations (Page 27): The 5th Paragraph

OLD	NEW
To identify the genuineness of vehicles against malicious vehicles, an authentication method is required. A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the vehicular cloud. Also, Transport Layer Security (TLS) certificates can be used for the vehicle authentication to allow secure E2E vehicle communications. To identify the genuineness of vehicles against malicious	To identify malicious vehicles among vehicles, an authentication method is required. A Vehicle Identification Number (VIN) and a user certificate (e.g., X.509 certificate [RFC5280]) along with an in- vehicle device's identifier generation can be used to efficiently authenticate a vehicle or its driver (having a user certificate) through a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the vehicular cloud. This authentication can be used to identify the vehicle that will communicate with an infrastructure node or another vehicle. In the

vehicles, an authentication method is required. For vehicle authentication, information available from a vehicle or a driver (e.g., Vehicle Identification Number (VIN) and Transport Layer Security (TLS) certificate [RFC8446]) needs to be used to efficiently authenticate a vehicle or a user with the help of a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the vehicular cloud.	case where a vehicle has an internal network (called Moving Network) and elements in the network (e.g., in-vehicle devices and a user's mobile devices), as shown in Figure 3, the elements in the network need to be authenticated individually for safe authentication. Also, Transport Layer Security (TLS) certificates [RFC8446][RFC5280] can be used for an element's authentication to allow secure E2E vehicular communications between an element in a vehicle and another element in a server in a vehicular cloud, or between an element in a vehicle and another element in another vehicle.

· Is the paragraph on pseudonym trying to assert that "In order to propagate the notion of pseudonym, the IPv6 address must also be updated periodically?" This is the first paragraph where there is mention of a "long-living transport-layer session". The document should make clear the types of connections and their expected lifetimes….especially as it relates to pseudonyms and the expectation that an infrastructure (mobility case) would have to cache and manage these.
=> Yes. For a long-living transport-layer session (e.g., voice call over IP and video streaming service), MAC address pseudonym is required, and the IPv6 address needs to be updated accordingly by the MAC address change for the pseudonym.

Section 6. Security Considerations (Page 28): The 8th Paragraph

OLD	NEW
To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym needs to be provided to the vehicle; that is, each vehicle periodically updates its MAC address and the corresponding IPv6 address [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can	To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, especially for a long-living transport-layer session (e.g., voice call over IP and video streaming service), a MAC address pseudonym needs to be provided to each vehicle; that is, each vehicle periodically updates its MAC address and its IPv6 address needs to be updated accordingly by the MAC address change [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is

observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses.	performed without strong E2E confidentiality (using either IPsec or TLS), there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses. Thus, the MAC address pseudonym and the IPv6 address update should be performed with strong E2E confidentiality.

Let me know if the comments need further elaboration or clarification.
Warm regards, Nancy

Reviewer 2. Fred L. Templin (The Boeing Company)

Hi, I read this draft and have some comments. In the aviation domain, we are designing an Aeronautical Telecommunications Network with Internet Protocol Services (ATN/IPS) with the goal of having a worldwide IPv6 Internetwork interconnecting aircraft, air traffic controllers and other authorized entities. This work is focused in the International Civil Aviation Organization (ICAO), but is now being brought into the IETF:

https://datatracker.ietf.org/liaison/1676/
https://datatracker.ietf.org/doc/draft-templin-6man-omni-interface/
https://datatracker.ietf.org/doc/draft-templin-intarea-6706bis/

However, the vehicular network model we have for the airplanes differs significantly from the vehicular model in this ipwave draft when in fact I think there should be no difference.
=> The vehicular network model of the IPWAVE PS draft is similar to that of the 6MAN OMNI draft with the following mapping:
https://tools.ietf.org/html/draft-ietf-ipwave-vehicular-networking-15

IPWAVE PS Draft	OMNI Draft
IP-RSU	Access Router (AR)
Vehicle (IP-OBU)	Mobile Node (MN)
Moving Network	End User Network (EUN)
Mobility Anchor	Mobility Service Endpoint (MSE)
Vehicular Cloud	Internetwork Routing System (INET RS)

Thus, we refer to the OMNI draft for the vehicular network architecture as follows.

Section 4.1. Vehicular Network Architecture (Page 11): The 1st Paragraph

OLD	NEW
Figure 1 shows an exemplary vehicular network architecture for V2I and V2V in a road network. The vehicular network architecture contains vehicles, IP-RSUs, Vehicular Cloud, Traffic Control Center, and Mobility Anchor as components. However, some components in the vehicular network architecture may not be needed for vehicular networks, such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor.	Figure 1 shows an exemplary vehicular network architecture for V2I and V2V in a road network [OMNI-Interface]. The vehicular network architecture contains vehicles (including IP-OBU), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as components. Note that the components of the vehicular network architecture can be mapped to those of an IP-based aeronautical network architecture in [OMNI-Interface], as shown in Figure 2. These components are not mandatory, and they can be deployed into vehicular networks in various ways. Some of them (e.g., Mobility Anchor, Traffic Control Center, and Vehicular Cloud) may not be needed for the vehicular networks according to target use cases in Section 3.

In particular, in the ATN/IPS aircraft are statically configured with a Mobile Network Prefix (MNP) (sort of like a VIN) that travels with the aircraft wherever it goes. It uses this MNP to form a unique link-local address, then assigns the address to the OMNI interface which is a virtual interface configured over the wireless data link interfaces.
=> In the IPWAVE PS draft, there is no discussion on Mobile Network Prefix (MNP) for a moving network in a vehicle, but the delegation and configuration of the MNP can be included in the IPWAVE PS draft in the next revision.

Section 4.2. V2I-based Internetworking (Page 16): The 3rd Paragraph

OLD	NEW
As shown in Figure 3, as internal networks, a vehicle's moving network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for the communication with another vehicle or another EN. Internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the	As shown in Figure 3, as internal networks, a vehicle's moving network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for the communication with another vehicle or another EN. Internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the

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

Then, on the wireless links themselves, there are no on-link prefixes and no PIOs advertised by access routers. The wireless links therefore carry only link-local or MNP-addressed IPv6 packets, therefore no two vehicles will appear to be on the same subnet and no multi-link issues for subnet partitions and merges occur. Also, DAD is not needed at all due to the unique assignment of MNPs.

=> The usage of ULA (Unique Local Address) for the OMNI interface in the SPAN is a good solution for the multihop routing in the entire OMNI link of the SPAN. The IPv6 address autoconfiguration based on MNP does not need DAD because a unique IPv6 can be derived from the MNP and Interface ID (for MN) and the MNP and MSID (for AR and MSE).

