Revision Letter

Editor: Jaehoon (Paul) Jeong
Date: March 30, 2022

OLD: draft-ietf-ipwave-vehicular-networking-27
NEW: draft-ietf-ipwave-vehicular-networking-28

Hi Pascal, Fred, Jim, and Daniel,

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 Pascal Thubert and Response by Authors]

I am an assigned INT directorate reviewer for draft-ietf-ipwave-vehicular-networking-27. These comments were written primarily for the benefit of the Internet Area Directors. Document editors and shepherd(s) should treat these comments just like they would treat comments from any other IETF contributors and resolve them along with any other Last Call comments that have been received. For more details on the INT Directorate, see https://datatracker.ietf.org/group/intdir/about/ <https://datatracker.ietf.org/group/intdir/about/>.

Based on my review, the document IS ready to go to IETF Last Call and therefore CAN be forwarded to the IESG.

I find the document well written, well referenced, and very informative. It fits the general goal of use-cases and problem statement publication.

The following are other issues I found with this document that SHOULD be corrected before publication:

Fig 1 and section 4.1 show a “Corresponding Node”. Not sure where the term comes from, in NMIP and NEMO it is “Correspondent Node” see and refer to RFC 4885.

=> [PAUL] We have updated the term to align with RFC 4885.

Fig. 1 is updated with “Correspondent Node”.

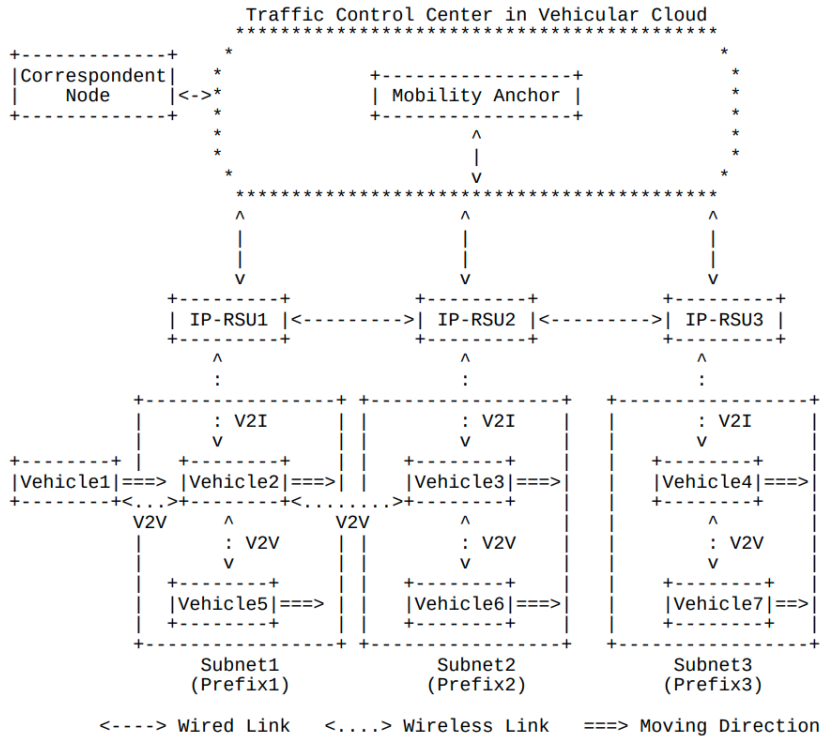

Figure 1: An Example Vehicular Network Architecture for V2I and V2V

The last paragraph, Section 4.1

Old	New
In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a corresponding node in the vehicular cloud, Vehicle2 can move from IP-RSU1's wireless coverage to IP-RSU2's wireless coverage.	In 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.

About

Section 3.1: “

To support applications of these V2I use cases, the required functions of IPv6 include IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and an infrastructure node (e.g., IP-RSU) in the vehicular network.

“

Section 3.2: “ To support applications of these V2I use cases, the required functions of IPv6 include IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and an infrastructure node (e.g., IP-RSU) in the vehicular network.

”

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.

“

Each time, the text could clarify what goes in “packet exchange” since as written that seems to refer to data plane while the problem for IP is mostly control plane. e.g., the problem of discovering adjacent peers (addresses, networks) should be listed there shouldn’t it? Addressing is an topic of interest as well (BYO Address/Prefix vs. obtain a local address, how that relates with DAD and global connectivity). The doc discusses that heavily (around 5.1) and then there’s the discussion in 4.3 on ND variations and (MANET) NHDP, that must happen before IPv6 packets can be exchanged.

As a hint, a suggestion can be:

“

… functions of IPv6 include IPv6 communication enablement with neighborhood discovery and IPv6 address management, reachability with adapted network models and routing methods, transport-layer …

“

=> [PAUL] We revised the text to reflect this comment as follows.

The last paragraph, Section 3.2

Old	New
To support applications of these V2I use cases, the required functions of IPv6 include IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and an infrastructure node (e.g., IP-RSU) in the vehicular network.	To support applications of these V2I use cases, the required functions of IPv6 include IPv6 communication enablement with neighborhood discovery and IPv6 address management, reachability with adapted network models and routing methods, transport-layer session continuity, and secure, safe communication between a vehicle and an infrastructure node

	(e.g., IP-RSU) in the vehicular network.

Section 3.2

Fred said ‘
3) Section 3.2, change the paragraph beginning: "The existing IPv6 protocol must be augmented through protocol changes..."
to:
"The existing IPv6 protocol must be augmented either through protocol changes or by including a new adaptation layer in the architecture that efficiently maps IPv6 to a diversity of link layer technologies. Augmentation is necessary to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles."
‘

I agree that the document omits V2V2I completely. This is true in Fred’s highway case, but true also in a simple parking lot to share Wi-Fi access when the AP is too far. In the MIPv6 family we called that nested NEMO. The problem statement of nested NEMO is RFC 4888. I believe you need to provide a minimum of hint that V2V2I exists and for the lack of more reference you can search “nested NEMO”.

Note that the early RPL was a solution for nested NEMO and interworked with NEMO. It has been tested successfully by NASA at their Glenn Center but I do not think something was published at the time, so no ref.

Note that I also agree with Fred’s point on 3.3. Maybe you can make it more verbose but in each case there’s a need to indicate that V2A2B can exist and needs future attention, even if it is a harder problem.
=> [PAUL] The nested NEMO scenario described in RFC 4888 is a bit different from the scenario in the current draft. RFC 4888 considered the problem where a Mobile Network Node (MNN) located inside a multiple nested Mobile Router (MR) may have a sub-optimal pinball route toward a Correspondent Node (CN). But for the case of V2V2I based on the architecture (i.e., Figure 3) in the current draft, each vehicle (i.e., MR) is not nested by another vehicle and only hosts and routers inside a vehicle fall into the nested NEMO scenario. For a more complete description for the issue, we added the nested NEMO scenario in this context.

