Revision Letter

Editor: Jaehoon (Paul) Jeong
Date: May 19, 2022

OLD: draft-ietf-ipwave-vehicular-networking-28
NEW: draft-ietf-ipwave-vehicular-networking-29

Hi Éric, Lars, Roman, Alvaro, Murray, Paul, Zaheduzzaman, and Robert,

I sincerely appreciate your keen and productive comments to improve our draft. I have addressed your comments below, which use a bold font. My answers in a regular font start with a prefix "=> [PAUL]".

This is the table of contents for this revision letter for the reviewers.

[Review by Éric Vyncke and Response by Authors]

--
DISCUSS:
--

Thank you for the work put into this document. I found the use cases part of section 3.1 very interesting to read even if some of them seem very far fetched
;-)

Please find below some blocking DISCUSS points (easy to address though), some

non-blocking COMMENT points (but replies would be appreciated even if only for my own education), and some nits.

Special thanks to

- Carlos Bernardos for the shepherd's write-up even if a justification for the informational status would have been welcome but the WG consensus description is appreciated.

- Pascal Thubert for his IETF last call INT directorate review at:
https://datatracker.ietf.org/doc/review-ietf-ipwave-vehicular-networking-20-intdir-lc-thubert-2021-06-18/
and for his IESG telechat INT directorate review
https://datatracker.ietf.org/doc/review-ietf-ipwave-vehicular-networking-27-intdir-telechat-thubert-2022-02-28/
Pascal's Last Call & telechat reviews were (at least partially) acted upon by Paul ;-)

I hope that this helps to improve the document,

Regards,

-éric

# DISCUSS

As noted in https://www.ietf.org/blog/handling-iesg-ballot-positions/, a DISCUSS ballot is a request to have a discussion on the following topics:

## Abstract & Section 1

"then enumerates requirements for the extensions of those IPv6 protocols" does not match any IPWAVE WG work item, i.e., it is outside the scope of the charter of IPWAVE WG. As the document does not explicitly specify requirements, I strongly suggest to use the word "gaps" rather than "requirements" in the abstract and section 1.
=> [PAUL] We replaced “requirements” with “gaps” in abstract.
Abstract

OLD	NEW
First, this document explains use cases using V2V, V2I, and V2X networking. Next, for IPv6-based	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 enumerates requirements for the extensions of those IPv6 protocols for IPv6-based vehicular networking.	vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then enumerates gaps for the extensions of those IPv6 protocols for IPv6-based vehicular networking.

## Section 4.1

Using an IPv6 address out of a ULA prefix still requires DAD. So the text below should be updated to be corrected:

"their own IPv6 Unique Local Addresses
(ULAs) [RFC4193] over the wireless network, which does not require
the messaging (e.g., Duplicate Address Detection (DAD)) of IPv6
Stateless Address Autoconfiguration (SLAAC) [RFC4862]."

=> [PAUL] We removed the later part of this sentence.

5th paragraph, Section 4.1

OLD	NEW
Alternatively, mobile nodes can employ a "Bring-Your-Own-Addresses (BYOA)" (or "Bring-Your-Own-Prefix (BYOP)") technique using their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network~~, which does not require the messaging (e.g., Duplicate Address Detection (DAD)) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]~~.	Alternatively, mobile nodes can employ a "Bring-Your-Own-Addresses (BYOA)" (or "Bring-Your-Own-Prefix (BYOP)") technique using their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network.

## Section 4.2

Very similar comment as above (i.e., DAD & MLD must be done for all IPv6 addresses of an interface and not only for the global one):

"... When global IPv6
addresses are used, wireless interface configuration and control
overhead for DAD"

=> [PAUL] We deleted “global” to lift the scope limit for all IPv6 addresses of an interface.

7th paragraph, Section 4.2

OLD	NEW
As shown in Figure 2, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be link-local IPv6 addresses, ULAs, or global IPv6 addresses. When ~~global~~ IPv6 addresses are used, wireless interface configuration and control overhead for DAD [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways.	As shown in Figure 2, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be link-local IPv6 addresses, ULAs, or global IPv6 addresses. When IPv6 addresses are used, wireless interface configuration and control overhead for DAD [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways.

## Section 5.2

"... If DHCPv6 is used to assign
a unique IPv6 address to each vehicle in this shared link, DAD is not
required. "

This is incorrect and must be changed (see section 18.2.10.1. of RFC 8415)

=> [PAUL] We deleted the sentence about the non-obligation of the DAD in DHCPv6 for clarity.

5th paragraph, Section 5.2

OLD	NEW
For a mobility management scheme in a domain, 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, DAD is not required.~~ On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213]), 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	For a mobility management scheme in a domain, where the wireless subnets of multiple IP-RSUs share the same prefix, 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 [RFC5213]), 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

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.	networks needs to consider this tradeoff to support efficient mobility management.

--
COMMENT:
--

# COMMENTS

"100km/h as the speed limit in highway" will make many European drivers smile as it is really slow...
=> [PAUL] Yes, that is true. We updated the text to include more cases.

1st paragraph, Section 5

OLD	NEW
For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1km) and 100km/h as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is in the order of a minute (e.g., about 72 seconds), and the lifetime of a link between two vehicles is about a half minute.	For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1km, which is 0.6213 miles) and 100km/h (i.e., 62.1371 MPH) as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is in the order of a minute (e.g., about 72 seconds), and the lifetime of a link between two vehicles is about a half minute. Note that some countries (e.g., Germany) can have a much higher speed limit or even no limit.

## Section 1

"Most countries and regions in the world have adopted the same frequency allocation for vehicular networks." but there are TWO frequency allocations described just before, so, which one has been adopted ?

=> [PAUL] For the same frequency allocation, we mean the 5.9 GHz band for ITS purposes. Though different countries divide the band into different channels, they all use this band for vehicular networks. In addition, there have been updates for the ITS band in the US recently. We added the new information in this paragraph. We modified the paragraph as follows:

1st paragraph, Section 1

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]. Most countries and regions in the world have adopted the same frequency allocation for vehicular networks.	Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks. Since 2003, the Federal Communications Commission (FCC) in the US had 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). In November 2020, the FCC adjusted the lower 45 MHz (i.e., 5.850 - 5.895 GHz) of the 5.9 GHz band for unlicensed use instead of ITS-dedicated use [FCC-DSRC-Modification]. 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]. Most countries and regions in the world have adopted the 5.9 GHz band for vehicular networks, though different countries use different ways to divide the band into channels.

## Section 2

"GPS" is just the USA commercial example of the more generic "global navigation satellite system" (GNSS), GNSS should be used in this document.
=> [PAUL] We updated the description for the term as follows.

6st entry, Section 2

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

6th entry, Section 2

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

1st paragraph, Section 5.2

OLD	NEW
The seamless connectivity and timely data exchange between two end points requires efficient mobility management including location management and handover. Most vehicles are equipped with a GPS	The seamless connectivity and timely data exchange between two end points requires efficient mobility management including location management and handover. Most vehicles are equipped with a GNSS

receiver as part of a dedicated navigation system or a corresponding smartphone App. Note that the GPS receiver may not provide vehicles with accurate location information in adverse environments such as a building area or a tunnel. The location precision can be improved with assistance of the IP-RSUs or a cellular system with a GPS receiver for location information.	receiver as part of a dedicated navigation system or a corresponding smartphone App. Note that the GNSS receiver may not provide vehicles with accurate location information in adverse environments such as a building area or a tunnel. The location precision can be improved with assistance of the IP-RSUs or a cellular system with a GNSS receiver for location information.

2nd paragraph, Section 5.2

OLD	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).	With a GNSS 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).

As IP-RSU have at least 2 interfaces, should "Also, it may have *the* third IP-enabled wireless interface" be replaced by "Also, it may have *a* third IP-enabled wireless interface" ?

=> [PAUL] We updated the text.

2nd paragraph, Section 5.2

OLD	NEW
Also, it may have the third IP-enabled wireless interface running in 3GPP C-V2X in addition to the IP-RSU defined in [RFC8691].	Also, it may have a third IP-enabled wireless interface running in 3GPP C-V2X in addition to the IP-RSU defined in [RFC8691].

LiDAR ... "by measuring the reflected pulsed light" but on which kind of metrics ?

=> [PAUL] We modified the description to make it more clear.

Section 2

OLD	NEW

LiDAR: "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.	LiDAR: "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the round-trip time of the emitted pulsed light.

## Section 3.1

Should the 1st and 5th bullets be grouped together ?
=> [PAUL] Since the 1st bullet is for terrestrial vehicles, and the 5th bullet is for aerial vehicles, these two bullets are not grouped together. I reordered the bullets and the corresponding contents such that the title and contents of the 5th bullet is placed as the 2nd bullet for the logical grouping of these two bullets.

Section 3.1

OLD	NEW
● Context-aware navigation for safe driving and collision avoidance; ● Cooperative adaptive cruise control in a roadway; ● Platooning in a highway; ● Cooperative environment sensing. ● Collision avoidance service of end systems of Urban Air Mobility (UAM).	● Context-aware navigation for safe driving and collision avoidance; ● Collision avoidance service of end systems of Urban Air Mobility (UAM); ● Cooperative adaptive cruise control in a roadway; ● Platooning in a highway; ● Cooperative environment sensing.

Please describe "UAM" (e.g., in the terminology section) as it is unclear to the reader whether it is a crewed / uncrewed aircraft.
=> [PAUL] UAM can be manned or unmanned aircraft. We updated the text to clarify this point by adding a new term in Section 2.