Section 4.2. V2I-based Internetworking (Page 16): The 3rd Paragraph

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

This same model could be applied to ipwave vehicles, and would alleviate the problems stated in Section 5. In particular, the link model could adopt the OMNI link model (see the OMNI draft) where all nodes within the transportation system are "neighbors" on a shared NBMA virtual link. IPv6 ND works with no modifications, and the link model is always connected. So, there would be no need for vehicular extensions to IPv6 and ND.

Likewise, mobility management services would work the same as the ATN/IPS design and would not require any adaptations for fast-moving vehicles.

=> As you said, as another requirement in the IPWAVE draft, we can say that the vehicular link model needs to minimize the changes of IPv6, ND, and Mobility Management.

Section 5.1. Neighbor Discovery (Page 22): The 8th Paragraph

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

Section 5.1.1. Link Model (Page 24): The 7th Paragraph

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

Section 5.2. Mobility Management (Page 26): The 6th Paragraph

OLD	NEW
Therefore, for the proactive and seamless IPv6 mobility of vehicles, the vehicular infrastructure (including IP-RSUs and MA) needs to efficiently perform the mobility management of the vehicles with their mobility information and link-layer information.	Therefore, for the proactive and seamless IPv6 mobility of vehicles, the vehicular infrastructure (including IP-RSUs and MA) needs to efficiently perform the mobility management of the vehicles with their mobility information and link-layer information. Also, in IPv6-based vehicular networking, IPv6 mobility management should have minimum changes for the interoperability with the legacy IPv6 mobility management schemes such as PMIPv6, DMM, LISP, and AERO.

Final comment for now - the document lists only MIPv6 and PMIPv6 as example mobility services. We are considering them in the aviation domain, but also have AERO and LISP as candidate services. Since these would also apply in the ipwave case, it would be good to list them as candidates here also.
=> The IPWAVE PS draft can have AERO and LISP for mobility services as follows.

Section 1. Introduction (Page 3): The 4th Paragraph

OLD	NEW
Along with these WAVE standards, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275] and Proxy MIPv6 (PMIPv6) [RFC5213] can be applied to vehicular networks. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].	Along with these WAVE standards, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Locator/ID Separation Protocol (LISP) [RFC6830], and Asymmetric Extended Route Optimization (AERO) [RFC6706]) for IP mobility can be applied to vehicular networks. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].

Fred

Reviewer 3. Jung-Soo Park (ETRI)

Hi, all.

I reviewed IPWAVE draft and wrote down the humble comments.

#Clause 1.

At the third paragraph, my proposal is adding new reference, [ISO-ITS-IPv6-Amd1].

“Along with these WAVE standards, IPv6 …

For Land Mobile (CALM) [ISO-ITS-IPv6], [ISO-ITS-IPv6-Amd1].

=> A new reference of [ISO-ITS-IPv6- AMD1] is added.

Section 1. Introduction (Page 3): The 4th Paragraph

OLD	NEW
In addition, ISO has approved a standard	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].	specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6][ISO-ITS-IPv6-AMD1].

Section 7. Informative References (Page 31): The 17th Paragraph

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

#Clause 2.

-New term, V2X should be added.

Generally speaking, vehicle-to-everything (V2X) term is including V2I and V2V.

So, new term should be define in Clause 2 (Terminology) with a sentence excluding V2I and V2V use cases like a description of the first paragraph of Clause 3. And this term should also include the V2P and V2D use cases.

=> Vehicle-to-Everything (V2X) is defined as follows.

Section 2. Terminology (Page 6): The 23rd Paragraph

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

-About Edge Network (EN), "In" is changed to "It".
=> "In" is replaced by "It".

-About IP-OBU,

This term is currently focused on a vehicle.

In case of a Device or Pedestrian, I want to know whether the IP-OBU functionality is supported in them or not. I think this issue is solved in this term.
=> IP-OBU encompasses a vehicle and a device (e.g., a pedestrian's smartphone and IoT device) as follows.

Section 2. Terminology (Page 4): The 8th Paragraph

OLD	NEW
o IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle such as a car, bicycle, autobike or similar. It has at least one IP interface that runs in mode OCB of 802.11 and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP]. See the definition of the term "OBU" in [RFC8691].	o IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, autobike, motor cycle, and a similar one) and a device (e.g., smartphone and IoT device). It has at least one IP interface that runs in mode OCB of 802.11 and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP][TR-22.886-3GPP][TS-23.287-3GPP]. See the definition of the term "OBU" in [RFC8691].

-About Vehicle Detection Loop (i.e., Loop Detector),

This term is only used to define TCC in this document.

So, I think this term is useless.
=> Vehicle Detection Loop is deleted from the text.

#Clause 3,
-In Clause 3.1 V2V

In the first paragraph of Clause 3.1, these are four use cases of V2V networking.

The second "cruise control" use case is described for urban environment.

The third "platooning" is also described for the highway.

So, I suggest that "in an urban roadway" and "in a highway" is redundant at the second and third bullet points.
=> "Cruise control" and "platooning" are a little different from each other in that "cruise control" is for an individual vehicle and "platooning" is for a group of vehicles. Thus, I keep them as two use cases as follows.

Section 3.1. V2V (Page 7): The 1st Paragraph

OLD	NEW
The use cases of V2V networking discussed in this section include o Context-aware navigation for driving safety	The use cases of V2V networking discussed in this section include o Context-aware navigation for safe driving

and collision avoidance; o Cooperative adaptive cruise control in an urban roadway; o Platooning in a highway; o Cooperative environment sensing.	and collision avoidance; o Cooperative adaptive cruise control in a roadway; o Platooning in a highway; o Cooperative environment sensing.

Section 3.1. V2V (Page 7): The 4th Paragraph

OLD	NEW
Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles in an urban roadway or a highway. Thus, CACC can help adjacent vehicles to efficiently adjust their speed in an interactive way through V2V networking in order to avoid collision. … Platooning [Truck-Platooning] allows a series of vehicles (e.g., trucks) to follow each other very closely.	Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps individual vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles in an urban roadway or a highway. Thus, CACC can help adjacent vehicles to efficiently adjust their speed in an interactive way through V2V networking in order to avoid collision. … Platooning [Truck-Platooning] allows a series (or group) of vehicles (e.g., trucks) to follow each other very closely.

-In Clause 3.1

In "Cooperative-environment-sensing" use case, describing the reward system is better. For more active cooperation, the supporter of information should have the benefit.
=> A blockchain-based incentive system is described for such a reward system for "Cooperative-environment-sensing" use case.

Section 3.1. V2V (Page 8): The 7th Paragraph

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

-In Clause 3.3 V2X
V2I2X is not described in upper part.
=> We define V2I2X in the Terminology section as follows.