For the case of V2V2I, another draft in IPWAVE WG proposes a vehicular ND with multihop DAD process (i.e., Vehicular Neighbor Discovery for IP-Based Vehicular Networks) for vehicles which are not covered by an RSU to have prefix information to configure an IPv6 address. Based on the comment from Fred, we also updated the text accordingly.

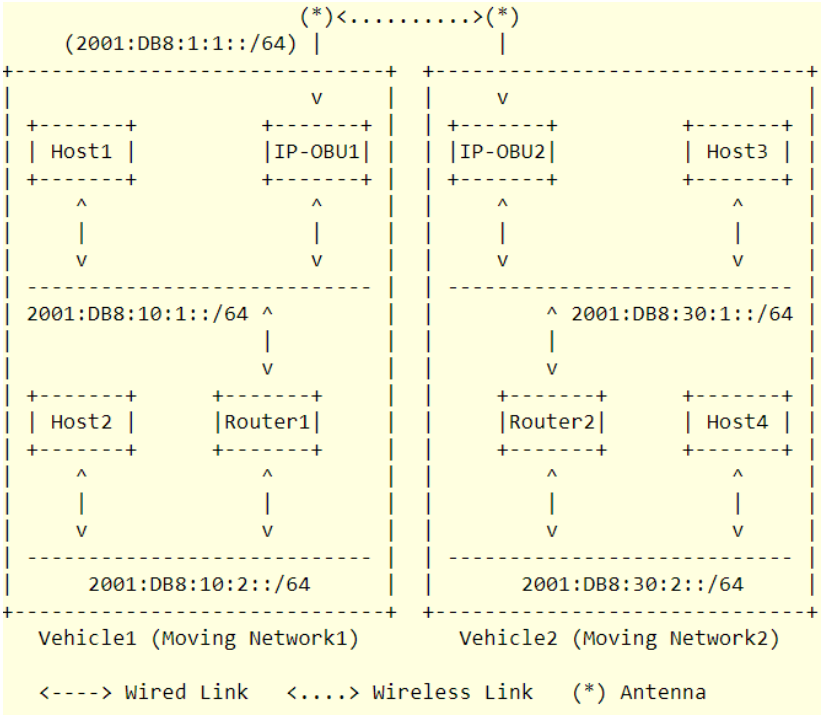

Figure 3: Internetworking between Two Vehicles

The 7th paragraph, Section 3.2

Old	New
The existing IPv6 protocol must be augmented through protocol changes in order to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles. Thus, IPv6 needs to be extended for multihop V2I communications.	In some scenarios such as vehicles moving in highways or staying in parking lots, a V2V2I network is necessary for vehicles to access the Internet since some vehicles may not be covered by an RSU. For those vehicles, a few relay vehicles can help to build the Internet access. For the nested NEMO described in [RFC4888], hosts inside a vehicle shown in Figure 3 for the case of V2V2I may have the same issue in the nested NEMO scenario. To better support these use cases,

	the existing IPv6 protocol must be augmented either through protocol changes or by including a new adaptation layer in the architecture that efficiently maps IPv6 to a diversity of link layer technologies. Augmentation is necessary to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles as packet forwarders. Thus, IPv6 needs to be extended for multihop V2I communications.

Section 4.1:
“

In
this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275] …

…
“

Section 4.2:

“

Existing network architectures, such as the network architectures of PMIPv6 [RFC5213] …

“

I see you have a reference to NEMO in the introduction, but this is where the reference makes the most sense and it is missing, next to PMIPv6.

It is easy to confuse network-based mobility (which is PMIPv6 vs. MIPv6, and is MIPv4 anyway) and network mobility, which is the case of a car that has a /64 inside and has to handle mobility for the /64.

Indeed NEMO is the MIPv6 for networks (a mobile prefix inside the car vs. MIP/PMIP which is a host address moving) and vehicles where a main use case for it. PMIPv6 is a variation of MIPv6 that distributes the roles differently for the lack of support by end devices, but does not route for a mobile

prefix. Network-based does not mean “mobile network”, and then you often call the mobile network a moving network, again per RFC 4885.

For the latter, please stick to IETF terminology of “mobile network” as in RFC 3963, that will help the reader. I suggest you reference RFC 3963 here, and add RFC 4888 for completeness.
=> [PAUL] We added the reference for NEMO (i.e., RFC 3963) and Network Mobility Support (i.e., RFC 4885 and RFC 4888). Also, we replaced “moving network” with “mobile network” in the document.

The last paragraph, Section 4.1

Old	New
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] and AERO [I-D.templin-6man-aero]). This document describes issues in mobility management for vehicular networks in Section 5.2.	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.

Section 4.1:

“

Alternatively, mobile nodes can employ a "Bring-Your-Own-Addresses (BYOA)" 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].

“

Again listing Bring your own prefix as well as address would improve completeness. A typical car has a mobile prefix inside.
=> [PAUL] We added the “prefix” as "Bring-Your-Own-Prefix (BYOP)" to make the description more complete.

The last paragraph, Section 4.1

Old	New

Alternatively, mobile nodes can employ a "Bring-Your-Own-Addresses (BYOA)" 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, which does not require the messaging (e.g., Duplicate Address Detection (DAD)) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862].

Section 4.2:
“
OMNI can support the
“

Suggest “OMNI is designed to support” unless there’s an actual reference?
=> [PAUL] We rephrased the sentence to reflect this point.

The 2nd paragraph, Section 4.1

Old	New
Also, refer to Appendix A for the description of how OMNI can support the use of multiple radio technologies in V2X.	Also, refer to Appendix A for the description of how OMNI is designed to support the use of multiple radio technologies in V2X.

Section 4.3
Fred says “
Section 4.3, final paragraph, there is no reason to cite as examples all RFC variants of the OLSR protocol and all extensions of the DLEP protocol - pick one (or at most 2) RFCs for each. Also, it is important to state that standard OSPF routing has been optimized to support MANET applications.
Suggested rewrite:
"...which serves MANET routing protocols such as the different versions of Optimized Link State Routing Protocol (OLSR) [RFC3626][RFC7181], Open Shortest Path First (OSPF) derivatives (e.g., [RFC5614]) and the Dynamic Link Exchange Protocol (DLEP) [RFC8175] with its extensions."

“
I agree. Maybe mention that there are V2V use case with a fixed set of cars (platooning) and others with variable neighborhood (parking lot, on the road), and the optimum solution may vary.

=> [PAUL] We updated the text to simplify the description based on Fred's comment. We also augmented the description based on Pascal's comment.