Section 2

OLD	NEW
	Urban Air Mobility (UAM): It refers to using a lower-altitude aircraft to transport passengers or cargo in

	urban and suburban areas. The carriers that are used for UAM can be either manned or unmanned vehicles, which can include traditional helicopters, electrical vertical-takeoff-and-landing aircraft (eVTOL), and unmanned aerial vehicles (UAV).

If both road and air vehicles are use case, what about river / sea ships or trains ?
=> [PAUL] They are also included in the use cases. We updated the text to include these cases.

2nd paragraph, Section 3.1

OLD	NEW
These five techniques will be important elements for autonomous vehicles, which may be either terrestrial vehicles or UAM end systems.	The above use cases are examples for using V2V networking, which can be extended to other terrestrial vehicles, river/sea ships, railed vehicles, or UAM end systems.

Does the paragraph about "reward system" belong to the use case ? It rather sounds like a business requirement. Suggest to remove this part.
=> [PAUL] We have removed it from Section 3.1.

Like written by Pascal Thubert in his telechat review, the last paragraph "IPv6-based packet exchange and secure" should be clear that this is not only about data plane traffic but also control plane L2/L3 ones. Please also use the Oxford comma, i.e., add a "," after "exchange".
=> [PAUL] We included control and data planes in this text. We also added a comma after “exchange”.

last paragraph, Section 3.1

OLD	NEW
To support applications of these V2V use cases, the required functions of IPv6 include IPv6-based packet exchange and secure, safe communication between two vehicles. For the support of V2V under	To support applications of these V2V use cases, the required functions of IPv6 include IPv6-based packet exchange in both control and data planes, and secure, safe communication between two vehicles.

multiple radio technologies (e.g., DSRC and 5G V2X), refer to Appendix A.	For the support of V2V under multiple radio technologies (e.g., DSRC and 5G V2X), refer to Appendix A.

## Section 3.2

Suggest to also mention "5G" after "IP-RSU or 4G-LTE networks"

=> [PAUL] We added “5G” term.

4th paragraph, Section 3.2

OLD	NEW
The emergency communication between accident vehicles (or emergency vehicles) and a TCC can be performed via either IP-RSU or 4G-LTE networks.	The emergency communication between accident vehicles (or emergency vehicles) and a TCC can be performed via either IP-RSU, 4G-LTE or 5G networks.

How is the UAM use case different from a driverless terrestrial EV ? Suggest to merge those use cases.

=> [PAUL] We merge the two use cases with the phrases of a UAM navigation service as follows.

4th-5th paragraph, Section 3.2

OLD	NEW
An EV charging service with V2I can facilitate 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 or be notified that the charging station is out of service 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.	An EV charging service with V2I can facilitate 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 or be notified that the charging station is out of service 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. For a UAM navigation service, an efficient

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

## Section 4.1

As noted by other ADs, "Existing network architectures," the list should not include OMNI yet as it is not deployed and would probably not be described as an architecture.
=> [PAUL] Though AERO/OMNI is not actually deployed in the industry, this AERO/OMNI is mentioned as a possible approach for vehicular networks in this document.

2nd paragraph, Section 4.1

OLD	NEW
	Note that though AERO/OMNI is not actually deployed in the industry, this AERO/OMNI is mentioned as a possible approach for vehicular networks in this document.

"the wireless media interfaces are autoconfigured with a global IPv6 prefix", is it the same shared prefix or multiple prefixes ?
=> [PAUL] Actually, it can be either the same shared prefix or multiple prefixes. Since this information is described in the next paragraph, we modified the text and merged the two paragraphs as follows.

3th paragraph, Section 4.1

OLD	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.~~ 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).	As shown in Figure 1, IP-RSUs as routers and vehicles with IP-OBU have wireless media interfaces for VANET. The 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).

Is "RSU" the same concept as "IP-RSU" ?
=> [PAUL] Yes, it is. We updated the term. We also checked other places to replace “RSU” with “IP-RSU”.

4th paragraph, Section 4.1

OLD	NEW
Multiple vehicles under the coverage of an RSU share a prefix just as mobile nodes share a prefix of a	Multiple vehicles under the coverage of an IP-RSU share a prefix just as mobile nodes share a prefix of a

Wi-Fi access point in a wireless LAN.	Wi-Fi access point in a wireless LAN.

The last paragraph is about TCP session continuity, but does not explain why multi-path TCP or QUIC session resumption cannot be used.
=> [PAUL] MPTCP or QUIC session resumption can also be used to improve session continuity. We updated the text to include the cases.

7th paragraph, Section 4.1

OLD	NEW
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 correspondent 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], NEMO [RFC3963][RFC4885] [RFC4888], and AERO [I-D.templin-6man-aero]). This document describes issues in mobility management for vehicular networks in Section 5.2.	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 correspondent 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], NEMO [RFC3963][RFC4885] [RFC4888], and AERO [I-D.templin-6man-aero]). This document describes issues in mobility management for vehicular networks in Section 5.2. For improving TCP session continuity or successful UDP packet delivery, the Multipath TCP (MPTCP) [RFC8684] or QUIC protocol [RFC9000] can also be used. IP-OBUs, however, may still experience more session time-out and re-establishment procedures due to lossy connections among vehicles caused by the high mobility dynamics

	of them.

## Section 4.2

The computation about "dwell time" is interesting even if it is computed in the best case. But, I really wonder whether using IPv6 and routing are applicable to the use case as opposed to more layer-2 + tunnel solutions (like 3GPP) with such short time for hand-over. I am a strong supporter of layer-3 (IPv6 and routing), but I cannot refrain from thinking that IPv6 is the wrong technical solution for those use cases... Was this discussed in the WG ?
=> [PAUL] Since this document is about the gap analysis and problem statement, we do not assert which solution is better than others in the studied network architectures. Generally both solutions can work for the current scenario, so the problem is whether they are good enough to meet the minimum performance requirements or not.

## Section 5.1

What is "legacy DAD" ?
=> [PAUL] It means the current DAD procedure used in the IPv6 standard. We rephrase the term to remove ambiguity.

5th paragraph, Section 5.1

OLD	NEW
To efficiently prevent IPv6 address duplication due to the VANET partitioning and merging from happening in vehicular networks, the vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD.	To efficiently prevent IPv6 address duplication due to the VANET partitioning and merging from happening in vehicular networks, the vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the current DAD.

"...the NA interval needs to be
dynamically adjusted according to a vehicle's speed so that the
vehicle can maintain its neighboring vehicles in a stable way"

With the issues linked to multicast over wireless, are the authors and the WG sure that increasing the amount of multicast will not aggravate the problem ? See RFC 9119 (cited as a normative down reference)

=> [PAUL] We noticed this issue in our WG discussion. We can use some multicast optimization techniques to mitigate the issue as described in RFC 9119. We updated the text to reflect this issue.

7th paragraph, Section 5.1

OLD	NEW
ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles. The ND time-related parameters can be an operational setting or an optimization point particularly for vehicular networks.	ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles. The ND time-related parameters can be an operational setting or an optimization point particularly for vehicular networks. Note that the link-scope multicast messages in ND protocol may cause the performance issue in vehicular networks. [RFC 9119] suggests several optimization approaches for the issue.

## Section 5.1.2

Please add some references to the MADINAS WG current work items. The authors may also consider adding this use case to the MADINAS use case.

"The pseudonym of a MAC address affects an IPv6 address based on the MAC address", nearly no implementations use EUI-64 anymore so this part should probably be removed from the document. But, the change of MAC address probably has other impact on the IP stack, e.g., the neighbour cache.

=> [PAUL] We cited the WG documents from MADINAS in the text. We will try to suggest MADINAS WG to add the use case in the current draft into its WG document.

We removed the sentence to reflect the suggestion.

1st paragraph, Section 5.1.2

OLD	NEW
For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used, so that the MAC address can be changed periodically. However, although such a pseudonym of a MAC address can protect to some extent the privacy of a vehicle, it may not be able to resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. ~~The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP and SCTP) session with an IPv6 address pair.~~ However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.	For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used, so that the MAC address can be changed periodically. However, although such a pseudonym of a MAC address can protect to some extent the privacy of a vehicle, it may not be able to resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking. Note that [I-D.ietf-madinas-mac-address-randomization] discusses more about MAC address randomization, and [I-D.ietf-madinas-use-cases] describes several use cases for MAC address randomization.

## Section 5.1.3

AFAIK, RPL relies on messages to discover the topology and I am afraid that in such a moving / dynamic environment, there will be too many of RPL messages.
Will RPL scale in this ever changing network ? Please note that I am not a RPL expert.
=> [PAUL] The mentioned issue may happen in IPv6-based vehicular networks when RPL is used. This can be an operational or optimization point for a practitioner. We updated the text to reflect the concern and modified some terms for consistency.

5th paragraph, Section 5.1.3

OLD	NEW
RPL can be used in IPv6-based vehicular networks, but it is	RPL can be used in IPv6-based vehicular networks, but it is

primarily designed for lossy networks, which puts energy efficiency first. For using it in IPv6-based vehicular networks, there have not been actual experiences and practical implementations~~ for vehicular networks~~, though it was tested in IoT low-power and lossy networks (LLN) scenarios.	primarily designed for low-power networks, which puts energy efficiency first. For using it in IPv6-based vehicular networks, there have not been actual experiences and practical implementations, though it was tested in IoT low-power and lossy networks (LLN) scenarios. Another concern is that RPL may generate excessive topology discovery messages in a highly moving environment such as vehicular networks. This issue can be an operational or optimization point for a practitioner.