Section 2. Terminology (Page 6): The 22nd Paragraph

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

#Clause 4,
-In the fourth paragraph on page 12

We suggest like this;
“In the host-based mobility scheme, an IP-RSU plays a role of a home agent.” We propose just deleting the “in a visited network”.
=> I delete “in a visited network” from the text.

-In Clause 4.2 V2I-based Internetworking
In Figure 2, the internal network of Vehicle1 is constructed using wired and wireless. So, the internal network of Vehicle1 should be changed including two types of arrows (wired and wireless link) unlike EN1.
=> Though a driver’s or passenger’s mobile devices (e.g., smartphone and tablet PC) can connect to a router within the internal network of a vehicle, Figure 2 focuses on the in-vehicle devices (e.g., ECUs and sensors).

-In Figure 4,
It just comments. I think the Figure 4 can be used in Platooning environment.
In that case, a Host has a role of leading vehicle with driver’s operation. Others will be a driverless vehicles. So, star topology will be also used.
=> The use case of platooning is mentioned with a linear topology as follows.

Section 4.3. V2V-based Internetworking (Page 19): The 3rd Paragraph

OLD	NEW
Figure 5 shows multihop internetworking between the moving networks of two vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-OBU2 in Vehicle2, and IP-OBU3 in Vehicle3 in a linear	As a V2V use case in Section 3, Figure 5 shows the linear network topology of platooning vehicles for V2V communications where Vehicle3 is the leading vehicle with a driver, and Vehicle2 and Vehicle1 are the following vehicles without drivers.

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

#Clause 6
-In the second paragraph of Clause 6,
“Also, in-vehicle devices (e.g., ECU) and mobile devices (e.g., smartphone) in a vehicle need to …in another vehicle,”

I think that “mobile devices” can be existed out of the vehicle, just near the vehicle. And the pedestrian also has them. So, this sentence should be extended to include others such as pedestrian.
=> Since a driver and passengers can carry their mobile devices (e.g., smartphone and tablet PC) and let them connect to a router within a vehicle, the current text is clarified as follows.

Section 6. Security Considerations (Page 26): The 2nd Paragraph

OLD	NEW
Security and privacy are paramount in the V2I, V2V, and V2X networking. Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. Also, in-vehicle devices (e.g., ECU) and mobile devices (e.g., smartphone) in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers behind an IP-RSU in a secure way.	Security and privacy are paramount in V2I, V2V, and V2X networking. Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. Also, in-vehicle devices (e.g., ECU) and a driver/passenger’s mobile devices (e.g., smartphone and tablet PC) in a vehicle need to communicate with other in-vehicle devices and another driver/passenger’s mobile devices in another vehicle, or other servers behind an IP-RSU in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles’ information. In this case, an attack mitigation process may be required to reduce the aftermath of malicious behaviors.

#Clause 7
[ISO-ITS-IPv6-Amd1]
ISO/TC 204, Intelligent transport systems - Communications access for Land mobiles (CALM) - IPv6 Networking Amendment 1, September 2017.
=> This reference is added to Informative References section.

Thanks.

Jungsoo, PARK

Reviewer 4. Zeungil (Ben) Kim (Hyundai Motors)

Hi All

I reviewed IPWAVE draft and wrote down the comments the below for your reference.

[In page 3]
Since IPWAVE is IP based wireless standard it can be adapted with any access technology. I think it is better to emphasize clearly that we can use IPWAVE for vehicular network independent with radio access technology.

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213]) can be applied to vehicular networks.
--> Along with these WAVE standards or cellular networks, regardless of access technology, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile .....
=> The text is updated with the above guideline as follows.

Section 1. Introduction (Page 3): The 3rd Paragraph

OLD	NEW
Along with these WAVE standards, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213]) can be applied to vehicular networks. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].	3GPP has standardized Cellular Vehicle-to-Everything (C-V2X) communications to support V2X among vehicles in LTE and 5G mobile networks [TS-23.285-3GPP][TR-22.886-3GPP][TS-23.287-3GPP]. With C-V2X, vehicles can directly communicate with each other without relay nodes (e.g., eNodeB in LTE and gNodeB in 5G). Along with these WAVE standards and C-V2X standards, regardless of a wireless access

	technology under the IP stack of a vehicle, vehicular networks can operate IP mobility with IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Locator/ID Separation Protocol (LISP) [RFC6830], and Asymmetric Extended Route Optimization (AERO) [RFC6706]). In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6][ISO-ITS-IPv6-AMD1].

[In page 8]
I'd like to add up another comments for cooperative-environment-sensing.

Through the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment.

+ Vehicles can share their intended maneuvering information such as lane change, ramp out or in, cut in and abrupt braking.

It can help more efficient traffic flow and minimize unnecessary acceleration and deceleration to achieve best ride comfort.
=> These above sentences are added with the clarification of environmental information as follows.

Section 3.1. V2V (Page 8): The 6th Paragraph

OLD	NEW
Cooperative-environment-sensing use cases suggest that vehicles can share environmental information from various vehicle-mounted sensors, such as radars, LiDARs, and cameras with other vehicles and pedestrians. [Automotive-Sensing] introduces a millimeter-wave vehicular communication for massive automotive sensing. A lot of data can be generated by those sensors, and these data typically need to be routed to different destinations. In addition, from the	Cooperative-environment-sensing use cases suggest that vehicles can share environmental information (e.g., air pollution, hazards/ obstacles, slippery areas by snow or rain, road accidents, traffic congestion, and driving behaviors of neighboring vehicles) from various vehicle-mounted sensors, such as radars, LiDARs, and cameras with other vehicles and pedestrians. [Automotive-Sensing] introduces a millimeter-wave vehicular communication for massive

perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver-operated vehicles. Through the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment.	automotive sensing. A lot of data can be generated by those sensors, and these data typically need to be routed to different destinations. In addition, from the perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver-operated vehicles. Through the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment. Vehicles can also share their intended maneuvering information (e.g., lane change, speed change, ramp in-and-out, cut-in, and abrupt braking) with neighboring vehicles. Thus, this information sharing can help the vehicles behave as more efficient traffic flows and minimize unnecessary acceleration and deceleration to achieve the best ride comfort.

Besides this information, vehicles can exchange various non-safety but useful information with each other like file sharing, fuel efficiency information.

How about add practical use case for EV(Electric Vehicle) ?
o Navigation service;
o Energy-efficient speed recommendation service;
o Accident notification service.
o Electric vehicle(EV) charging, EV energy management and over the air software update for vehicle ECU.

Charging station can act as IP-RSU. It can be connected to EV through wireless channel and provide a variety of IP based value added services like over the air update and media streaming as well as charging communication.
=> I use the above suggestion on electric vehicle as another use case of V2I as follows.