The last paragraph, Section 4.3

Old	New
For the reliability required in V2V networking, the ND optimization defined in MANET [RFC6130] [RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases, which serves the MANET routing protocols such as the difference versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181] [RFC7188] [RFC7722] [RFC7779] [RFC8218] and the Dynamic Link Exchange Protocol (DLEP) with its extensions [RFC8175] [RFC8629] [RFC8651] [RFC8703]. In short, the MANET ND mainly deals with maintaining extended network neighbors. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes to improve the reliability, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services. For a more reliable V2V networking, some redundancy mechanisms should be provided in L3 in the case of the failure of L2.	For the reliability required in V2V networking, the ND optimization defined in MANET [RFC6130] [RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases, which serves the MANET routing protocols such as the different versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181], Open Shortest Path First (OSPF) derivatives (e.g., [RFC5614]), and Dynamic Link Exchange Protocol (DLEP) [RFC8175] with its extensions [RFC8629] [RFC8757]. In short, the MANET ND mainly deals with maintaining extended network neighbors to enhance the link reliability. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes to improve the reliability, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services. For a more reliable V2V networking, some redundancy mechanisms should be provided in L3 in cases of the failure of L2. For different use cases, the optimal solution to improve V2V networking reliability may vary. For example, a group of vehicles in platooning may have stabler neighbors than freely moving vehicles, as described in Section 3.1.

Section 5:

“is 72 seconds” looks precise though in fact it is very rough. Could say “in the order of a minute”. Same for V2V, 36s.
=> [PAUL] We reflected this comment by updating the text as follows:

The 2nd paragraph, Section 5

Old	New
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 72 seconds, and the lifetime of a link between two vehicles is 36 seconds.	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.

Section 5.1.1

“off-link”

That terminology does not really exist. All we have is “not-onlink”.
=> [PAUL] We updated the term by using “not-onlink” throughout the draft.

The 4th paragraph, Section 5.1

Old	New
According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or an off-link host even though the source vehicle can use the same prefix as the destination vehicle [I-D.ietf-intarea-ippl].	According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or a not-onlink host even though the source vehicle can use the same prefix as the destination vehicle [I-D.ietf-intarea-ippl].

The 5th paragraph, Section 5.1.1

Old	New
From the previous observation, a	From the previous observation, a

vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model needs to use an on-link prefix and off-link prefix according to the network topology of vehicles such as a one-hop reachable network and a multihop reachable network (or partitioned networks). If the vehicles with the same prefix are reachable from each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable from each other in one hop due to either the multihop topology in the VANET or multiple partitions, the prefix should be off-link. In most cases in vehicular networks, due to the partitioning and merging of VANETs, and the multihop network topology of VANETS, off-link prefixes will be used for vehicles as default.	vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model needs to use an on-link prefix and not-onlink prefix according to the network topology of vehicles such as a one-hop reachable network and a multihop reachable network (or partitioned networks). If the vehicles with the same prefix are reachable from each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable from each other in one hop due to either the multihop topology in the VANET or multiple partitions, the prefix should be not-onlink. In most cases in vehicular networks, due to the partitioning and merging of VANETs, and the multihop network topology of VANETS, not-onlink prefixes will be used for vehicles as default.

Section 5.2

“There is nonnegligible
control overhead to set up and maintain routes to such a tunnel home over the VANET.”

There again a link to RFC 4888
=> [PAUL] We added a reference for RFC4888 as follows:

The 6th paragraph, Section 5.2

Old	New
There is nonnegligible control overhead to set up and maintain routes to such a tunnel home over the VANET.	There is nonnegligible control overhead to set up and maintain routes to such a tunnel home [RFC4888] over the VANET.

“Vehicles can use the TCC as their Home Network having a home agent

for mobility management as in MIPv6 [RFC6275] and PMIPv6 [RFC5213],"

add "and NEMO [RFC 3963]"
=> [PAUL] We added the reference for NEMO as follows:

The 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] and PMIPv6 [RFC5213], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management.	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.

Appendix A: Mentions OMNI but fails to document real world implemented protocols such as DLEP which abstract the radio modem over ethernet
=> [PAUL] We augmented Appendix A to include the DLEP case.

Appendix A

Old	New
Vehicular networks may consist of multiple radio technologies such as DSRC and 5G V2X. Although a Layer-2 solution can provide a support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X. Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., Overlay Multilink Network (OMNI) Interface [I-D.templin-6man-omni]) and/or protocol changes in order to support both wireless single-hop/multihop	Vehicular networks may consist of multiple radio technologies such as DSRC and 5G V2X. Although a Layer-2 solution can provide support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X. Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., OMNI [I-D.templin-6man-omni] and DLEP [RFC8175]) and/or protocol changes in order to support both wireless single-hop/multihop V2V

V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard information in a highway having multiple kinds of radio technologies.	communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard information in a highway having multiple kinds of radio technologies.

The following are minor issues (typos, misspelling, minor text improvements) with the document:

Section 5.1:
“

This merging and partitioning should be considered for the IPv6 ND such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862].

“

“

they may not communicate with each other not in one hop in the same

“

I can understand but the language seems incorrect.
=> [PAUL] We updated the text to make it clearer for the description.

The 4th paragraph, Section 5.1.1

Old	New
Even though two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, they may not communicate with each other not in one hop in the same VANET because of the multihop network connectivity between them.	Considering that two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, if they are not in one hop (that is, they have the multihop network connectivity between them), then they may not be able to communicate with each other.

Also Fred says:
‘

change: "they need to be configured with a link-local IPv6 address or a global IPv6 address"
to:

"they need to be configured with link-local, unique-local and/or global IPv6 addresses"

‘

I mostly agree but then, those addresses are not necessarily configured. Maybe just says that they need the addresses.
=> [PAUL] We simplify the text for a concise description.

The 2nd paragraph, Section 5.1

Old	New
Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and run IPv6 ND.	Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need IPv6 addresses to run IPv6 ND.

Section 6.1

“the DAD”: we usually do not have the “the”. This appears throughout.
=> [PAUL] We have removed “the” before DAD throughout the draft.

Voila!

Pascal

[Review by Fred Templin and Response by Authors]

Comments from Fred
Comments on 'draft-ietf-ipwave-vehicular-networking-26.txt':
****

1) Section 1, change: "Asymmetric Extended Route Optimization (AERO)
[I-D.templin-6man-aero]"
to:
"Automatic Extended Route Optimization based on the Overlay Multilink
Network Interface (AERO/OMNI)
[I-D.templin-6man-aero][I-D.templin-6man-omni]".

=> [PAUL] We have updated the name for AERO and the references based on this comment.

2) Section 3, change: "The use cases presented in this section serve as
the description and motivation for the need to extend IPv6 and its protocols
to facilitate "Vehicular IPv6"."
to:
"The use cases presented in this section serve as the description and
motivation
for the need to augment IPv6 and its protocols to facilitate "Vehicular
IPv6"."