## Section 6.1

Some explanations on how SEND protects against DAD flooding would be welcome.
=> [PAUL] SEND can protect against DAD flooding by using a cryptographically generated address (CGA) to verify the true owner of a received ND message, along with the filtering of DAD messages from an invalid owner with an invalid CGA.

1st paragraph, Section 6.1

OLD	NEW
Based on the SEND [RFC3971], the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires using the CGA ND option in the ND protocols.	Based on the SEND [RFC3971], the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, cryptographically generated addresses (CGA) can be used to verify the true owner of a received ND message, which requires using the CGA ND option in the ND protocols. This CGA can protect vehicles against DAD flooding by DAD filtering based on the verification for the true owner of the received DAD message.

Is "classical IPv6 ND" the same as the previously used "legacy ND" ?

=> [PAUL] Yes, they have the same meaning with different names. We modified the text to clarify the term used here.

1st paragraph, Section 6.1

OLD	NEW
For the classical IPv6 ND, DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface.	For the classical IPv6 ND (i.e., the legacy ND), DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. ......

Wondering why "Vehicle Identification Number (VIN)" is suggested to be used as SubjectAltName in a certificate rather than a car manufacturer cert ?
=> [PAUL] A car manufacturer certificate can also be used. We updated the sentences to reflect this point.

4th paragraph, Section 6.1

OLD	NEW
To identify malicious vehicles among vehicles, an authentication method may be 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.	To identify malicious vehicles among vehicles, an authentication method may be required. A Vehicle Identification Number (VIN) (or a vehicle manufacturer certificate) 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. ......

## Section 6.3

The part about bitcoin and blockchain errs probably too far away from the IETF remit.
=> [PAUL] In some sense, we agree on this point. But this draft is to discuss existing gaps and issues for IPv6-based vehicular networks. For a non-repudiation of a harmful activity from a vehicle, the blockchain

technology is a way to deal with it, though it may need further development particularly for IPv6-based vehicular networks. We would like to keep the blockchain stuff and rephrase the sentences as follows.

3rd paragraph, Section 6.3

OLD	NEW
For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.	For the non-repudiation of the harmful activities from malicious vehicles, which it is difficult for other normal vehicles to identify, an additional and advanced approach is needed. One possible approach is to use a blockchain-based approach [Bitcoin] as an IPv6 security checking framework. Each IPv6 packet from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.

## Appendix B

I fail to understand how RPL and OMNI can be compared as they are vastly different technologies (routing vs. tunneling).
=> [PAUL] Yes, they are about routing and tunneling, respectively.
Since the topic discussed here is about multihop V2X networking, the use of both OMNI and AERO together enables multiple vehicles to forward IPv6 packets via the newly defined virtual interfaces from OMNI. That is why we put them together for multihop V2X networking. We modified the text to reflect this issue as follows:

1st paragraph, Appendix D

OLD	NEW
The multihop V2X networking can be	The multihop V2X networking can be

supported by RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] and Overlay Multilink Network Interface (OMNI) [I-D.templin-6man-omni].	supported by RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] and Overlay Multilink Network Interface (OMNI) [I-D.templin-6man-omni] with AERO [I-D.templin-6man-aero].

"In OMNI protocol, each wireless media interface is configured with an IPv6 Unique Local Address (ULA)" but from my last read of OMNI drafts (1+ year ago), the OMNI virtual interface can have a ULA indeed but the wireless physical ones are using any prefix.
=> [PAUL] The original here was suggested by the author of OMNI (i.e., Fred Templin), but it is modified according to the above comment as follows.

6th paragraph, Appendix B

OLD	NEW
In OMNI protocol, each wireless media interface is configured with an IPv6 Unique Local Address (ULA).	In OMNI protocol, an OMNI virtual interface can have a ULA [RFC4193] indeed, but wireless physical interfaces associated with the OMNI virtual interface are using any prefix.

## Appendix D

What will be the impact of high packet loss rate (that I am expecting on such networks) on IP parcels ?
=> [PAUL] The possible impact of high packet loss rate on IP parcels in vehicular networks can be that multiple TCP sessions need simultaneously either packet retransmissions or reestablishment of the sessions. We revised the text to discuss this issue as follows.

last paragraph, Appendix D

OLD	NEW
Performance studies over the course of many decades have proven that applications will see greater performance by sending smaller numbers of large packets (as opposed to larger numbers of small packets) even if fragmentation is needed. The OAL further supports even larger	Performance studies over the course of many decades have proven that applications will see greater performance by sending smaller numbers of large packets (as opposed to larger numbers of small packets) even if fragmentation is needed. The OAL further supports even larger

packet sizes through the IP Parcels construct [I-D.templin-intarea-parcels] which provides "packets-in-packet" encapsulation for a total size up to 4MB. Together, the OAL and IP Parcels will provide a revolutionary new capability for greater efficiency in both mobile and fixed networks.	packet sizes through the IP Parcels construct [I-D.templin-intarea-parcels] which provides "packets-in-packet" encapsulation for a total size up to 4MB. Together, the OAL and IP Parcels will provide a revolutionary new capability for greater efficiency in both mobile and fixed networks. On the other hand, due to the high dynamics of vehicular networks, a high packet loss may not be able to be avoided. The high packet loss on IP Parcels can simultaneously cause multiple TCP sessions to experience packet re-transmissions, session time-out, or re-establishment of the sessions. Other protocols such as MPTCP and QUIC may also experience the similar issue. A mechanism for mitigating this issue in OAL and IP Parcels should be considered.

# NITS

Please check that all IPv6 addresses are in lowercase (e.g., in section 4.1).
=> [PAUL] We have updated all IPv6 addresses with lowercase in the draft.

[Review by Lars Eggert and Response by Authors]

--
COMMENT:
--

Section 1. , paragraph 5, comment:

> **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], Network**
> **Mobility (NEMO) [RFC3963], Locator/ID Separation Protocol (LISP)**
> **[I-D.ietf-lisp-rfc6830bis], and Automatic Extended Route Optimization**

> based on the Overlay Multilink Network Interface (AERO/OMNI)
> [I-D.templin-6man-aero] [I-D.templin-6man-omni]). 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].

Isn't it a bit premature to list AERO and OMNI alongside a number of published standards from the IETF and other organizations? As far as I know they are individual documents that have not been adopted? (Here and elsewhere in the document.)

=> [PAUL] We agree on this point. We removed AERO and OMNI in the section.

1st paragraph, Section 1

OLD	NEW
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], Network Mobility (NEMO) [RFC3963], Locator/ID Separation Protocol (LISP) [I-D.ietf-lisp-rfc6830bis], ~~and Automatic Extended Route Optimization based on the Overlay Multilink Network Interface (AERO/OMNI) [I-D.templin-6man-aero] [I-D.templin-6man-omni])~~.	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], Network Mobility (NEMO) [RFC3963], and Locator/ID Separation Protocol (LISP) [I-D.ietf-lisp-rfc6830bis].

Found terminology that should be reviewed for inclusivity; see https://www.rfc-editor.org/part2/#inclusive_language for background and more guidance:

* **Term "invalid"; alternatives might be "not valid", "unenforceable", "not binding", "inoperative", "illegitimate", "incorrect", "improper", "unacceptable", "inapplicable", "revoked", "rescinded".**

=> [PAUL] We replaced one “invalid” by “not valid”.

NIT

--

All comments below are about very minor potential issues that you may choose to address in some way - or ignore - as you see fit. Some were flagged by automated tools (via https://github.com/larseggert/ietf-reviewtool), so there will likely be some false positives. There is no need to let me know what you did with these suggestions.

Section 5.2. , paragraph 7, nit:

```
-    home.  There is nonnegligible control overhead to set up and maintain
+    home.  There is non-negligible control overhead to set up and maintain
+                       +
```

=> [PAUL] We updated the word.

Section 1. , paragraph 3, nit:

```
> 9.4 [WAVE-1609.4] specifies the multi-channel operation. IEEE 802.11p was
fi
>                                 ^^^^^^^^^^^^^
```

This word is normally spelled as one.

=> [PAUL] We updated the word.

Section 4.1. , paragraph 7, nit:

```
> arty. To minimize this kind of risk, an reinforced identification and
verific
>                                      ^^
```

**Use "a" instead of "an" if the following word doesn't start with a vowel sound,
e.g. "a sentence", "a university".**

=> [PAUL] We corrected the word.

Section 4.3. , paragraph 17, nit:

```
> livered to relevant vehicles in an efficient way (e.g., multicasting). With
>                              ^^^^^^^^^^^^^^^^^^^
```

Consider replacing this phrase with the adverb "efficiently" to avoid wordiness.

=> [PAUL] We rephrased the sentence by using “efficiently”.

Section 4.3. , paragraph 17, nit:

```
> layers (e.g., IPv6, TCP, and UDP). Hence the bandwidth selection according
t
>                                    ^^^^^
```

A comma may be missing after the conjunctive/linking adverb "Hence".