Section 3.2. V2I (Page 6): The 1st Paragraph and the 5th Paragraph

NEW
o Electric vehicle (EV) charging service. … An EV charging service with V2I can facilitates the efficient battery charging of EVs. In the case where an EV charging station is connected to an IP-RSU, an EV can be guided toward the deck of the EV charging station through a battery charging server connected to the IP-RSU. In

addition to this EV charging service, other value-added services (e.g., air firmware/software update and media streaming) can be provided to an EV while it is charging its battery at the EV charging station.

[In page 18]
typo

from happing in vehicular networks, --> from happening in vehicular networks
=> This typo is corrected.

Best wishes
Zeungil(Ben) Kim

Reviewer 5. Kyoungjae Sun (Soongsil University)

Hi, Paul

I reviewed your revised draft. Check my comments below.

1) In "2. Terminology", '[RFC7429]' was not hyperlinked. it is the only reference which is not hyperlinked.
=> This hyperlink problem seems to be caused by the xml2rfc tool of IETF. I see that the hyperlink is created well at https://xml2rfc.tools.ietf.org/.

2) In 3.1, position of paragraph starting with "The existing IPv6 protocol does not." may not suitable. I suggest to move this paragraph in front of last paragraph. For the same reason, similar paragraphs in 3.2 and 3.3 are suggested to move position.
=> According to your comments, I move such a paragraph starting with “The existing IPv6” in front of the last paragraph for Sections 3.1, 3.2, and 3.3.

3) In 3.2, when "TCC" is written firstly, there is no explanation for this abbreviation.
=> TCC is defined in Section 2. Terminology.

4) In 3.3, you explained about V2I2V use case. Can we say that the scenario you mentioned in the third paragraph is correct to define 'IP-RSU relaying'? If an edge computing is running and processing between vehicle and pedestrian, it seems to be two separated V2I communications between edge and two nodes.
=> The scenario for V2I2V is correct because an edge computing may perform the mobility management, but an actual V2I2V-based data path from a vehicle to its destination is V2I2V.

5) I suggest to move figure 1 under the chapter 4 because this figure was explained in chapter 4.1. For the same reason, Figure 2 can be placed under the chapter 4.2, and Figure 3 under the chapter 4.3.
=> Figures 1, 2, and 3 are relocated after they are mentioned in the text according to the above comments.

6) In fifth paragraph of 4.1, I think that "which are part of a Vehicular Cloud." is not necessary. Also, "which is a controller for the mobility management of vehicles." is not necessary because it seems to duplicate meaning for previous sentence.
=> Those two phrases are deleted.

7) In the first paragraph of 4.1, "However, some components..." is suggested to change in the way like "These components are not mandatory and there can be deployed in various ways".
=> The suggested text is reflected as follows:

Section 4.1. Vehicular Network Architecture (Page 13): The 2nd Paragraph

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

8) Second paragraph 4.1 seems to be specified PMIPv6 as a default mobility management protocol. If not, I suggest this paragraph to modify or remove.
=> This paragraph is revised such that a vehicular network architecture can be designed by referring to the existing network architectures such as an IP-based aeronautical network architecture [OMNI-Interface], a network architecture of PMIPv6 [RFC5213], and a low-power and lossy network architecture [RFC6550] as follows.

Section 4.1. Vehicular Network Architecture (Page 13): The 3rd Paragraph

OLD	NEW
The existing, well-known architecture such as PMIPv6 [RFC5213] can be extended to a vehicular network architecture (as shown in Figure 1) such that it can support wireless multi-hop V2I, multi-hop V2V, and multi-hop V2X (or V2I2X).	An existing network architecture (e.g., an IP-based aeronautical network architecture [OMNI-Interface], a network architecture of PMIPv6 [RFC5213], and a low-power and lossy network architecture [RFC6550]) can be extended to a vehicular network architecture

	for multihop V2V, V2I, and V2X, as shown in Figure 1. In a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). For example, RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

9) In 4.1, SDN concept pops up in sudden and it is used for mobility management. If you want to add CP/DP separation concept for mobility management, I think that CP/DP separation definition and explanation which is defined in the DMM WG will be better. In "draft-ietf-dmm-fpc-cpdp", they defined Forwarding Policy Configuration (FPC) architecture which adapts CP/DP separation. I think this document can be helpful.
=> I refer to "draft-ietf-dmm-fpc-cpdp-13" for the separation of control plane (CP) and data plane (DP) through the SDN concept.

Best Regards,

KJ.

Reviewer 6. Zhiwei Yan (CNNIC)

Hi, All,
I reviewed this IPWAVE PS draft and have the following comments for your reference:
1) In Section 1, the ITS/WAVE based standards are introduced, but the IPv6/MIPv6/PMIPv6 are not so proper here because these protocols (as other TCP/IP protocols) are not dedicated to ITS. Then it will be better if there is some works/extensions to be added particular for ITS based on IPv6.
=> I add more mobility management schemes for a reference model for vehicular networks. We can design a new mobility management scheme tailored for ITS later.

Section 1. Introduction (Page 3): The 4th Paragraph

OLD	NEW
Along with these WAVE standards, IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213]) can be applied to	Along with these WAVE standards and C-V2X standards, regardless of a wireless access technology under the IP stack of a vehicle, vehicular networks can operate IP mobility

vehicular networks. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].	with IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Locator/ID Separation Protocol (LISP) [RFC6830], and Asymmetric Extended Route Optimization (AERO) [RFC6706]). In addition, ISO has approved a standard specifying the IPv6 network protocols and services o be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6][ISO-ITS-IPv6-AMD1].

2) In page 4, “Edge Network (EN): In is an access network” should be “Edge Network (EN): It is an access network”.
=> It is corrected as mentioned.

3) In page 4, why EC and ECD are for the sake of vehicles and pedestrians, while EN is only for the sake of vehicles?
=> As mentioned in the text in Section 2, EN is an access network having an IP-RSU for both wireless communication with other vehicles and wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and MA).

4) In page 4-5, the ITS related functions (such as measuring, sensing or communicating) can be executed by any device with the related ability. Then the draft should use “vehicle” (defined in Page5) as a representative “device” but not just denote “car” although typically it is “car”. It’s better to explains this more clearly and put this definition in front.
=> According to your comments, any device having an IP-OBU and a GPS receiver (e.g., smartphone and table PC) can be regarded as a vehicle in this document as follows.

Section 2. Terminology (Page 5): The 16th Paragraph

OLD	NEW
Vehicle: A Vehicle in this document is a node that has an IP-OBU for wireless communication with other vehicles and IP-RSUs. It has a radio navigation receiver of Global Positioning System (GPS) for efficient navigation.	Vehicle: A Vehicle in this document is a node that has an IP-OBU for wireless communication with other vehicles and IP-RSUs. It has a radio navigation receiver of Global Positioning System (GPS) for efficient navigation. Any device having an IP-OBU and a GPS receiver (e.g., smartphone and table PC) can be regarded as a vehicle in this document.