=> [PAUL] We updated the text according to this comment.

3) Section 3.2, change the paragraph beginning: "The existing IPv6 protocol
must be augmented through protocol changes..."
to:
"The existing IPv6 protocol must be augmented either through protocol changes
or by including a new adaptation layer in the architecture that efficiently
maps IPv6 to a diversity of link layer technologies. Augmentation is
necessary
to support wireless multihop V2I communications in a highway where RSUs are
sparsely deployed, so a vehicle can reach the wireless coverage of an RSU
through the multihop data forwarding of intermediate vehicles."

=> [PAUL] This comment has been resolved along with Pascal's comment above on Pages 4-6 in this document.

4) Section 3.3, change the paragraph beginning: "The existing IPv6 protocol must be augmented through protocol changes..."
to:
"The existing IPv6 protocol must be augmented through protocol changes or by including a new adaptation layer in the architecture that efficiently maps IPv6 to a diversity of underlying link layer technologies. Augmentation is necessary to support wireless multihop V2X or V2I2X communications in an urban road network where RSUs are deployed at intersections, so a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles (or pedestrians'smartphones) as packet forwarders."
=> [PAUL] This comment has been resolved along with Pascal's comment above on Pages 4-6 in this document.

5) Section 4.1, second paragraph, change: "OMNI (Overlay Multilink Network Interface) [I-D.templin-6man-omni]"
to:
"AERO/OMNI [I-D.templin-6man-aero][I-D.templin-6man-omni]".

=> [PAUL] We update the text and reference as follows.

The 2nd paragraph, Section 4.1

Old	New
Existing network architectures, such as the network architectures of PMIPv6 [RFC5213], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550], and OMNI (Overlay Multilink Network Interface) [I-D.templin-6man-omni], can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1.	Existing network architectures, such as the network architectures of PMIPv6 [RFC5213], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550], and AERO/OMNI [I-D.templin-6man-aero][I-D.templin-6man-omni], can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1.

6) Section 4.1, third paragraph, change: "Furthermore, the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking. Note that 2001:DB8::/32 is a documentation prefix [RFC3849] for example prefixes in this document, and also that any routable IPv6 address needs to be routable in a VANET and a vehicular network including IP-RSUs."
to:

"In a first addressing alternative, the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking. Note that 2001:DB8::/32 is a documentation prefix [RFC3849] for example prefixes in this document, and also that any routable IPv6 address needs to be routable in a VANET and a vehicular network including IP-RSUs. In a second alternative, each wireless media interface is configured with an IPv6 Unique Local Address (ULA) [RFC4193] that is assured unique within the vehicular network according to AERO/OMNI and [RFC5889]. The ULA supports both V2V and V2I multihop forwarding within the vehicular network (e.g., via a VANET routing protocol) while each vehicle can communicate with Internet correspondents using global IPv6 addresses via OMNI interface encapsulation over the wireless interface."

=> [PAUL] Since the purpose of this draft is for a problem statement, the content suggested in this comment falls into a solution space, which is not aligned with the purpose. We would like to put the suggested text into Appendix B as follows.

The 5th paragraph, Appendix B

Old	New
	In OMNI protocol, each wireless media interface is configured with an IPv6 Unique Local Address (ULA) [RFC4193] that is assured unique within the vehicular network according to AERO/OMNI and [RFC5889]. The ULA supports both V2V and V2I multihop forwarding within the vehicular network (e.g., via a VANET routing protocol) while each vehicle can communicate with Internet correspondents using global IPv6 addresses via OMNI interface encapsulation over the wireless interface.

7) Section 4.1, fifth paragraph, change: "Alternatively, mobile nodes can employ a "Bring-Your-Own-Addresses (BYOA)" 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]."
to:
"Alternatively, mobile nodes can configure IPv6 Unique Local Addresses (ULAs) according AERO/OMNI then support global communications through OMNI interface encapsulation and forwarding of packets with MNP-based global IPv6 addresses over the wireless networks. The use of AERO/OMNI ULA autoconfiguration assures uniqueness such that Duplicate Address Detection (DAD) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862] is not needed."
=> [PAUL] We believe that this comment has been reflected in the 5th and 6th paragraphs of Appendix B.

The 5th paragraph, Appendix B

Old	New
	OMNI defines a protocol for the transmission of IPv6 packets over Overlay Multilink Network Interfaces that are virtual interfaces governing multiple physical network interfaces. OMNI supports multihop V2V communication between vehicles in multiple forwarding hops via intermediate vehicles with OMNI links. It also supports multihop V2I communication between a vehicle and an infrastructure access point by multihop V2V communication. The OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD Messaging. In OMNI protocol, each wireless media interface is configured with an IPv6 Unique Local Address (ULA) [RFC4193] that is assured unique within the vehicular network according to AERO/OMNI and [RFC5889]. The ULA supports both V2V and V2I multihop forwarding within the vehicular network (e.g., via a

	VANET routing protocol) while each vehicle can communicate with Internet correspondents using global IPv6 addresses via OMNI interface encapsulation over the wireless interface.

8) Section 4.2, add the following as a final paragraph:
"In a second alternative when vehicles configure an OMNI interface over an underlying VANET based on ULA addressing, the global IPv6 addresses covered by the MNP on-board the vehicle are not injected into the VANET routing system but instead traverse the VANET in the forwarding plane via OMNI encapsulation. This allows each vehicle to maintain a constant and unchanging MNP delegation even as it moves between IP-RSUs. This avoids any need for vehicle on-board network renumbering due to mobility and avoids repeated injections and withdrawals of MNP prefixes within the VANET.
=> [PAUL] This is the detailed step for OMNI. I will not include it in the IPWAVE PS document. I hope that you can accept this.

9) Section 4.3, add new paragraph following paragraph beginning "Figure 3 shows the internetworking" as follows:
"When two vehicles within a ULA-based VANET need to communicate without the assistance of any infrastructure, they can exchange unencapsulated IPv6 packets with ULA-based addresses which will be forwarded according to the VANET routing protocol. Alternatively, the vehicles can use OMNI interface encapsulation to exchange IPv6 packets with global addresses taken from their respective MNPs. The encapsulation source and destination ULAs are algorithmically bound to the IPv6 source and destination global addresses which allows for stateless encapsulation address determination."
=> [PAUL] This is also the detailed step for OMNI. I will not include it in the IPWAVE PS document. I hope that you can accept this.

10) Section 4.3, final paragraph, there is no reason to cite as examples all RFC variants of the OLSR protocol and all extensions of the DLEP protocol - pick one (or at most 2) RFCs for each. Also, it is important to state that standard OSPF routing has been optimized to support MANET applications. Suggested rewrite:
"...which serves MANET routing protocols such as the different versions of Optimized Link State Routing Protocol (OLSR) [RFC3626][RFC7181], Open Shortest Path First (OSPF) derivatives (e.g., [RFC5614]) and the Dynamic Link Exchange Protocol (DLEP) [RFC8175] with its extensions."