=> [PAUL] We added a comma here.

```
Section 5.1.1. , paragraph 4, nit:
> y with standard IPv6 links in an efficient fashion to support IPv6 DAD, MLD
a
>                            ^^^^^^^^^^^^^^^^^^^^^^^
Consider replacing this phrase with the adverb "efficiently" to avoid
wordiness.
=> [PAUL] We rephrased the sentence by using “efficiently”.

Section 5.1.2. , paragraph 2, nit:
> ergy constraints, RPL does not suggest to use a proactive mechanism (e.g.,
k
>                                ^^^^^^^^^^^^^^
The verb "suggest" is used with the gerund form.
=> [PAUL] We corrected the form by “suggest using”.

Section 5.2. , paragraph 4, nit:
> lic Key Infrastructure (PKI) in an efficient way. To provide safe
interactio
>                              ^^^^^^^^^^^^^^^^^^^
Consider replacing this phrase with the adverb "efficiently" to avoid
wordiness.
=> [PAUL] We rephrased the sentence by using “efficiently”.

Section 5.2. , paragraph 5, nit:
> other servers behind an IP-RSU in a secure way. Even though a vehicle is
per
>                                ^^^^^^^^^^^^^^^
Consider replacing this phrase with the adverb "securely" to avoid wordiness.
=> [PAUL] We rephrased the sentence by using “securely”.


Section 5.2. , paragraph 8, nit:
> eceived ND message, which requires to use the CGA ND option in the ND
protoc
>                                    ^^^^^^
Did you mean "using"? Or maybe you should add a pronoun? In active voice,
"require" + "to" takes an object, usually a pronoun.
=> [PAUL] We corrected the sentence by using “requires using”

Section 6. , paragraph 3, nit:
>  taking a safe maneuver. Since cyber security issues in vehicular networks
ma
>                                ^^^^^^^^^^^^^^
```

The word "cybersecurity" is spelled as one.
=> [PAUL] We updated the word by combining them.

Section 6.1. , paragraph 4, nit:

```
> ensus algorithm needs to be developed or an existing consensus algorithm
need
>                                      ^^^
```

Use a comma before "or" if it connects two independent clauses (unless they are closely connected and short).
=> [PAUL] We added a comma before “or”.

Section 8.2. , paragraph 7, nit:

```
>  Device-free human counting through WiFi fine-grained subcarrier
information
>                                     ^^^^
```

Did you mean "Wi-Fi"? (This is the officially approved term by the Wi-Fi Alliance.).
=> [PAUL] Yes, we updated WiFi with “Wi-Fi” in the document except “Device-free human counting through WiFi fine-grained subcarrier information” because this is the title of a published paper, so I cannot change WiFi into Wi-Fi.

Section 8.2. , paragraph 23, nit:

```
> unction (called OF), which allows to adapt the activity of the routing
proto
>                                   ^^^^^^^^
```

Did you mean "adapting"? Or maybe you should add a pronoun? In active voice, "allow" + "to" takes an object, usually a pronoun.
=> [PAUL] We replaced “to adapt” with “adapting”.

"Appendix B. ", paragraph 5, nit:

```
> ST, CEA Saclay, Gif-sur-Yvette, Ile-de-France 91190, France, Phone:
+33169089
>                                 ^^^^^^^^^^^^^
```

"Ile-de-France" is an imported foreign expression, which originally has a diacritic. Consider using "Île-de-France".
=> [PAUL] We replaced the expression with “Île-de-France”. For using the expression, we replaced the encoding method “US-ASCII” with “UTF-8” at the beginning of the document.

Uncited references: [RFC3849].
=> [PAUL] We removed the reference RFC3894.

[Review by Roman Danyliw and Response by Authors]

DISCUSS:

I had difficulty in understanding the bounds for the scope of the use cases and proposed architecture. At times I had trouble understanding what was an example of related work, and what was narrative formally describing the gaps in IPv6 for vehicular networking. In that spirit:

**** The Privacy Considerations are under-specified:**

-- Section 6.3 suggests the needs for logging, “To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded 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. To solve the issue ultimately, we need a solution where, without privacy breakage, …”.

Some discussion on the “privacy breakage” is needed.
What exactly would be the trade offs between a centralized vs. distributed log?
=> [PAUL] The trade-offs between a centralized and a distributed log approach for monitoring suspicious behaviors of vehicles can be that using a centralized log system may cause a higher delay when accessing the log information as a distributed log system is closer to a scene. A distributed log system may also provide more local information for an operator to analyze the activities of vehicles instead of retrieving log information from a centralized log system.

Who would get to see this information?
=> [PAUL] If a distributed log approach is used, a vehicle’s neighboring vehicles and any authorized remote entity (e.g., a vehicle manufacturer and a security service provider for vehicular networks) can access the information. If a centralized log approach is used, any authorized entity can access the information, and a vehicle that senses suspicious behavior can also request the information of the suspicious vehicle with a proper encryption.

What is sensitive about this information?
=> [PAUL] This information is sensitive in the sense that it includes the network activities of vehicles such as the count of TCP sessions established.

We augmented the paragraph to include these discussions.

2nd paragraph, Section 6.3

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. To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded 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. To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.	Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles. To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded 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. The trade-offs between central and distributed ways can be that using a centralized approach may cause a higher delay when accessing the log information as a distributed approach is closer to a scene. A distributed approach may also provide more local information for an operator to analyze the activities of vehicles instead of retrieving log information from a centralized logging system. The logged information can be accessed by a suspicious vehicle’s neighboring vehicles and any authorized remote entity (e.g., a vehicle manufacturer and a security service provider for vehicular networks). The information of communication activities for vehicles is sensitive since it discloses the network behavior and status of a vehicle such as the count of TCP sessions established. To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle

	shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.

-- Section 5.1.2 and 6.3 highlights the use of MAC address pseudonyms. This is helpful. More discussion is needed about the associate privacy threat being mitigated.

Section 6.3 mentions an "adversary from tracking a vehicle" which I think means a passive observer of the path. However, there are other entities in which ecosystem – what is the privacy exposure to the TCC, V2I, etc? The opening in Section 6 notes that "vehicles and infrastructure must be authenticated" and those credentials (perhaps bound to even MAC pseudonyms) would also facilitate tracking even given MAC pseudonyms. Section 6.1 explicit comments on using VINs in certificates. Who are the assumed trusted actors?
=> [PAUL] The privacy exposure to the TCC and V2I is mostly about the location information of vehicles, and may also include other in-vehicle activities such as transactions of credit cards.

The assumed trusted actors are the owner of a vehicle, an authorized vehicle service provider (e.g., navigation service provider), and an authorized vehicle manufacturer for providing after-sales services.

6th paragraph, Section 6.3

OLD	NEW
Privacy concerns for excessively collecting vehicle activities from roadway operators such as public transportation administrators and private contractors may also pose threats on violating privacy rights of vehicles. It might be interesting	The privacy exposure to the TCC and via V2I is mostly about the location information of vehicles, and may also include other in-vehicle activities such as transactions of credit cards. The assumed trusted actors are the owner of a vehicle,

to find a solution from a technology point of view along with public policy development for the issue.	an authorized vehicle service provider (e.g., navigation service provider), and an authorized vehicle manufacturer for providing after-sales services. In addition, privacy concerns for excessively collecting vehicle activities from roadway operators such as public transportation administrators and private contractors may also pose threats on violating privacy rights of vehicles. It might be interesting to find a solution from a technology point of view along with public policy development for the issue.

-- Section 3.3 notes a V2P use case where the pedestrian's smart-phone is sharing unspecified information. Does that include location information? Who gets it? What kind of identifiers are shared?

=> [PAUL] It includes location information of a vulnerable road user (VRU)'s smartphone. The location information is multicasted only to the nearby vehicles. The true identifiers of the VRU's smartphone shall be protected, and only the type of the user (such as pedestrian, cyclist, and scooter) is disclosed to the nearby vehicles. We updated the text as follows.

1st-2nd paragraphs, Section 3.3

OLD	NEW
A pedestrian protection service, such as Safety-Aware Navigation Application (SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., Wi-Fi) with an IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU. An edge computing device behind the IP-RSU can collect the mobility information from vehicles and pedestrians, compute wireless communication scheduling for the sake of them. This scheduling can	The use case of V2X networking discussed in this section is for a vulnerable road user (VRU) (e.g., pedestrian and cyclist) protection service. Note that the application area of this use case is currently limited to a specific environment, such as construction sites, plants, and factories, since not every VRU (e.g., children) in a public area (e.g., streets) is equipped with a smart device (e.g., smartphone). A VRU protection service, such as Safety-Aware Navigation Application (SANA) [SANA], using V2I2P networking can reduce the collision

save the battery of each pedestrian's smartphone by allowing it to work in sleeping mode before the communication with vehicles, considering their mobility.	of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., Wi-Fi) with an IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU. An edge computing device behind the IP-RSU can collect the mobility information from vehicles and pedestrians, compute wireless communication scheduling for the sake of them. This scheduling can save the battery of each pedestrian's smartphone by allowing it to work in sleeping mode before the communication with vehicles, considering their mobility. The location information of a VRU from a smart device is multicasted only to the nearby vehicles. The true identifiers of a VRU’s smart-phone shall be protected, and only the type of the VRU, such as pedestrian, cyclist, and scooter, is disclosed to the nearby vehicles.

**** Section 4.2**

> **Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. To minimize this kind of risk, an reinforced identification and verification protocol shall be implemented.**

-- What are these dangers?

=> [PAUL] These dangers can include unauthorized driving control input and unauthorized driving information disclosure to an unauthorized third party. We updated the text as follows.

2nd paragraph, Section 4.2

OLD	NEW
Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. To minimize this kind of risk, a	Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. These dangers can include

reinforced identification and verification protocol shall be implemented.	unauthorized driving control input and unauthorized driving information disclosure to an unauthorized third party. To minimize this kind of risk, an augmented identification and verification protocol with extra means shall be implemented.