5) In Section 3, it will be clearer if the organization can be adjusted as: V2V/V2I/V2X definitions, use cases explanations of V2V/V2I/V2X and challenge analysis of these use cases under IPv6.
=> The text in Section 3 is reorganized to link the use cases and challenge analysis under IPv6 according to the comments of this reviewer and other reviewers.

6) In Subsection 4.1, more explanation is needed "However, some components in the vehicular network architecture may not be needed for vehicular networks, such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor." For example, because the related services are not deployed or requested.
=> The text is improved as follows.

Section 4.1. Vehicular Network Architecture (Page 11): The 1st Paragraph and the 2nd Paragraph

OLD	NEW
Figure 1 shows an exemplary vehicular network architecture for V2I and V2V in a road network. The vehicular network architecture contains vehicles, IP-RSUs, Vehicular Cloud, Traffic Control Center, and Mobility Anchor as components. However, some components in the vehicular network architecture may not be needed for vehicular networks, such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor.	Figure 1 shows an exemplary vehicular network architecture for V2I and V2V in a road network [OMNI-Interface]. The vehicular network architecture contains vehicles (including IP-OBU), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as components. Note that the components of the vehicular network architecture can be mapped to those of an IP-based aeronautical network architecture in [OMNI-Interface], as shown in Figure 2. These components are not mandatory, and they can be deployed into vehicular networks in various ways. Some of them (e.g., Mobility Anchor, Traffic Control Center, and Vehicular Cloud) may not be needed for the vehicular networks according to target use cases in Section 3.

7) In Subsection 4.1, the PMIPv6 is mentioned but it is very unexpected and sudden. It's better if the elements in Figure 1 can be explained first, and then the related communications can be explained and at last the adopted and extended protocols involved (such as OCB and PMIP) can be explained.
=> In Subsection 4.1, the elements in Figures (e.g., IP-RSU and TCC) are explained first, and the related communications is explained. Lastly, OCB and PMIP are explained for mobility management as follows.

Section 4.1. Vehicular Network Architecture (Page 13): The 4th Paragraph and the 5th Paragraph

NEW
As shown in this figure, IP-RSUs as routers and vehicles with IP-OBU have wireless media interfaces for VANET. Furthermore, the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking. Note that 2001:DB8::/32 is a documentation prefix [RFC3849] for example prefixes in this document, and also that any routable IPv6 address needs to be routable in a VANET and a vehicular network including IP- RSUs. In Figure 1, three IP-RSUs (IP-RSU1, IP-RSU2, and IP-RSU3) are deployed in the road network and are connected with each other through the wired networks (e.g., Ethernet). A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of IP-RSUs and vehicles in the road network. A Mobility Anchor (MA) may be located in the TCC as a mobility management controller. Vehicle2, Vehicle3, and Vehicle4 are wirelessly connected to IP-RSU1, IP-RSU2, and IP-RSU3, respectively. The three wireless networks of IP-RSU1, IP-RSU2, and IP-RSU3 can belong to three different subnets (i.e., Subnet1, Subnet2, and Subnet3), respectively. Those three subnets use three different prefixes (i.e., Prefix1, Prefix2, and Prefix3).

Section 4.1. Vehicular Network Architecture (Page 14): The 8th Paragraph

NEW
In wireless subnets in vehicular networks (e.g., Subnet1 and Subnet2 in Figure 1), vehicles can construct a connected VANET (with an arbitrary graph topology) and can communicate with each other via V2V communication. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the wireless communication range for each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., IP-RSU2 and IP- RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range for each other.

Section 4.1. Vehicular Network Architecture (Page 14): The 9th Paragraph

NEW
For IPv6 packets transported over IEEE 802.11-OCB, [RFC8691] specifies several details, including Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. An Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC layer and IPv6 network layer, which is located between IEEE 802.11-OCB's logical link control layer and IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IPv6-based vehicular networks.

An IPv6 mobility solution is needed in vehicular networks so that a vehicle's TCP session can be continued while it moves from an IP- RSU's wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session with a corresponding node in the vehicular cloud, Vehicle2 can move from IP- RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host- based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213]). In the host-based mobility scheme, an IP-RSU plays a role of a home agent. On the other hand, in the network-based mobility scheme, an MA plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213].

8) In Subsection 4.1, in page 12, the mobility management is mentioned, but it's better to describe mobility management as a protocol to guarantee the communication continuity. Because the mobility management protocols are not just used to maintain the TCP connectivity, but also to avoid the UDP packet loss or avoid the session disruption during network layer handover.

=> For the mobility management, the communication continuity of both a TCP session and a UDP session is explained as follows.

Section 4.1. Vehicular Network Architecture (Page 14): The 10th Paragraph

OLD	NEW
An IPv6 mobility solution is needed in vehicular networks so that a vehicle's TCP session can be continued while it moves from an IP- RSU's wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session with a corresponding node in the vehicular cloud, Vehicle2 can move from IP- RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host- based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213]). In the host-based mobility scheme, an IP-RSU plays a role of a home agent in a visited network. On the other hand, in the network-based mobility scheme, an MA plays a role of a mobility management	An IPv6 mobility solution is needed for the guarantee of communication continuity in vehicular networks so that a vehicle's TCP session can be continued, or UDP packets can be delivered to a vehicle as a destination without loss while it moves from an IP-RSU's wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a corresponding node in the vehicular cloud, Vehicle2 can move from IP-RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213]). In the host-based mobility scheme, an IP-RSU plays a role of a home

controller such as a Local Mobility Anchor (LMA) in PMIPv6, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213].	agent. On the other hand, in the network-based mobility scheme, an MA plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213].

9) In Subsection 4.1, in page 12, both the host-based mobility management protocol and network-based mobility management protocol are introduced, but only PMIP as network-based mobility management protocol is mentioned before this part. And “an IP-RSU plays a role of a home agent in a visited network.” It should be checked, whether MA acts as HA or IP-RSU acts as HA.
=> The revised text explains a host-based mobility scheme as well as a network-based mobility scheme. Also, the revised text lets MA act as HA in the similar way with PMIPv6.