=> [PAUL] We have reflected this comment along with Pascal's comment above in Pages 8-9 in this document.

11) Section 5.1, second paragraph, change: "they need to be configured with a link-local IPv6 address or a global IPv6 address"
to:
"they need to be configured with link-local, unique-local and/or global IPv6 addresses"

=> [PAUL] We updated the text to reflect this comment along with Pascal's comment above in Page 14.

The 2nd paragraph, Section 5.1

Old	New
Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and run IPv6 ND.	Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need IPv6 addresses, and to run IPv6 ND.

12) Section 5.2, third paragraph, change: "An efficient DAD is required to reduce the overhead of the DAD packets during a vehicle's travel in a road network"
to:
"DAD is not needed in networks that follow the OMNI ULA autoconfiguration procedures. In other cases when DAD is needed, it must be made efficient to reduce the overhead of the DAD packets during a vehicle's travel in a road network"
=> [PAUL] This comment is for the 3rd paragraph of Section 5.1, instead of Section 5.2. Since the focus of this draft is on problem statements, we believe that the point of this comment has been solved in the 5th and 6th paragraphs of the Appendix B.

13) Section 5.1.1, third paragraph, change: "There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses."
to:
"There is a relationship between a link and a prefix, besides the

different scopes that are expected from the link-local, unique-local and global types of IPv6 addresses."
=> [PAUL] We updated the text to reflect this comment as follows:

The 3rd paragraph, Section 5.1.1

Old	New
There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses.	There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local, unique-local, and global types of IPv6 addresses.

14) Section 5.1.1, add a new second-to-last paragraph as follows:
"Often when two VANETs merge some vehicles may configure addresses from a first subnet prefix while other vehicles configure addresses from other subnet prefixes. These merge events must not interfere with the vehicle-to-vehicle multihop forwarding necessary to support continuous communications. Additionally, when a vehicle enters the network for the first time it may need to use a temporary ULA address in initial messages to negotiate with an IP-RSU for an address within the subnet. The VANET must therefore provide (short-term) forwarding for vehicles with foreign addresses, while the subnet prefix serves as an aggregation point of reference for a particular IP-RSU without impeding multihop forwarding between vehicles that may belong to different subnets."
=> [PAUL] Even though this description has useful information, but it has too detailed information, I would not include this text into the document. I hope that you can accept this.

15) Section 5.1.3 goes too far in expanding on RPL. It is based on the claim that: "However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead [RFC9119].". But, the AERO/OMNI approach uses only the MANET routing protocol control messages at the subnet level then applies unicast-only IPv6 ND messaging at the OMNI interface level so that there is no traffic amplification due to multicast IPv6 ND within the subnet. Therefore, a new third paragraph telling how it works in AERO/OMNI should be added as follows:
"The AERO/OMNI approach avoids this issue by using MANET routing protocols only (i.e., and no multicast IPv6 ND messaging) in the wireless network underlay while applying efficient unicast IPv6 ND messaging in the OMNI overlay on an as-needed basis for router discovery and NUD. This greatly reduces the overhead for VANET-wide multicasting while providing agile

accommodation for dynamic topology changes."

Additionally, the RPL text should be reduced by at least 50%.
=> [PAUL] Since RPL is in already published RFCs, we describe it in detail for possible technology gaps in vehicular networks. We reflected your comment about AERO/OMNI on the 7th paragraph of Appendix B as follows:

The 7th paragraph, Appendix B

Old	New
	For the control traffic overhead for running both vehicular ND and a VANET routing protocol, the AERO/OMNI approach may avoid this issue by using MANET routing protocols only (i.e., no multicast of IPv6 ND messaging) in the wireless underlay network while applying efficient unicast IPv6 ND messaging in the OMNI overlay on an as-needed basis for router discovery and NUD. This greatly reduces the overhead for VANET-wide multicasting while providing agile accommodation for dynamic topology changes.

16) Section 5.2, paragraph 6 change: "Even though the SLAAC with classic ND costs a DAD during mobility management, the SLAAC with [RFC8505] does not cost a DAD."
to:
"Even though classic IPv6 ND requires the use of DAD on many link types during mobility management, address autoconfiguration based on [RFC8505] and/or AERO/OMNI does not require DAD."
=> [PAUL] We would like to minimally revise the text to reflect this comment as follows.

The 6th paragraph, Section 5.2

Old	New
Even though the SLAAC with classic ND costs a DAD during mobility management, the SLAAC with [RFC8505] does not cost a DAD.	Even though the SLAAC with classic ND costs a DAD during mobility management, the SLAAC with [RFC8505] and/or AERO/OMNI do not cost a DAD.

17) Section 5.2, paragraph 6, remove the following text entirely: "On the other hand, a BYOA does not allow such direct routability to the Internet since the BYOA is not topologically correct, that is, not routable in the Internet. In addition, a vehicle configured with a BYOA needs a tunnel home (e.g., IP-RSU) connected to the Internet, and the vehicle needs to know which neighboring vehicle is reachable inside the VANET toward the tunnel home. There is nonnegligible control overhead to set up and maintain routes to such a tunnel home over the VANET."

Reason: There is always a cost for maintaining mobility management for addresses within an MNP. It can be done either by frequent advertisements/withdrawals of the MNP in the global routing system or through coordination with a mobility anchor point in an overlay via encapsulation. The Connexion by Boeing experience showed that dynamic routing protocol updates do not scale in the global Internet. The AERO/OMNI services instead minimize routing protocol disturbance while using efficient mobility signaling in the overlay.
=> [PAUL] Since this draft is a problem statement, the issues in IP-based vehicular networks with a BYOA approach discussed here seems proper. We would like to keep this text as it is.

18) Section 5.2, near the end, remove the following sentence: "IP tunneling over the wireless link should be avoided for performance efficiency."

Reason: IP tunneling is used only in support of global-scoped IPv6 communication (not local-scoped) and can use effective header compression for greater efficiency as in AERO/OMNI. In addition, there is value in using encapsulation both from the standpoint of minimizing global routing protocol overhead and by accommodating path MTU diversity (see below).
=> [PAUL] We updated this sentence for clarity along with Fred’s latest comment as follows.

The 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	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. IP tunneling over the wireless link should be avoided for performance efficiency. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.	mobility information of vehicles for location management. Encapsulation over the wireless link should be minimized for performance efficiency. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.