-- What is a 'reinforced identification'?
=> [PAUL] We replace 'reinforced identification' with 'augmented identification' since 'reinforced identification' is not a well-known term. An 'augmented identification' is to identify with extra means an entity that tries to access the internal network of a vehicle. These extra means can be certificate-based, biometric, credit-based, and one-time passcode (OTP) approaches in addition to a used approach. We updated the text as follows.

2nd paragraph, Section 4.2

OLD	NEW
To minimize this kind of risk, a reinforced identification and verification protocol shall be implemented.	To minimize this kind of risk, an augmented identification and verification protocol with extra means shall be implemented. These extra means can be certificate-based, biometric, credit-based, and one-time passcode (OTP) approaches in addition to a used approach [RFC8002].

-- Who are the parties in this verification protocol? What security properties is this verification providing?
=> [PAUL] The parties in the context can be a group of hackers, a criminal group, and a competitor for industrial espionage or sabotage.
The verification shall provide security properties such as confidentiality, integrity, authentication, authorization, and accounting.

2nd paragraph, Section 4.2

OLD	NEW
Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. These dangers can include unauthorized driving control input	Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. These dangers can include unauthorized driving control input

and unauthorized driving information disclosure to an unauthorized third party. To minimize this kind of risk, a reinforced identification and verification protocol shall be implemented. To minimize this kind of risk, a reinforced identification and verification protocol with extra means shall be implemented. These extra means can be certificate-based, biometric, credit-based, and one-time passcode (OTP) approaches in addition to a used approach.	and unauthorized driving information disclosure to an unauthorized third party. A malicious party can be a group of hackers, a criminal group, and a competitor for industrial espionage or sabotage. To minimize this kind of risk, an augmented identification and verification protocol with extra means shall be implemented. These extra means can be certificate-based, biometric, credit-based, and one-time passcode (OTP) approaches in addition to a used approach [RFC8002]. The verification shall provide security properties such as confidentiality, integrity, authentication, authorization, and accounting [RFC7427].

**** Section 6.**
Vehicles and infrastructure must be authenticated in order to participate in vehicular networking.

Authenticated with respect to whom? Vehicles to infrastructure and vice-versa? Or to someone else?
=> [PAUL] The authentication shall be done mutually, i.e., vehicles and infrastructure shall be authenticated to each other by a password, a key, and/or a fingerprint, which can prove the identity of a participant for vehicular networking.

2nd paragraph, Section 6

OLD	NEW
Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. For the authentication in vehicular networks, vehicular cloud needs to support a kind of Public Key Infrastructure (PKI) efficiently.	Vehicles and infrastructure must be authenticated to each other by a password, a key, and/or a fingerprint in order to participate in vehicular networking. For the authentication in vehicular networks, vehicular cloud needs to support a kind of Public Key Infrastructure (PKI) efficiently , as either a dedicated or a co-located component inside a TCC.

**** Section 6 makes references to “secure communication” - what is the expected key management approach and is that in scope?**

=> [PAUL] Any key management approach can be used, and particularly for IPv6-based vehicular networks a new or enhanced key management approach resilient to wireless networks is required.

2nd paragraph, Section 6

OLD	NEW
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 2 [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 3. 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).	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 2 [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 3. For secure V2I/V2V 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). Note that any key management approach can be used for the secure communication, and particularly for IPv6-based vehicular networks, a new or enhanced key management approach resilient to wireless networks is required.

**** The need for safety properties (very helpful) is asserted multiple times but not further discussed in the Security Considerations:**

-- Section 3:

> **In addition, IPv6**
> **security needs to be extended to support those V2V use cases in a safe, secure, privacy-preserving way.**

-- Section 3.1:
To support applications of these V2V use cases, the required functions of IPv6 include IPv6-based packet exchange and secure, safe communication between two vehicles.

-- Section 3.3:
To support applications of these V2X use cases, the required functions of IPv6 include IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU.

=> [PAUL] We have updated the text to include safety properties as follows.

2nd paragraph, Section 4.2

OLD	NEW
Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. These dangers can include unauthorized driving control input and unauthorized driving information disclosure to an unauthorized third party. To minimize this kind of risk, a reinforced identification and verification protocol shall be implemented. To minimize this kind of risk, a reinforced identification and verification protocol with extra means shall be implemented. These extra means can be certificate-based, biometric, credit-based, and one-time passcode (OTP) approaches in addition to a used approach.	Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. These dangers can include unauthorized driving control input and unauthorized driving information disclosure to an unauthorized third party. A malicious party can be a group of hackers, a criminal group, and a competitor for industrial espionage or sabotage. To minimize this kind of risk, an augmented identification and verification protocol with extra means shall be implemented. These extra means can be certificate-based, biometric, credit-based, and one-time passcode (OTP) approaches in addition to a used approach [RFC8002]. The verification shall provide security properties such as confidentiality, integrity, authentication, authorization, and accounting [RFC7427].

--

COMMENT:

--

Thank you to Daniel Migault for the SECDIR review.

**** Section 1. Editorial**
Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks.

This first sentence is unrelated to the reset of the paragraph which is focused on spectrum allocation.
=> [PAUL] We updated the sentence to reflect this point.

1st paragraph, Section 1

OLD	NEW
Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks.	Vehicular networking studies have mainly focused on improving road safety and efficiency, and also enabling entertainment in vehicular networks. To proliferate the use cases of vehicular networks, several governments and private organizations have committed to allocate dedicated spectrum for vehicular communications.

**** Section 1.**

Most countries and regions in the world have adopted the same frequency allocation for vehicular networks.

This statement seems incongruent with the previous two sentences which describe how the US and EU have allocated very similar but not “same” spectrum (5.850 – 5.925 vs. 5.875 vs. 5.905).
=> [PAUL] We have rephrased the sentence to clarify the issue.
1st paragraph, Section 1

OLD	NEW
Most countries and regions in the world have adopted the 5.9 GHz band for vehicular networks, though different countries use different ways to divide the band into channels.	Most other countries and regions in the world have adopted the 5.9 GHz band for vehicular networks, though different countries use different ways to divide the band into channels.

**** Section 2. Edge Computing is defined but doesn’t seem to be used in the**

rest of the document beyond in ECD. Is it needed?
=> [PAUL] Since we mostly use Edge Network (EN) throughout the document, we have removed the definition of “Edge Computing” for simplicity.

1st paragraph, Section 2

OLD	NEW
~~● Edge Computing (EC): It is the local computing near an access network (i.e., edge network) for the sake of vehicles and pedestrians.~~ ● Edge Computing Device (ECD): It is a computing device (or server) for edge computing for the sake of vehicles and pedestrians. ● Edge Network (EN): It is an access network that has an IP-RSU for wireless communication with other vehicles having an IP-OBU and wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and MA). It may have a global navigation satellite system (GNSS), such as Global Positioning System (GPS), radio receiver for its position recognition and the localization service for the sake of vehicles.	● Edge Computing Device (ECD): It is a computing device (or server) for edge computing for the sake of vehicles and pedestrians. ● Edge Network (EN): It is an access network that has an IP-RSU for wireless communication with other vehicles having an IP-OBU and wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and MA). It may have a global navigation satellite system (GNSS), such as Global Positioning System (GPS), radio receiver for its position recognition and the localization service for the sake of vehicles.

**** Section 2.**

IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle

Is this “computer” the same as an ECD defined earlier in the section?
=> [PAUL] It is different from an ECD. An ECD is an edge server co-located with or connected to an IP-RSU, which has a powerful computing capability for different kinds of computing tasks, such as image processing and classification.

The computer for an IP-OBU inside a vehicle can be a computing platform with a general computing power or driven by a low-power CPU (e.g., ARM). Generally it has much less computing capability compared to an ECD.
We updated the definitions as follows.

1st paragraph, Section 6.3

OLD	NEW
● Edge Computing Device (ECD): It is a computing device (or server) for edge computing for the sake of vehicles and pedestrians. ...... ● IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, autobike, motorcycle, and a similar one). It has at least one IP interface that runs in IEEE 802.11-OCB and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. It can play a role of a router connecting multiple computers (or in-vehicle devices) inside a vehicle. See the definition of the term "OBU" in [RFC8691].	● Edge Computing Device (ECD): It is a computing device (or server) at edge for vehicles and vulnerable road users. It co-locates with or connects to an IP-RSU, which has a powerful computing capability for different kinds of computing tasks, such as image processing and classification. ...... ● IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, autobike, motorcycle, and a similar one), which has a basic processing ability and can be driven by a low-power CPU (e.g., ARM). It has at least one IP interface that runs in IEEE 802.11-OCB and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. It can play the role of a router connecting multiple computers (or in-vehicle devices) inside a vehicle. See the definition of the term "IP-OBU" in [RFC8691].

**** Section 3.1. Editorial.**

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

systems.

This sentence seems to suggest that all give techniques are relevant to both terrestrial and UAMs. As far as I can tell, the first three (1 - 3) are terrestrial related, the fourth is relevant to both terrestrial and UAM, and the fifth is UAM only.
=> [PAUL] We updated the paragraph to remove ambiguity.

2nd paragraph, Section 3.1

OLD	NEW
These five techniques will be important elements for autonomous vehicles, which may be terrestrial vehicles, river / sea ships, railed vehicles, or UAM end systems.	The above use cases are examples for using V2V networking, which can be extended to other terrestrial vehicles, river/sea ships, railed vehicles, or UAM end systems.