Section 4.1. Vehicular Network Architecture (Page 14): The 10th Paragraph, the 11th Paragraph, and the 12th Paragraph

OLD	NEW
An IPv6 mobility solution is needed in vehicular networks so that a vehicle’s TCP session can be continued while it moves from an IP- RSU’s wireless coverage to another IP-RSU’s wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session with a corresponding node in the vehicular cloud, Vehicle2 can move from IP- RSU1’s wireless coverage to IP-RSU2’s wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host- based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213]). In the host-based mobility scheme, an IP-RSU plays a role of a home agent in a visited network. On the other hand, in the network-based mobility scheme, an MA plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213].	An IPv6 mobility solution is needed for the guarantee of communication continuity in vehicular networks so that a vehicle’s TCP session can be continued, or UDP packets can be delivered to a vehicle as a destination without loss while it moves from an IP-RSU’s wireless coverage to another IP-RSU’s wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a corresponding node in the vehicular cloud, Vehicle2 can move from IP-RSU1’s wireless coverage to IP-RSU2’s wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213]). In the host-based mobility scheme (e.g., MIPv6), an IP-RSU plays a role of a home agent. On the other hand, in the network-based mobility scheme (e.g., PMIPv6, an MA

	plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, which also serves vehicles as a home agent, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213]. The host-based mobility scheme needs client functionality in IPv6 stack of a vehicle as a mobile node for mobility signaling message exchange between the vehicle and home agent. On the other hand, the network-based mobility scheme does not need such a client functionality for a vehicle because the network infrastructure node (e.g., MAG in PMIPv6) as a proxy mobility agent handles the mobility signaling message exchange with the home agent (e.g., LMA in PMIPv6) for the sake of the vehicle. There are a scalability issue and a route optimization issue in the network-based mobility scheme (e.g., PMIPv6) when an MA covers a large vehicular network governing many IP-RSUs. In this case, a distributed mobility scheme (e.g., DMM [RFC7429]) can mitigate the scalability issue by distributing multiple MAs in the vehicular network such that they are positioned closer to vehicles for route optimization and bottleneck mitigation in a central MA in the network-based mobility scheme. All these mobility approaches (i.e., a host-based mobility scheme, network-based mobility scheme, and distributed mobility scheme) and a hybrid approach of a combination of them need to provide an efficient mobility service to vehicles moving fast and moving along with the relatively predictable trajectories along the roadways.

10) Why SDN can only be adopted in mobility management process?

=> In vehicular networks, Software-Defined Networking (SDN) [RFC7149] can be used to separate the control plane from the data plane for efficient mobility management and data forwarding. Also, SDN can be used for efficient mobility management in DMM as follows.

Section 4.1. Vehicular Network Architecture (Page 15): The 13th Paragraph

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

11) In Subsection 5.1, the ND protocol challenges are analyzed. This should be analyzed corresponding to the mobility management protocols deployed. If MIPv6 is used or without mobility management support, the vehicle needs to configure an IPv6 address in the shared link and then the DAD is needed. However, if PMIPv6 is used, the vehicle can receive a unique IPv6 prefix through the point-to-point link with RUS and then the DAD is unnecessary. And due to the applications in ITS always need the configuration to be finished as fast as possible, then the traditional DAD should not be used directly because its inefficiency.

=> You are right. For a mobility management scheme in a shared link, an efficient vehicular-network-wide DAD is required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 and OMNI), DAD is not required because the IPv6 address of a vehicle's external wireless interface is guaranteed to be unique. There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support an efficient mobility management. The discussion is added to Section 5.2 (Mobility Management) since the DAD issue is related to mobility management as follows.

Section 5.2. Mobility Management (Page 26): The 5th Paragraph

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

12) In Subsection 5.2, the mobility management should be performed more efficiently with the help of GPS and ND protocol (at least). Also here, the above problem exists because the vehicle may use PMIP or MIP. Besides, the vehicle may also use DHCP for address/prefix configuration but not only SLAAC.
=> The usage of GPS for proactive mobility management is explained as follows.

Section 5.2. Mobility Management (Page 25): The 2nd Paragraph

NEW
With a GPS navigator, efficient mobility management can be performed with the help of vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having IP-RSUs and an MA in TCC). This vehicular infrastructure can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the efficient mobility management (e.g., proactive handover).

=> The help of ND for efficient mobility management is explained as follows.

Section 5.2. Mobility Management (Page 26): The 5th Paragraph

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

=> The usage of DHCPv6 for address autoconfiguration is explained as follows.

Section 5.2. Mobility Management (Page 26): The 5th Paragraph

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

BR,
Zhiwei Yan

Reviewer 7. Yong-Joon Joe (LSware)

Hello,

I reviewed your revised draft, and here are my comments which focused on Section 6.

[Page 22]

(1)
>> "~~ need to communicate with other in-vehicle devices and mobile devices in another vehicle, [and -> and/or] other servers in an IP-RSU in a secure way."
When we do not have to connect to both in-vehicle devices and mobile devices, then 'and/or' is better than 'and'.
=> I use "or" because "A or B" means "A", "B", and "A and B" in logic.

(2)
>> "Even a perfectly authorized and legitimate vehicle may be hacked to run malicious applications to track and collect its and other vehicles' information."
The whole sentence is enclosed in 'Even'. 'Even a vehicle is perfectly authorized and legitimate, the vehicle may be hacked' is better than 'Even ~ may be hacked'. When a hacker's object is tracking and collecting and running malicious applications is only the method, 'for running malicious applications' is better than 'to run malicious application'.
=> "Even though a vehicle is perfectly authenticated and legitimate" and "for running malicious applications" are used.

(3)
>> "For safety applications, " 'For safety applications' could be shown as a security software as like as anti-virus. 'For application safety' seems to be proper for original intention.
=> Safety applications means application for safe driving, so I revise the sentence as follows.

Section 6. Security Considerations (Page 27): The 3rd Paragraph

OLD	NEW
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.	Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safe driving applications (e.g., context-aware navigation, cooperative adaptive cruise control, and platooning), as explained in Section 3.1, the cooperative action among vehicles is assumed.

(4)
>> "the cooperation among vehicles is assumed"
In general, the representation 'cooperation' seems to be no problem. However, in the Game Theory field, the word 'cooperation' does not always mean only '(full and friendly) cooperation', but also '()'. Of course, this document is not for economic/game theory. However, who is working in the security area may tackle this representation. When you want to represent this clearly, 'cooperative action' may be better.
=> I replace “cooperation” with “cooperative action”.

(5)
>> "Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe."
As like my comment (2), making someone(or a vehicle) unsafe is not the object of a hacker but a means for the original purpose. In this assumption, 'for disturbing safe drive' is proper than 'to make driving be unsafe'.

For example, a hacker would take a 'moderate' attack such as disseminating fake traffic info to neighbor vehicles to make other vehicles away from the front of the hacker by themselves. This case would be fit for a Sybil attack. (This could occur frequently because this is not so harmful to the others too much). Of course, this would be related to the path-finding algorithm and traffic-control algorithm. In my lab, we have studied a mechanism design such as False-Name Proofness in game theory.
=> I replace “to make driving be unsafe” with “for disturbing safe driving”.