19) Add a new Section 5.3 as follows:
"5.3 Accommodating MTU Diversity

The wireless and/or wired-line links in paths between both mobile nodes and fixed network correspondents may configure a variety of Maximum Transmission Units (MTUs), where all IPv6 links are required to support a minimum MTU of 1280 octets and MAY support larger MTUs. Unfortunately, determining the path MTU (i.e., the minimum link MTU in the path) has proven to be inefficient and unreliable due to the uncertain nature of the loss-oriented ICMPv6 messaging service used for path MTU discovery. Recent developments have produced a more reliable path MTU determination service for TCP [RFC4821] and UDP [RFC8899] however the MTUs discovered are always limited by the most restrictive link MTU in the path (often 1500 octets or smaller).

The AERO/OMNI service addresses the MTU issue by introducing a new layer in the Internet architecture known as the "OMNI Adaptation Layer (OAL)". The OAL allows end systems that configure an OMNI interface to utilize a full 65535 octet MTU by leveraging the IPv6 fragmentation and reassembly service during encapsulation to produce fragment sizes that are assured of traversing the path without loss due to a size restriction. (This allows end systems to send packets that are often much larger than the actual path MTU.)

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 "packet-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."

=> [PAUL] We would like to add a new appendix (as Appendix D) to describe the MTU issue as follows.

Appendix D

Old	New
	Appendix D. Support of MTU Diversity for IP-based Vehicular Networks The wireless and/or wired-line links in paths between both mobile nodes and fixed network correspondents may configure a variety of Maximum Transmission Units (MTUs), where all IPv6 links are required to support a minimum MTU of 1280 octets and MAY support larger MTUs. Unfortunately, determining the path MTU (i.e., the minimum link MTU in the path) has proven to be inefficient and unreliable due to the uncertain nature of the loss-oriented ICMPv6 messaging service used for path MTU discovery. Recent developments have produced a more reliable path MTU determination service for TCP [RFC4821] and UDP [RFC8899] however the MTUs discovered are always limited by the most restrictive link MTU in the path (often 1500 octets or smaller). The AERO/OMNI service addresses the MTU issue by introducing a new layer in the Internet architecture known as the "OMNI Adaptation Layer (OAL)". The OAL allows end systems that configure an OMNI interface to utilize a full 65535 octet MTU by leveraging the IPv6 fragmentation and reassembly service during encapsulation to produce fragment sizes that are assured of traversing the path without loss due to a size restriction. (This allows end systems to send packets that are often much larger than the actual path MTU.)

	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.

20) Appendix B, add the following as a final paragraph:
"AERO and OMNI together securely and efficiently address the following 6 M's of Modern Internetworking for mobile V2V, V2I and V2X Clients:

1. **Multilink: A Client's ability to coordinate multiple diverse underlying data links as a single logical unit (i.e., the OMNI interface) to achieve the required communications performance and reliability objectives.**

2. **Multinet: The ability to span the OMNI link over a segment routing topology with multiple diverse administrative domain network segments while maintaining seamless E2E communications between mobile Clients and correspondents such as air traffic controllers and fleet administrators.**

3. **Mobility: A Client's ability to change network points of attachment (e.g., moving between wireless base stations) which may result in an underlying interface address change without disruptions to ongoing communication sessions with peers over the OMNI link.**

4. **Multicast: The ability to send a single network transmission that reaches multiple Clients belonging to the same interest group without disturbing other Clients not subscribed to the interest**

group.

5. **Multihop: A mobile Client's V2V relaying capability useful when multiple forwarding hops between vehicles may be necessary to reach back to an infrastructure access point connection to the OMNI link.**

6. **MTU Assurance: The ability to deliver packets of various robust sizes between peers without loss due to a link size restriction, and to dynamically adjust packet sizes in order to achieve the optimal performance for each independent traffic flow."**

=> [PAUL] We have introduced the major functions of AERO/OMNI in this draft and added feature description for AERO/OMNI in Appendices A, B, C, and D. For the current text, we believe that AERO/OMNI has been explained clearly. So we would like not to add this new text into Appendix B to minimize the redundant explanation in the document. We hope that you can understand our motivation.

All, I would like to make the following change to the set of comments I submitted on 2/24/2022:

> 18) Section 5.2, near the end, remove the following sentence: "IP
> tunneling over the wireless link should be avoided for performance
> efficiency."

Rather than removing the sentence, I would instead prefer for the document to make the following revision:

Change:
"IP tunneling over the wireless link should be avoided for performance efficiency."

To:
"Encapsulation over the wireless link should be minimized for performance efficiency."

=> [PAUL] We have updated the text as follows:

The 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	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. IP tunneling over the wireless link should be avoided for performance efficiency. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.	[RFC6275], PMIPv6 [RFC5213], and NEMO [RFC3963], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. Encapsulation over the wireless link should be minimized for performance efficiency. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.

I would expect for all of my other comments to be addressed in the next document version and/or discussed here on the list.

Thank you,

Fred Templin

[Review by Jim Fenton and Response by Authors]

Reviewer: Jim Fenton
Review result: Almost Ready

I am the assigned ART reciewer for draft-ietf-ipwave-vehicular-networking-27. Please note that since I don't have specific background in mobile networking, these comments tend to be editorial in nature.

2. Terminology

The introduction to this section refers to terminology described in RFC 8691, but several of the definitions overlap with definitions there but are not quite the same. Please make it clear which version of the definitions apply here. For example:

- IP-OBU has the additional phrase, "and a device (e.g., smartphone and Internet-of-Things (IoT) device." Does this mean that an additional device is needed in order to have a complete IP-OBU?
=> [PAUL] For clarity, we removed the additional phrase, “and a device (e.g., smartphone and Internet-of-Things (IoT) device)”, as follows.

Section 2

Old	New
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)~~ and a device (e.g., smartphone and Internet-of-Things (IoT) device)~~.	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).

- IP-RSU has the additional sentence, "Also, it may have an IP interface unit that runs in a C-V2X along with an "RSU" transceiver."
=> [PAUL] The term of IP-RSU defined in RFC 8691 is mainly concerned with the wireless 802.11-OCB interface. However, along with the development of the vehicular communication technologies, C-V2X becomes another available wireless interface for vehicular communications. We modified the text to reflect this comment.

Section 2

Old	New
IP-RSU: "IP Roadside Unit": An IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. An IP-RSU communicates with the IP-OBU over an 802.11 wireless link operating in OCB mode. Also, it may have an IP interface that runs in C-V2X along with an "RSU" transceiver.	IP-RSU: "IP Roadside Unit": An IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. An IP-RSU communicates with the IP-OBU over an 802.11 wireless link operating in OCB mode. Also, it may have the third IP-enabled wireless interface running in 3GPP C-V2X in addition to the IP-RSU defined in RFC 8691.

Definition of VSP: It appears there is a word missing following "privacy"
=> [PAUL] We updated the text to reflect this comment.