**** Section 3.1**

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

I'm struggling to link this proposed solution to stated uses case or gap-analysis for IPv6. Can the IPv6 enablers be described.
=> [PAUL] The above sentences are deleted because the reward for cooperative environmental sensing is not tightly linked to IPv6 as follows.

7th paragraph, Section 3.1

OLD	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 the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain].	

** Section 3.2. Typo? s/air firmware/over-the-air firmware/. If not a typo, what is an “air firmware/software update”?

=> [PAUL] We updated the term as follows.

5th paragraph, Section 3.2

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

** Section 3.2. Editorial?

For this battery charging schedule, a UAM
end system can communicate with an infrastructure node (e.g., IP-RSU)
toward a cloud server via V2I communications.

Is there is a missing word here. What does it mean to “... communicate with an infrastructure node … toward a cloud server”

=> [PAUL] We rephrase the sentence as follows.

5th paragraph, Section 3.2

OLD	NEW
For this battery charging schedule, a UAM end system can communicate with an infrastructure node (e.g., IP-RSU) toward a cloud server via V2I communications.	For this battery charging schedule, a UAM end system can communicate with a cloud server via an infrastructure node (e.g., IP-RSU).

** Section 4.2

> **It is reasonable to consider the interaction between the internal network and an external network within another vehicle or an EN.**

Can the intent of this be clarified? Isn’t something on the internal vehicle network talking to another vehicle the definition of V2V per Section 3.1?
=> [PAUL] The intent of this is to describe that a host of a vehicle can communicate with a host of another vehicle or an EN. We modified the sentence to clarify it.
2nd paragraph, Section 4.2

OLD	NEW
It is reasonable to consider the interaction between the internal network and an external network within another vehicle or an EN.	It is reasonable to consider interactions between the internal network of a vehicle and that of another vehicle or an EN.

**** Section 4.2. Is there any expectation of any perimeter-based policy enforcement between this internal network and the edge network (e.g., firewall?).**
=> [PAUL] A perimeter-based policy enforcement can be applied between the internal network of a vehicle and the edge network. We updated the text to reflect this point.
6th paragraph, Section 4.2

OLD	NEW
Through the mutual knowledge of the network parameters of internal networks, packets can be transmitted between the vehicle's moving network and the EN's fixed network. Thus, V2I requires an efficient protocol for the mutual knowledge of network parameters.	Through the mutual knowledge of the network parameters of internal networks, packets can be transmitted between the vehicle's moving network and the EN's fixed network. Thus, V2I requires an efficient protocol for the mutual knowledge of network parameters. Note that from a security point of view, a perimeter-based policy enforcement can be applied to protect parts of the internal network of a vehicle.

**** Section 4.3. Is there implicit trust between the platooning vehicles? Security impact if one becomes untrusted?**
=> [PAUL] Yes, before the vehicles can be platooned, they shall be mutually authenticated to reduce possible security risks.
1st paragraph, Section 4.3

OLD	NEW
As a V2V use case in Section 3.1, Figure 4 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.	As a V2V use case in Section 3.1, Figure 4 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. From a security point of view, before vehicles can be platooned, they shall be mutually authenticated to reduce possible security risks.

**** Section 5.**

> **For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges.**

This is a helpful performance envelope. Can this be more tightly linked to IPv6? It seems like this kind of performance is related to the capabilities of the link layer to move the IPv6 packets fast enough.
=> [PAUL] The typical IPv6 control-plane operations such as ND messages and DAD take some time to be ready for actual IPv6 data packet transmissions. We updated the text to link it to IPv6 more.

2nd paragraph, Section 5

OLD	NEW
For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges.	For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so the IPv6 control plane (e.g., ND procedure and DAD) needs to support this order of magnitude for application message exchanges.

**** Section 5.1.1**

> **For instance, some IPv6 protocols assume symmetry in the connectivity**

among neighboring interfaces [RFC6250].

RFC6250 (Section 3.1.1) seems to be saying the opposite of this sentence which is that symmetry can’t be assumed. What protocols are making this assumption?

=> [PAUL] Here the referred RFC6250 is to say the asymmetry of the links. We modified the sentence to reflect this point.

2nd paragraph, Section 5.1.1

OLD	NEW
For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces [RFC6250]. However, radio interference and different levels of transmission power may cause asymmetric links to appear in vehicular wireless links. As a result, a new vehicular link model needs to consider the asymmetry of dynamically changing vehicular wireless links.	For instance, some IPv6 protocols such as NUD [RFC4861] and MIPv6 [RFC6275] assume symmetry in the connectivity among neighboring interfaces. However, radio interference and different levels of transmission power may cause asymmetric links to appear in vehicular wireless links [RFC6250]. As a result, a new vehicular link model needs to consider the asymmetry of dynamically changing vehicular wireless links.

**** Section 5.1.2**

However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

No issues. However, isn’t this true for all of the VIP and VND work (as in, it needs more testing)?

=> [PAUL] Yes, it is true. To clarify it, we removed this sentence.

1st paragraph, Section 5.1.2

OLD	NEW
For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used, so that the MAC address can be changed periodically. However, although such a pseudonym of a MAC address can protect to some extent the privacy of a vehicle, it may not be able to	For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used, so that the MAC address can be changed periodically. However, although such a pseudonym of a MAC address can protect to some extent the privacy of a vehicle, it may not be able to

resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. ~~However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.~~ Note that [I-D.ietf-madinas-mac-address-randomization] discusses more about MAC address randomization, and [I-D.ietf-madinas-use-cases] describes several use cases for MAC address randomization.	resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. Note that [I-D.ietf-madinas-mac-address-randomization] discusses more about MAC address randomization, and [I-D.ietf-madinas-use-cases] describes several use cases for MAC address randomization.

**** Section 6.**

For the authentication in vehicular networks, vehicular cloud needs to support a kind of Public Key Infrastructure (PKI) in an efficient way.

What does the qualifier of “a kind of” PKI mean?

=> [PAUL] We wanted to express that a PKI can be either a dedicated infrastructure or a co-located component inside a TCC. We updated the text to reflect this point.

1st paragraph, Section 6

OLD	NEW
For the authentication in vehicular networks, vehicular cloud needs to support a ~~kind of~~ Public Key Infrastructure (PKI) efficiently.	For the authentication in vehicular networks, vehicular cloud needs to support a Public Key Infrastructure (PKI) efficiently, either a dedicated or a co-located component inside a TCC.

**** Section 6**

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.

Is securing arbitrary communication between a smartphone-A in vehicle-1 and smartphone-B in vehicle-2 in scope?
=> [PAUL] Yes, in the current text, it is included in the scope, though 3GPP has some standards (such as Device-to-Device communications) to enable two UEs to communicate with each other directly. A smartphone inside a vehicle can use the link provided by the vehicle to communicate with a device in another vehicle.

** Section 6.
Even though a vehicle is perfectly authenticated and legitimate,

What does it mean for a vehicle to be legitimate? Authenticated to whom?
=> [PAUL] Being legitimate here means legitimately tracking or collecting another vehicle's data for such as telemetry use. In this context, an authenticated vehicle means that the identity of the vehicle has been verified by another vehicle or a security server with one or more security means such as a certificate authentication.

We updated the text to clarify this point.

2nd paragraph, Section 6

OLD	NEW
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.	Even though a vehicle is perfectly authenticated by another entity and legitimate to use the data generated by another vehicle, it may be hacked for running malicious applications to track and collect its and other vehicles' information.

** Section 6
Note that when driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks.

This doesn't seem framed right. Why is it _more vulnerable_? More relative to what? I think the central idea is that like any network (e.g., public library, IETF conference network), the end-node assumes risk of its packets transiting a network it doesn't control, and exposes itself to "local network/segment" attacks of any peer nodes on the network.
=> [PAUL] Yes, it is what we mean in this context. We modified the text to make it more clear.
2nd paragraph, Section 6

OLD	NEW
Note that when driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks.	Note that when driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks due to the exposure of its in-flight traffic packets.

**** Section 6.3**
Alternatively, for
completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.

-- What is a “completely secure vehicular network”?
=> [PAUL] It means that a failure to prevent a cyberattack shall never happen, though it sounds impossible. But for a special case of vehicular networks, it requires the level of security guarantee. We augmented the text to explain more about the point.
3rd paragraph, Section 6.3

OLD	NEW
To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.	To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. In this way, a failure to prevent a cyberattack shall never happen on a vehicular network. Thus, we need to have an efficient zero-trust framework or mechanism for vehicular networks.

-- There seems to be an architecture mismatch in this aspirational zero trust architecture. How does the premise of “verifying every message” align with focus of this document being IPv6 protocol mechanisms. What is an “IPv6 message”? Is that a packet? It would seem to me that these messages would be application layer matters.

=> [PAUL] The messages to be verified include the control messages generated in the IPv6 layer, such as RS/RA, NS/NA, DAD, and NUD messages. Other application layer messages shall also be verified. We updated the text to clarify it.

1st paragraph, Section 6.3

OLD	NEW
To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. In this way a failure to prevent a cyberattack shall never happen on a vehicular network, considering the special case of it. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.	To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message (such as IPv6 control messages including ND, DAD, NUD, and application layer messages) is necessary. In this way, a failure to prevent a cyberattack shall never happen on a vehicular network. Thus, we need to have an efficient zero-trust framework or mechanism for vehicular networks.

**** Section 6.3**

Each message from a
   vehicle can be treated as a transaction and the neighboring vehicles
   can play the role of peers in a consensus method of a blockchain
   [Bitcoin] [Vehicular-BlockChain].