(6)

>> "This Sybil attack needs to be prevented through the cooperation between good vehicles and IP-RSUs. Note that good vehicles are ones with valid certificates that are determined by the authentication process with an authentication server in the vehicular cloud."

I'm not sure that the representation 'good vehicle' is a common terminology, and the sentence is too long. How about 'This Sybil attack needs to be prevented through the cooperation between [good -> certified] vehicles and IP-RSUs. Note that vehicles would be certified by an authentication server in the vehicular cloud authenticate ????'

=> Though I agree that “certificated vehicles” is better, according to another reviewer (Nancy), I removed a sentence having “good vehicles”.

[Page 23]

(7)

>> "To identify the genuineness of vehicles against malicious vehicles, an authentication method is required."

I think 'To identify the genuineness of malicious vehicles', 'To identify a malicious vehicle from vehicles', or 'To identify the genuineness of malice from vehicles' seems to be better than the original form because of the expression 'genuineness'. Because we could not genuine malice but false(bogus) identity by an authentication. Of course, we could infer/decide a specific identity would be malice based on long-term observation. But I don't think this representation wants to say such a thing.

=> I use “To identify malicious vehicles among vehicles”.

I think authentication is a solution that is specialized for identifying false(bogus) identity to prevent Sybil attack, but not for the general solution against other malicious actions.

=> Yes, you are right. To observe malicious actions including Sybil attack, vehicles’ activities need to be logged in either a central way or a distributed way as follows.

Section 6. Security Considerations (Page 27): The 4th Paragraph

NEW
Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles, so their communication activities need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play a role of peers in a consensus method of a blockchain such as PoW and PoS [Bitcoin] [Vehicular-BlockChain].

>> A Vehicle Identification Number (VIN) and a user certificate along with an in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., IP-RSU) connected to an authentication server in

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

Section 6. Security Considerations (Page 27): The 5th Paragraph

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

(8)

>> "Also, Transport Layer Security (TLS) certificates can be used for the vehicle authentication to allow secure E2E vehicle communications"
In my knowledge, TLS is not for authentication but for channel(communication) security. Of course, during the TLS process, authentication by the certificate is performed. If this representation intends to say about the authentication by certificate, then it should refer to PKI[RFC5280].
=> RFC5280 is about Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. I let the document refer to RFC5280 for a user certificate.

Section 6. Security Considerations (Page 27): The 5th Paragraph

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

(9)
>> "A Vehicle Identification Number (VIN) and a user certificate along with an in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or a user

through a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the vehicular cloud."

In a driving environment, communication partners are changed frequently. (an IP-RSU would be a long-term communicating partner). In such a circumstance, I have a question that TLS is really efficient. Yes, when the vehicle wants to authenticate AND establish a secure channel at once, TLS seems to be only a solution presently. But, any vehicles which are not driving in the same direction, there would not enough time for establishing the TLS channel. (I'm not familiar with 5G and its hardware)

=> For the setup of a secure channel over TLS, the multihop V2I communications over DSRC need to involve multiple intermediate vehicles as relay nodes toward an IP-RSU connected to an authentication server in the vehicular cloud. The V2I over 5G V2X needs to allow a vehicle to communicate directly with a gNodeB connected to an authentication server in the vehicular cloud. This discussion is added to the text as follows.

Section 6. Security Considerations (Page 28): The 7th Paragraph

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

And, I have another question that PKI(or TLS certificate) is not enough solution against Sybil attack (using False identifier)

PKI could identify the bogus certificate.

However, when a hacker uses EXIST and VALID certificate(such as using certificates of the hacker's 2nd, 3rd, 4th car which is sleeping in his garage) for emitting fake information, PKI is not helpful because those certificates have no problem.

=> To detect the illegal activities, the following logging system is used.

Section 6. Security Considerations (Page 27): The 4th Paragraph

NEW
Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles, so their communication activities need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play a role of peers in a consensus method of a blockchain such as PoW and PoS [Bitcoin] [Vehicular-BlockChain].

(10)
>> "For secure V2I communication, a secure channel between a mobile router ..."
I think TLS should be emphasized in this paragraph.
=> TLS is specified as an example for a secure channel in V2I as follows.

Section 6. Security Considerations (Page 28): The 6th Paragraph

OLD	NEW
For secure V2I communication, a secure channel between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 2.	For secure V2I communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 3 [RFC4301][RFC4302][RFC4303][RFC4308][RFC7296].

(11)
MAC address pseudonym needs to be provided to [the -> each] vehicle
=> I replace “the vehicle” with “each vehicle”.

(12)
>>" For the mobility management, a malicious vehicle can construct multiple virtual bogus vehicles, and register them with IP-RSUs and MA. This registration makes the IP-RSUs and MA waste their resources. The IP-RSUs and MA need to determine whether a vehicle is genuine or bogus in the mobility management. Also, the confidentiality of control packets and data packets among IP-RSUs and MA, the E2E paths (e.g., tunnels) need to be protected by secure communication channels. In addition, to prevent bogus IP-RSUs and MA from interfering IPv6 mobility of vehicles, the mutual authentication among them needs to be performed by certificates (e.g., TLS certificate)."
I think this paragraph should be following after the first paragraph of page 23 "To identify the genuineness ~~".
=> Through the revision according to another reviewer (i.e., Nancy), the paragraph of “To identify the genuineness” has been updated, so this paragraph about the security of the mobility management seems to be in a right place.

Typos:

Have to unify representation about
*** 'one-hop' and 'one hop'**
*** 'multi-hop' and 'multihop'**
=> “one-hop” is used as adjective, and “one hop” is used as a noun phrase. “multihop” is used in the whole text.

Page #3

~~ to motivate [_ -> the] development of key protocols for IPWAVE.
A vehicle can make [_ -> a] safety plan by classifying
=> This comment is applied.

Page #6
'management' and 'security' is uncountable
VMM: It is [an -> _] IPv6-based mobility management for vehicular networks.
VSP: It is [an -> _] IPv6-based security and privacy for vehicular networks.
=> Since management and privacy are uncountable nouns, an article “an” cannot be used.

Page #7
an interactive way through V2V networking in order to avoid [_ -> a] collision.
Platooning can maximize the throughput of vehicular traffic in a highway and reduce [the -> _] gas consumption
=> “a collision” is used. “gas consumption” looks fine.

Page #8
such as VND and VSP are [prerequisite -> prerequisites] for the IPv6-based packet exchange
=> “prerequisites” are used.