Section 2

Old	New
VSP: "Vehicular Security and Privacy". It is an IPv6-based security and privacy for vehicular networks.	VSP: "Vehicular Security and Privacy". It is an IPv6-based security and privacy term for vehicular networks.

The definitions of Edge Computing and Edge Network use the term "for the sake of". I'm not clear on what that means: perhaps "to be used by" or "to protect"?
=> [PAUL] We updated the phrase by using “to be used by”.

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	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.	recognition and the localization service to be used by vehicles.

Section 3.1, bullet 5: draft-templin-ipwave-uam-its has expired. Generally this problem statement is not clear on whether Urban Air Mobility is in scope or not. More comments on this below.
=> [PAUL] We have moved the reference for draft-templin-ipwave-uam-its in bullet 5 to the text below. Since this reference is suggested by another reviewer, we cite it in the current version.

Bullet 5, Section 3.1

Old	New
Collision avoidance service of end systems of Urban Air Mobility (UAM) [I-D.templin-ipwave-uam-its].	Collision avoidance service of end systems of Urban Air Mobility (UAM).

Paragraph 7, Section 3.1

Old	New
A collision avoidance service of UAM end systems in air can be envisioned as a use case in air vehicular environments.	A collision avoidance service of UAM end systems in air can be envisioned as a use case in air vehicular environments [I-D.templin-ipwave-uam-its].

Section 3.1 paragraph 5 on EV charging might also mention notification of charging stations that are out of service (a problem I have encountered).
=> [PAUL] It is a good suggestion. We updated the text to reflect this comment in Section 3.2.

Paragraph 5, 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 through a battery charging server connected to the IP-RSU.	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.

Section 4.1 paragraph 3 spends more time talking about RFC 3849 documentation prefixes than anything particularly relevant here. Suggest removing the example prefix since it doesn't really add to the discussion.
=> [PAUL] We removed the text related to the example prefix mentioned here as follows.

Paragraph 3, 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. ~~Note that 2001:DB8::/32 is a documentation prefix [RFC3849] for example prefixes in this document, and also that any routable IPv6 address needs to be routable in a VANET and a vehicular network including IP-RSUs.~~	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.

Section 4.2 paragraph 2 describes connecting user devices to a vehicle's internal network. This is a dangerous idea; it should at a minimum be a separate network.
=> [PAUL] This is a good point. It is dangerous if a vehicle's internal network is controlled by a malicious party. However, for other functions or services such as OTA firmware update and advanced navigation service hosts inside a vehicle may need to be accessed from an external network but with reinforced identification and verification procedures, which can minimize the risk. So developing an identification and verification protocol for this kind of architecture is pivotal. We updated the text to reflect this comment as follows.

Paragraph 2, Section 4.2

Old	New
A vehicle's internal network often uses Ethernet to interconnect Electronic Control Units (ECUs) in the vehicle. The internal network can support Wi-Fi and Bluetooth to accommodate a driver's and passenger's mobile devices (e.g., smartphone or tablet). The network topology and subnetting depend on each vendor's network configuration	A vehicle's internal network often uses Ethernet to interconnect Electronic Control Units (ECUs) in the vehicle. The internal network can support Wi-Fi and Bluetooth to accommodate a driver's and passenger's mobile devices (e.g., smartphone or tablet). The network topology and subnetting depend on each vendor's network configuration

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

Section 4.2 last paragraph and section 5 paragraph 2 calculate dwell (not dwelling) time based on a highway maximum speed of 100 km/h. It is not acceptable to deny service to vehicles exceeding the speed limit, nor to emergency vehicles that may be legitimately doing so. It also isn't clear how this might apply to airborne vehicles. Suggest that if the network is designed around a given maximum speed, that should be at least 250 km/h. It also assumes that traffic can be passed for the entire dwell time, and does not consider physical link establishment, authentication, packet loss, and channel contention from other vehicles.

=> [PAUL] This paragraph is giving an example for the dwelling time estimation, showing a direct experience about the time that a ground vehicle can have Internet access. We updated the text to be more specific about the case of ground vehicles with higher speed and discuss the case of airborne vehicles.

Last paragraph, Section 4.2

Old	New
Let us consider the upload/download time of a vehicle when it passes through the wireless communication coverage of an IP-RSU. For a given typical setting where 1km is the maximum DSRC communication range [DSRC] and 100km/h is the speed limit in highway, the dwelling time can be calculated to be 72 seconds by dividing the diameter of the 2km (i.e., two times of DSRC communication range where an IP-RSU is located in the center of the circle of wireless communication) by the speed limit of 100km/h (i.e., about 28m/s). For the 72 seconds, a	Let us consider the upload/download time of a ground vehicle when it passes through the wireless communication coverage of an IP-RSU. For a given typical setting where 1km is the maximum DSRC communication range [DSRC] and 100km/h is the speed limit in highway for ground vehicles, the dwelling time can be calculated to be 72 seconds by dividing the diameter of the 2km (i.e., two times of DSRC communication range where an IP-RSU is located in the center of the circle of wireless communication) by the speed limit of

vehicle passing through the coverage of an IP-RSU can upload and download data packets to/from the IP-RSU.	100km/h (i.e., about 28m/s). For the 72 seconds, a vehicle passing through the coverage of an IP-RSU can upload and download data packets to/from the IP-RSU. For special cases such as emergency vehicles moving above the speed limit, the dwelling time is relatively shorter than that of other vehicles. For cases of airborne vehicles, considering a higher flying speed and a higher altitude, the dwelling time can be much shorter.

Section 5 paragraph 1 s/time relatively short/relatively short time/
=> [PAUL] We updated the text to reflect this comment as follows.

Paragraph 1, 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 time relatively short 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.

Section 5.1 last paragraph s/changes with the legacy/changes with respect to the legacy/
=> [PAUL] We updated the text to reflect this comment.

Last paragraph, Section 5.1

Old	New
From the interoperability point of view, in IPv6-based vehicular networking, IPv6 ND should have minimum changes with the legacy IPv6 ND used in the Internet, including DAD and NUD operations, so that	From the interoperability point of view, in IPv6-based vehicular networking, IPv6 ND should have minimum changes with respect to the legacy IPv6 ND used in the Internet, including DAD and NUD operations, so

IPv6-based vehicular networks can be seamlessly connected to other intelligent transportation elements (e.g., traffic signals, pedestrian wearable devices, electric scooters, and bus stops) that use the standard IPv6 network settings.	that IPv6-based vehicular networks can be seamlessly connected to other intelligent transportation elements (e.g., traffic signals, pedestrian wearable devices, electric scooters, and bus stops) that use the standard IPv6 network settings.

Section 6: Security Considerations

This problem statement has extreme security considerations so I am glad to see considerable text on this topic. Again, inclusion of driver/passenger's mobile devices (paragraph 2) introduces yet more (possibly avoidable) security issues and should perhaps be reconsidered.
=> [PAUL] Thanks for pointing out this issue. We reflect this issue as follows.