Same comment as for ZT -- what is an “IPv6 message” that could be put on a blockchain?

=> [PAUL] Here we consider a blockchain system as a security checking framework for IPv6 packets. It is more like a hypothesis. We updated the text to make it more clear.
4th paragraph, Section 6.3

OLD	NEW
For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.	For the non-repudiation of the harmful activities from malicious vehicles, which is difficult for other normal vehicles to identify them, an additional and advanced approach is needed. One possible approach is to use a blockchain-based approach [Bitcoin] as an IPv6 security checking framework. Each IPv6 packet from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.

**** Section 6.3**

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

Given the architecture layout in Figures 1 – 5? Where does this block live? Who checks it? Under what circumstances? It isn't clear how this architectural construct is linked a gap analysis of IPv6 for vehicular networking.
=> [PAUL] The mentioned block (i.e., blockchain framework) in this context can be considered as an infrastructure for IPv6-based vehicular networks.

This kind of infrastructure can record or verify IPv6 packets in a consensus-based way. The idea behind a blockchain system for vehicular networks is that it does not assume a central node to be a checking point for network security. It can be related to IPv6 for the security of vehicular networks when considering a consensus-based mechanism in the IPv6 layer.

We updated the text to clarify the point.

4th paragraph, Section 6.3

OLD	NEW
For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.	For the non-repudiation of the harmful activities from malicious vehicles, which is difficult for other normal vehicles to identify them, an additional and advanced approach is needed. One possible approach is to use a blockchain-based approach [Bitcoin] as an IPv6 security checking framework. Each IPv6 packet from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin] [Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced. In addition, a consensus-based mechanism for the security of vehicular networks in the IPv6 layer can also be considered. A group of servers as blockchain infrastructure can be part of the security checking process in the IP layer.

[Review by Alvaro Retana and Response by Authors]

COMMENT:

I support Roman's and Eric's DISCUSS positions. I, too, found the line between examples and gaps/requirements to be blurry, at best.

This document lists more than 40 Normative references! Most (all?) of them point at examples of potential technology or are there as background. For example, the first few point at MLD/MLDv2, OLSR, NEMO, and a couple of documents about terminology and documentation -- all clearly informative.

This is how the IESG Statement on Normative and Informative References [1] characterizes them:

> Within an RFC, references to other documents fall into two general categories: "normative" and "informative". Normative references specify documents that must be read to understand or implement the technology in the new RFC, or whose technology must be present for the technology in the new RFC to work. An informative reference is not normative; rather, it only provides additional information. For example, an informative reference might provide background or historical information. Informative references are not required to implement the technology in the RFC.

Please examine the references and classify them accordingly.
=> [PAUL] We have examined the references and moved most references to the Informative References section. Now the normative references include RFC4861, RFC4862, RFC6275, and RFC8691 only in the consideration that these RFCs are the core part of IPv6 protocols and IPv6-based vehicular networks.

[1] https://www.ietf.org/about/groups/iesg/statements/normative-informative-references/

[Review by Murray Kucherawy and Response by Authors]

--
COMMENT:
--

First off, this is really interesting stuff. Thanks for putting it together, and I'm looking forward to reading more.

I support Roman's and Eric's DISCUSS positions. I also concur with Alvaro's comments about references.

The shepherd writeup doesn't say why "Informational" is the right type of RFC here. (It becomes obvious quickly, but please still answer the question. We often go to the writeup first.)
=> [PAUL] This document aims at an informational RFC because it specifies a problem statement and use cases in IPv6 vehicular networks along with the gap analysis of the legacy IPv6 and other protocols related to vehicular networks. I believe that our IPWAVE WG chair (Carlos J. Bernardos) will put the above note into the shepherd writeup.

Section 2 defines "Class-Based Safety Plan", "V2I2D", "VMM", "VND", and "VSP", but then those terms don't appear anywhere in the document. (I did find "class-based automatic safety action plan" later.) It also defines "OCB" and "VIP', but then only really uses them as part of reference anchors. On the flipside, I would love to see a definition (or reference) for "UAM".
=> [PAUL] We updated the terms defined in the Terminology section by removing “Class-Based Safety Plan”, “V2I2D”, and “VIP”.

For “VND”, “VMM”, and “VSP”, we updated the text to cite them as follows.

The term “OCB” is used in the 1st paragraph of Section I.

The definition “UAM” has been added in the section.

8th paragraph, Section 5.1

OLD	NEW
For IPv6-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular networks, the delay-bounded data delivery is critical. IPv6 ND needs to work to support those IPv6-based safety	For IPv6-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular networks, the delay-bounded data delivery is critical. IPv6 ND needs to work to support those IPv6-based safety

applications efficiently.	applications efficiently. [I-D.jeong-ipwave-vehicular-neighbor-discovery] introduces a Vehicular Neighbor Discovery (VND) process as an extension of IPv6 ND for IP-based vehicular networks.

8th paragraph, Section 5.2

OLD	NEW
Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275], PMIPv6 [RFC5213], and NEMO [RFC3963], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.	Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275], PMIPv6 [RFC5213], and NEMO [RFC3963], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I. [I-D.jeong-ipwave-vehicular-mobility-management] discusses a Vehicular Mobility Management (VMM) scheme to proactively do handover for vehicles.

8th paragraph, Section 6

OLD	NEW
Vehicles and infrastructure must be authenticated to each other by a password, a key, and/or a fingerprint in order to participate in vehicular networking. For the authentication in vehicular networks, vehicular cloud needs to support a Public Key Infrastructure (PKI) efficiently, either a dedicated or a co-located component inside a TCC. To provide safe interaction between vehicles or between a vehicle and infrastructure, only authenticated nodes (i.e., vehicle and infrastructure node) can participate	Vehicles and infrastructure must be authenticated to each other by a password, a key, and/or a fingerprint in order to participate in vehicular networking. For the authentication in vehicular networks, vehicular cloud needs to support a Public Key Infrastructure (PKI) efficiently, either a dedicated or a co-located component inside a TCC. To provide safe interaction between vehicles or between a vehicle and infrastructure, only authenticated nodes (i.e., vehicle and infrastructure node) can participate

in vehicular networks. 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 securely. Even though a vehicle is perfectly authenticated by another entity and legitimate to use the data generated by the vehicle, 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. Note that when driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks due to the exposure to uncontrollable network traffic.	in vehicular networks. 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 securely. Even though a vehicle is perfectly authenticated by another entity and legitimate to use the data generated by the vehicle, 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. Note that when driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks due to the exposure to uncontrollable network traffic. [I-D.jeong-ipwave-security-privacy] discusses several types of threats for Vehicular Security and Privacy (VSP).

[Review by Paul Wouters and Response by Authors]

I concur with Ronan's DISCUSS concerns.

In addition, I have a few comments:

> **To encourage more vehicles to participate in this cooperative environmental sensing, a reward system will be needed.**

The reward system could be "you are allowed to sell your car and drive it here".
In other words, how things are encouraged seems very open, and not really limited to a reward system. I'd strongly recommend removing blockchain/bitcoin references as these are too speculative - if anything these reward systems seem to be headed towards getting banned or restricted by governments.
=> [PAUL] We removed the paragraph about blockchain stuff as follows.

8th paragraph, Section 3.1

OLD	NEW
~~To encourage more vehicles to participate in this cooperative environmental sensing, a reward system based on IPv6 vehicular networks 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. A logging system needs to use IPv6-based vehicular networks for uploading or sharing sensing activities. In the case of a blockchain, each sensing message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain].~~	

I'm very nervous about adding pedestrians to vehicle networks. It will

be a big privacy concern, especially if these networks are commercially run by for-profit companies as these days companies are very eager to monetize their data. Furthermore, pedestrian gadgets (phones, tablets) usually can only connect to one wifi network, so sacrificing this to V2X might not be what they want when sitting near an intersection at the coffee shop.
=> [PAUL] Yes, in some sense, it has the risk of leaking personal information. In this context, we assume that only the user type information (e.g., pedestrian, cyclist, and scooter) along with location information is shared with vehicle networks, and the actual identity information of a vulnerable road user (VRU) shall not be disclosed. We updated the text in Section 3.3 to reflect this issue.

For the wireless connection issue, we assume that a gadget of a VRU uses multiple interfaces or multiple channels by multiple antennas in wireless communications. That is, a VRU can use Wi-Fi, DSRC, 4G/5G V2X, and BLE for the VRU protection service. We enriched the text as follows.

2nd paragraph, Section 3.3

OLD	NEW
A VRU protection service, such as Safety-Aware Navigation Application (SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., Wi-Fi) with an IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU.	A VRU protection service, such as Safety-Aware Navigation Application (SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., Wi-Fi, DSRC, 4G/5G V2X, and BLE) with an IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU.

also think Bring-Your-Own-Prefix (BYOP)") does not avoid doing DAD, especially if there might be malicious parties around.
=> [PAUL] We have removed the inaccurate description for the case of BYOP.

> **Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. To minimize this kind of risk, an reinforced identification and verification protocol shall be implemented.**

I don't see easy solutions here. No one wants to give control of their vehicle network to another entity - even if identification/verification is "reinforced".

=> [PAUL] Yes, that is true. It can be envisioned that in the future all vehicles are unmanned, and there ought to be a way to control or telemetry vehicles through vehicular networks for either the driving safety or add-valued services. Perhaps separating the core control functions of a vehicle with other functions is one of the ways. From IPv6 protocol point of view, an enhanced version of the network layer protocol can be the starting point for the issue.