Page #9
will be available for V2I and V2V in [_ -> the] near future.
are [prerequisite -> prerequisites] for the IPv6-based packet exchange
=> “the near future” is used. “prerequisites” are used.

Page #16
Figure 3 shows [_ -> an] internetworking between the moving networks of two neighboring vehicles
=> “the internetworking” is used because “internetworking” seems an uncountable noun.

Page #17
protocol exchanges need to be completed in a time relatively [small -> short] compared to the lifetime of a link between a vehicle
'support' is uncountable
It assumes [an -> _] efficient and reliable support
=> “short” is used. “the efficient and reliable support” is used.

Page #18
****
The merging and partitioning of VANETs [occurs frequently -> frequently occurs] in vehicular networks
to [efficiently -> _] work to support IPv6-based safety applications [_ -> efficiently].
=> These two are applied.

Page #19
A VANET can have multiple links between pairs of vehicles within [_ -> the] wireless communication range,
for example, [wheh -> when] they are Vehicle1 and Vehicle3, as shown in Figure 4.
to directly communicate with each other via VANET rather than indirectly via IP-RSUs.
=> During the revision, these sentences are not used.

Page #20
to [directly -> _] communicate with each other via VANET rather than indirectly via IP-RSUs [_ -> directly].
TCP [and and -> and] SCTP
=> The first sentence is corrected with “to communicate with each other directly via VANET rather than indirectly via IP-RSUs”. The second one is corrected with one “and”.

Page #21
between to end points requires [an -> _] efficient mobility management
Most [of -> _] vehicles [are equipped with -> equip] a GPS receiver
the assistance [from -> of] the IP-RSUs or a cellular system
With a GPS navigator, [an -> _] efficient mobility management
for [the -> _] efficient mobility management
=> “efficient mobility management” is used. “Most vehicles” is used. “are equipped with” is correct. “the assistance of the IP-RSUs” is used. “for efficient mobility management” is used.

Page #22
The security and privacy [is one of -> are part of] key components
=> “Security and privacy are key components” is used according to another reviewer’s comment.

Maybe:
Only authorized vehicles to need to be allowed to use the vehicular [networking -> networkings]
=> “networking” is uncountable, so “the vehicular networking” is used.

[For -> In] this case
the aftermath of [the -> _] malicious behaviors
=> “In this case” is used. “the aftermath of malicious behaviors” is used.
For example, [_ -> a] Sybil attack, which tries to confuse a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver.
This [sybil -> Sybil] attack
=> “a Sybil attack” is used. The second one does not exist by the revision according to another reviewer.

Page #23
to such a [sybil -> Sybil] attack,
a user certificate along with [_ -> an] in-vehicle device's identifier generation

Transport Layer Security (TLS) certificates can be used for [the -> _] vehicle authentication
=> "a Sybil attack" is used. The second sentence does not exist by the revision according to another reviewer. "vehicle authentication" is used.

Page #24
For [the -> _] mobility management
in [the -> _] mobility management
=> Both are revised according to the comments.

Page #29
The definition of Mobility Anchor (MA) is clarified with [a -> _] reference to PMIPv6.
with [the -> _] reference to
=> "the reference" is used since "the" seems to be required.

Reviewer 8. Peter E. Yee (Akayla)

Page #18
"For IPv6-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular networks, the delay-bounded data delivery is critical. <u>Implementations for such applications are not available yet.</u> IPv6 ND needs to work to support IPv6-based safety applications efficiently."

Perhaps you could say why here? Is this because of some failing in IPv6 or in the lower layers?
=> I deleted "Implementations for such applications are not available yet" because my lab members and I are working for context-aware navigator now. As I know, other applications are under development.

Page #23
"For secure V2I communication, a secure channel between a mobile router (i.e., <u>IP-OBU</u>) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router (i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in another vehicle needs to be established, as shown in Figure 3."

Why do you assume that it has to be a router that makes the secure connection? Given you are talking about using TLS, why couldn't it be some device within the vehicle that makes the secure connection. That way only the device that needs to consume the data passed over the secure channel gets it as opposed to an IP-OBU which is ostensibly only a communications router, not a data consumer itself.
=> For confidentiality of packets between IP-OBU (as a mobile router in a vehicle) and IP-RSU (as a fixed router) in an access network, IPsec is used. In-vehicle devices in a vehicle can make

a secure connection with other in-vehicle devices in another vehicle via IPsec or TLS. The new text is as follows.

Section 6. Security Considerations (Page 27): The 6th Paragraph

OLD	NEW
For secure V2I communication, a secure channel between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router (i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in another vehicle needs to be established, as shown in Figure 3.	For secure V2I communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 3 [RFC4301][RFC4302][RFC4303][RFC4308][RFC7296]. Also, for secure V2V communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in another vehicle needs to be established, as shown in Figure 4. For secure communication, an element in a vehicle (e.g., an in-vehicle device and a driver/passenger's mobile device) needs to establish a secure connection (e.g., TLS) with another element in another vehicle or another element in a vehicular cloud (e.g., a server). Even though IEEE 1609.2 [WAVE-1609.2] specifies security services for applications and management messages. This WAVE specification is optional, so if WAVE does not support the security of a WAVE frame, either the network layer or the transport layer need to support security services for the WAVE frames.

"To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym needs to be provided to the vehicle; that is, each vehicle periodically updates its MAC address and the corresponding IPv6 address [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without <u>strong E2E confidentiality (using either IPsec or TLS)</u>, there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses."
At what layer? If you're using TLS, the confidentiality obtained has no impact on the MAC and IPv6 addresses.

=> For E2E confidentiality, IPsec or TLS can be used. Without such E2E confidentiality for a vehicle, the updated MAC and IPv6 addresses may be disclosed to an adversary, so the adversary can track the vehicle as follows.

Section 6. Security Considerations (Page 28): The 8th Paragraph

OLD	NEW
To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym needs to be provided to the vehicle; that is, each vehicle periodically updates its MAC address and the corresponding IPv6 address [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses.	To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, especially for a long-living transport-layer session (e.g., voice call over IP and video streaming service), a MAC address pseudonym needs to be provided to each vehicle; that is, each vehicle periodically updates its MAC address and its IPv6 address needs to be updated accordingly by the MAC address change [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality (using either IPsec or TLS), there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses. Thus, the MAC address pseudonym and the IPv6 address update should be performed with strong E2E confidentiality.

Thanks for your valuable comments and help.

Best Regards,
Paul
--
===========================
Jaehoon (Paul) Jeong
Associate Professor
Department of Software

Sungkyunkwan University
Office: +82-31-299-4957
Email: jaehoon.paul@gmail.com, pauljeong@skku.edu
Personal Homepage: http://iotlab.skku.edu/people-jaehoon-jeong.php