Paragraph 2, 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) in an efficient way. 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 in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles' information. In this case, an attack mitigation process may be	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) in an efficient way. 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 in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles' information. In this case, an attack mitigation process may be

required to reduce the aftermath of malicious behaviors.	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.

One of the primary concerns is the threat to human life. It is essential that these mechanisms fail safely, and be resilient to both malicious attack and equipment failure. As an example of the latter, one can imagine a situation where a cooperating vehicle has a sensor failure (e.g., LIDAR) and reports incorrect information about surrounding vehicles. If that caused other nearby vehicles to collide, there would be a rather interesting question of liability for the collision. While this is not a security concern in the classic sense of most IETF protocols, it needs to be considered in the design of IPWAVE technology.

=> [PAUL] We totally agree on this point. We augmented the text to describe more about this issue.

Paragraph 3, Section 6.1

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

	concerns when designing protocols in IPWAVE.

Privacy considerations are mentioned several times; this is a distinct enough topic to consider the inclusion of a Privacy Considerations section (RFC 6973). The document does describe the use of ephemeral IP addresses to evade tracking based on IP address, but also needs to address the need to protect other mechanisms such as authentication certificates as well. The threat actors for privacy need to be further considered: the document seems to focus primarily on the inability of passive attackers to perform tracking, but some users are also concerned about the ability of the roadway operator (effectively the government) to track their location as well. I am not sure how this problem would be solved, but it should be mentioned.
=> [PAUL] We augmented the text to include the privacy concerns for roadway operators.

Section 6.3

Old	New
To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, especially for a long-living transport-layer session (e.g., voice call over IP and video streaming service), a MAC address pseudonym needs to be provided to each vehicle; that is, each vehicle periodically updates its MAC address and its IPv6 address needs to be updated accordingly by the MAC address change [RFC4086][RFC8981]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality (using either IPsec or TLS), there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses. Thus, the MAC address pseudonym and the IPv6	To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, especially for a long-living transport-layer session (e.g., voice call over IP and video streaming service), a MAC address pseudonym needs to be provided to each vehicle; that is, each vehicle periodically updates its MAC address and its IPv6 address needs to be updated accordingly by the MAC address change [RFC4086][RFC8981]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality (using either IPsec or TLS), there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses. Thus, the MAC address pseudonym and the IPv6

address update should be performed with strong E2E confidentiality.	address update should be performed with strong E2E confidentiality. 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.

8. References

I'm not sure what constitutes a normative vs. informative reference for a problem statement such as this. But it does seem odd that all of the normative references are RFCs and nearly all of the informative references aren't.
=> [PAUL] We put the referenced RFCs in the normative reference section because they are important sources for this problem statement. On the other hand, other sources are put in the informative reference section.

With so many references, it would be nice to have them in alphabetical order. Perhaps the RFC editor will take care of that.
=> [PAUL] Thanks for this suggestion. The referenced RFCs are following alphabetical order.

[Review by Daniel Migault and Response by Authors]

Secdir Telechat review of -27 by Daniel Migault

1. Introduction

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

<mglt>
I am wondering US/EU covers all spectrum allocation worldwide ?
</mglt>
=> [PAUL] Not all, but most countries adopted the 5.9 GHz band for ITS purposes such as vehicular networks.

3.2. V2I

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

<mglt>
Is this use case restricted to the US or do we have any equivalent in EU for example ?
<mglt>
=> [PAUL] To our best knowledge, Public Safety Communications Europe (PSCE) (https://www.psc-europe.eu/) is the equivalent project in Europe for developing public safety communication networks. We updated the text to add this information as follows:

Paragraph 4, 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 First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, e.g., emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to the FirstNet's network core. The current RAN is mainly constructed using 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Report], but it is expected that DSRC-based vehicular networks [DSRC] will be available for V2I and V2V in the near future.	The emergency communication between accident vehicles (or emergency vehicles) and a TCC can be performed via either IP-RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, e.g., emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to the FirstNet's network core. The current RAN is mainly constructed using 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Report], but it is expected that DSRC-based vehicular networks [DSRC] will be available for V2I and V2V in the near future. An equivalent project in Europe is called Public Safety Communications Europe (PSCE) [PSCE], which is developing a network for emergency communications.

3.3. V2X

The use case of V2X networking discussed in this section is for a

pedestrian protection service.

<mglt>
I do have an issue with such use case - of course if my understanding is correct. My understanding from the description is that the use case explains how pedestrian can advertise its presence to a vehicle so avoid the vehicle to hit that pedestrian. Such assumption does not seem to me acceptable as not everyone has a phone, and their security - from a vehicle perspective - MUST NOT be provided by such a mechanism as it would given a false sense of security.
If a vehicle is not able to detect a pedestrian unless this pedestrian has a working smartphone with a specific application, the problem is bigger and out of scope of the IETF.
I can also see that in some countries, it will become the pedestrian's fault if it is hit without its application.
As I understand it, I find this use case extremely dangerous, so my request would be to remove it or if I misunderstood it to clarify its scope.
<mglt>
=> [PAUL] We would like to clarify the scope for the use cases of pedestrian protection service described in the section. In the current setting, it is true that a pedestrian may have a higher risk of being hit by a vehicle if the pedestrian is not with a smartphone. We would like to limit the scope for this use case to pedestrians with a smartphone. For the case of without a smartphone, other human sensing technologies (e.g., moving object detection in images and wireless signal-based human movement detection) can be used to provide the motion information of pedestrians to vehicles. A vehicle can obtain the motion information of a pedestrian via an IP-RSU that employs a human sensing technology by V2V2I networking. We clarify this issue as follows:

Paragraph 3, Section 3.3

Old	New
For Vehicle-to-Pedestrian (V2P), a vehicle can directly communicate with a pedestrian's smartphone by V2X without IP-RSU relaying. Light-weight mobile nodes such as bicycles may also communicate directly with a vehicle for collision avoidance using V2V.	For Vehicle-to-Pedestrian (V2P), a vehicle can directly communicate with a pedestrian's smartphone by V2X without IP-RSU relaying. Light-weight mobile nodes such as bicycles may also communicate directly with a vehicle for collision avoidance using V2V. Note that it is true that a pedestrian or a cyclist may have a higher risk of being hit by a vehicle if they are

	not with a smartphone in the current setting. For this case, other human sensing technologies (e.g., moving object detection in images and wireless signal-based human movement detection [LIFS] [DFC]) can be used to provide the motion information of them to vehicles. A vehicle by V2V2I networking can obtain the motion information of a vulnerable road user via an IP-RSU that either employs or connects to a human sensing technology.

Thanks for your valuable comments.

Best Regards,
Jaehoon (Paul) Jeong