> **For doing so, we shall have an**
> **efficient zero-trust framework or mechanism for vehicular networks.**

There is a lot of heavy lifting done by this one sentence. Especially when it is also being combined with blockchain/bitcoin solutions. All of these mechanisms seem many orders of magnitude slower than for an attacker to pretend to be a new and different vehicle.

=> [PAUL] We have removed the blockchain/bitcoin solutions in Section 3.

[Review by Zaheduzzaman Sarker and Response by Authors]

Thanks for working on this informational document.

I found this document a good read from the vehicular connectivity and networking point of view, however, there are some cases where the descriptions are not clear to convey the message and required ask. Specially in section 4 and section 6. I think Roman already have covered most of those. Hence supporting his discuss points regarding those sections.

I also have following observation/comments which I believe if addressed will improve the document-

*** Abstract: I actually didn't find enumerated requirements form the problem statements that obviously. Hence, I would suggest to remove this part ("then enumerates requirements for the extensions of those IPv6 protocols for IPv6-based vehicular networking") from the abstract. Lets stick to what the title says. Otherwise, I would expect a numbered list of requirements that the wg would like to refer to and fulfill in future works.**
=> [PAUL] We rephrased the sentence to clarify the point. Now it becomes "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 enumerates gaps for the extensions of those IPv6 protocols for IPv6-based vehicular networking."

*** Please add V2P (and X2P) definitions like others in the terminology section.**
=> [PAUL] We added the definition for V2P as follows.

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

*** Section 3.1: it says -**

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

This seems like a misfit to the use case section and felt more like belongs to some sort of requirement for a reward system. I would suggest to just remove this paragraph.
=> [PAUL] We have removed this paragraph for clarity.

*** Section 5: it says -**

"Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a relatively short time compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles"

While it is true that vehicles can move with "great speed", it is also true that the relative speeds between vehicles might not be that "great", e.g. platooning case. And when vehicles passes each other or a IP-RSU really fast there might not be enough time to setup the link layer connection and V2I communication becomes more important. I found the quoted section of problem statement to be ignorant of these facts and missing the potential relation among V2V, V2I and V2X connectivity and communication.
=> [PAUL] Thanks for pointing out the issue. We augmented the text to reflect this point.

1st paragraph, Section 5

OLD	NEW
In order to specify protocols using the architecture mentioned in Section 4.1, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a relatively short time compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles.	In order to specify protocols using the architecture mentioned in Section 4.1, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a relatively short time compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles. In these cases, vehicles may not have enough time either to build link-layer connections with each other and may rely more on connections with infrastructure. In other cases, the relative speed between vehicles may be low when vehicles move toward the same direction or are platooned. For those cases, vehicles can have more

	time to build and maintain connections with each other.

*** I would note that, for the use case and problem statement, tranport-layer session mobility and usage of available bandwidth mentioned in the document. However, those are not discussed with details but I understand would play vital role to support the discussed application use cases and architecture. I assume this might be due to the scope of the document but this document should say something about those aspect, at least mention as potential future work that need to fulfill the envisioned use cases.**

=> [PAUL] We updated the text to note the case as follows.

3rd paragraph, Section 5

OLD	NEW
This section presents key topics such as neighbor discovery and mobility management for links and sessions in IPv6-based vehicular networks.	This section presents key topics such as neighbor discovery and mobility management for links and sessions in IPv6-based vehicular networks. Note that the detailed discussion on the transport-layer session mobility and usage of available bandwidth to fulfill the use cases is left as potential future work.

[Review by Robert Wilton and Response by Authors]

I'm not an expect on these areas of technology, but I find parts of this document to be quite uncompelling. However, it is an informational document, where considerable latitude is allowed.

Although I'm happy for the authors to correct my misunderstandings below, if they wish, I'm doubtful that such a discussion will really be helpful, hence my abstain ballot.

Some of my concerns when reviewing this document:

(1) It feels like quite a lot of these problems are (or could be) solved today using the existing wireless networks and GPS already included in cars. E.g., presumably they are already making use of IP over 4G-LTE without needing these proposed protocol changes? I.e., how many of the problems described here can really be most efficiently solved by having a local dynamic network?
=> [PAUL] Yes, IP has already been used in 4G-LTE for UE communicating with a remote server (i.e., uplink and downlink), which is just like a traditional host-router model. But in vehicular networks, the things become different in that vehicles shall communicate with each other (i.e., V2V), vehicles can use relay vehicles to connect to the Internet (i.e., V2V2V), and in-vehicle devices (i.e., either built-in or not) shall also be able to communicate with devices in other vehicles (V2V2D). All these scenarios require changing or enhancing the existing IPv6 protocols.

For the IPv6 layer, an enhanced IPv6 ND process in the IP layer can better support multihop forwarding of IPv6 control messages by vehicles to improve the data packet forwarding, which may not be supported well now. In addition, better mobility handling in the IP layer that uses the trajectory information of vehicles can also improve the performance of the current mobility support.

(2) Having some sort of bitcoin/blockchain based micropayment scheme for sharing sensor data between vehicles feels highly implausible to me, given that the world hasn't seemed to manage a micropayment scheme for websites which seems like an easier problem to solve.
=> [PAUL] We have removed the paragraph in Section 3.1 about the blockchain stuff.

(3) Would vehicles even be able to safely trust sensor data coming from other vehicles? E.g., hacked vehicles that randomly occasionally inject false sensor readings. Who would have legal liability if your vehicle takes some action based on unreliable 3rd party sensor data? I appreciate that it

outside this type of technical document, but I think that it limits the likely hood of solving this in an ad hoc network.
=> [PAUL] Roman Danyliw also mentioned these issues. We have updated the text at several places in the draft to make it clearer such as the legal liability party. Please find the modifications from Roman Danyliw’s comments.

(4) I struggle to understand how the V2X use cases really work. In a street (at least in the UK) there would often be people in very close proximity to a vehicle (e.g., walking on the pavement [sidewalk] next to a vehicle, and presumably it is only people in front of the vehicle that are potential collision problems, and for these cases, are radar/lidar/cameras/sensors not a more robust choice (and are already deployed today, and seemingly improving every year). I would think that the only way that this could work with a smartphone is if it sharing very precise (0.1 m) location data all the time to everything around it, which would probably degrade the battery and would also seem to have some serious privacy considerations.
=> [PAUL] The scenario you mentioned is quite interesting. It is true that we need more accurate location information of vulnerable road users (VRUs). But we assume that motion predictions by those sensing means (i.e., radar, lidar, or camera) in a vehicle or an IP-RSU can send alarms to vehicles. For the scenario you mentioned, though vehicles and VRUs are in very close proximity, a prediction engine based on AI (i.e., machine learning or deep learning) is able to forecast a possible collision. Certainly this is a very practical issue and much research is ongoing, but for making that become true, the network part of a vehicular network shall be considered in near future.

(5) In Appendix D, I don't understand how the AERO/OMNI service solves the MTU problem. It seems to be just introducing another layer to solve exactly the problem that are already solved by existing transport layer protocols. If there is some data illustrating how TCP over OAL (with IP parcels) is more efficient that straight TCP over IP then that would be worth sharing.
=> [PAUL] According to AERO/OMNI, a bigger MTU is used to transmit bigger packets by using the IPv6 fragmentation and reassembly. The actual MTUs in the network would still be the same as they are. It is just that from the upper layers, larger packets can be sent out once instead of splitting them into multiple small packets.

Regards,
Rob

[Review by Daniel Migault and Response by Authors]

Reviewer: Daniel Migault
Review result: Has Nits

Hi,

I am still a bit uncomfortable with the message of the use case 3.3 where pedestrians or cyclists need to carry a mobile phone to avoid being knocked down by a car - at least that is how I read it.

The reason is that, in many places, drivers are not paying enough attention to pedestrians and cyclists - even considering their presence on the road as an aggression. As a rebound effect your application that aims at providing more security for the vulnerable pedestrian or cyclist, is likely to result in walking/cycling being more dangerous. Drivers may rely on that application to detect the presence of pedestrians and cyclists and defer the responsibility of being knocked down to the pedestrian or cyclist wearing this application. This is problematic as drivers will likely be even less careful toward pedestrians and cyclists which increases the most vulnerable persons (here I am thinking of kids) as they do not have such mobile phones.

For this reason, I do not think the use case is neither appropriate, nor convincing. The use case sounded to me a bit like the "IPv6 fridge". I would rather consider such use case more appropriate for specific environments such as construction sites where everyone may be required to carry such applications. My recommendation would be to reformulate the use case for these environments. This probably requires very minor changes in the text.

That said, I let you decide what to do with it, as it might also reflect a personal view, and I do not want to slow the publication of document. Feel free to let me know, if you need more information.
=> [PAUL] We understand the concerns from the reviewer. We modified the V2X use case to reflect this comment as follows.

1st paragraph, Section 3.3

OLD	NEW
The use case of V2X networking discussed in this section is for a vulnerable road user (VRU) (e.g., pedestrian) protection service.	The use case of V2X networking discussed in this section is for a vulnerable road user (VRU) (e.g., pedestrian) protection service. Note that the application area of this use case is currently limited to a

	specific environment, such as construction sites, plants, and factories, since not every VRU (e.g., children) in a public area (e.g., streets) is equipped with a smart device (e.g., smartphone).

Yours,
Daniel

Thanks for your valuable comments.

Best Regards,
Jaehoon (Paul) Jeong