Revision Letter

Jaehoon (Paul) Jeong
Date: 3/18/2021

OLD: draft-ietf-ipwave-vehicular-networking-19
NEW: draft-ietf-ipwave-vehicular-networking-20

Dear Erik,

We have addressed all comments from your email. The detail revision is shown as follows.

[abstract, section 1]

*** "lists up" -> "enumerates|sets forth|details|...", might be a better word/verb phrase**
==> We use “enumerates” to replace “lists up” in the abstract.

[section 2]

*** "table PC"? Perhaps "tablet PC", like in section 6.**
==> The term has been revised as “tablet PC”.

[section 3]

*** There are two sentences in the final paragraph which both direct the reader to section 5 for vehicular IPv6 problem statement and requirements. Probably only one of those sentences is really required.**
==> The 2nd reference has been removed.

[section 3.2]

*** "can facilitates" -> "can facilitate"**
==> It has been corrected.

*** "can make the battery charging schedule" is technically correct, but the**

multiple possible interpretations of "make" in this context tripped me up looking for some final (indirect) object or something.

Suggest something like "can plan the battery charging schedule", perhaps?
==> The sentence has been modified by the suggested way.

*** "The existing IPv6 protocol must be augmented ..."**

Should there be some explanation about why this needs to be done at the IPv6
layer and, more explicitly, why a Layer 2 solution is not an option that can also be considered? I can understand that L2 options are out of scope for the IETF to work on, but are they also out of scope overall? I could believe that the reason is RFC 4903 -style issues, but I figured I'd ask.
==> We rephrase this sentence as follows:

*** OLD ***
The existing IPv6 protocol must be augmented through the addition of an Overlay Multilink Network (OMNI) Interface [OMNI] and/or protocol changes in order to support wireless single-hop V2V communications as well as wireless multihop V2V communications. ~~Thus, the IPv6 needs to support both single-hop and multihop communications in a wireless medium so that~~ vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard in a highway.

*** NEW ***
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 5G V2X and DSRC. Therefore, the existing IPv6 protocol can be augmented through the addition of an Overlay Multilink Network (OMNI) Interface [OMNI] and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard in a highway having multiple kinds of radio technologies, such as 5G V2X and DSRC.

[section 4.1]

*** "...vehicles under the coverage of an RSU share a prefix such that mobile nodes share a prefix..."**

Perhaps s/such that/(just as)|(in the same way that)/?

==> The sentence has been updated as "...vehicles under the coverage of an RSU share a prefix **just as** mobile nodes share a prefix...".

[section 4.2/5(.0)]

*** The final paragraph of 4.2 hints at this, but I found myself wanting to read about the expected "dwell times" for a vehicle connected to an IP-RSU. For how long is a vehicle expected to be connected to any given access node?**

I think the maximum is probably uninteresting (the vehicle could be parked, for example), but what is the useful minimum time?

==> I add the new text for your question in Section 4.2 as follows.

*** 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 vehicle passing through the coverage of an IP-RSU can upload and download data packets to/from the IP-RSU.

(I see that section 5.1.2 goes include a helpful timescale reference.)

==> I revised the text for your comments in Section 5.1.2 as follows.

*** OLD ***

For vehicular networks with high mobility and density, this DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange application messages (e.g., collision avoidance and accident notification) with each other with a short interval (e.g., 0.5 second) [NHTSA-ACAS-Report].

*** NEW ***

For vehicular networks with high mobility and density, this DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange a driving safety message (e.g., collision avoidance and accident notification) with each other with a short interval (e.g., 0.5 second) by a technical report from NHTSA

(National Highway Traffic Safety Administration) [NHTSA-ACAS-Report]. Such a driving safety message may include a vehicle's mobility information (i.e., position, speed, direction, and acceleration/deceleration). The exchange interval of this message is 0.5 second, which is required to allow a driver to avoid a rear-end crash from another vehicle.

[section 5.1.1/5.2]

*** During handover, can a vehicle be connected to multiple IP-RSUs on the logical interface? If so, does this mean they need to use RFC 8028 -style address and next hop selection?**

==> A vehicle can be connected to multiple IP-RSUs on the logical interface, which means that it can follow the first-hop router selection rule described in RFC 8028. We updated the text as follows:

5th paragraph, Section 5.2

*** OLD ***

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

*** NEW ***

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

For the case of a multihomed network, a vehicle can follow the first-hop router selection rule described in [RFC 8028]. That is, the vehicle should select its default

router for each prefix by preferring the router that advertised the prefix.

A new reference for RFC 8028 is also added.

[section 6]

*** How can a vehicle authenticate other vehicles (and their ND information) and the RAs coming from IP-RSUs?**

Ah, I guess this is what the final two paragraphs are saying, actually, that there needs to be such a mechanism.

==> Yes, the authentication mechanism for vehicles along with their ND information and RAs coming from IP-RSUs should be well considered. Based on the SEND [RFC 3971] mechanism, 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 to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based mechanism [Vehicular-BlockChain] can be used.
We update the text as follows:

9th paragraph, Section 6
*** OLD ***
For the IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. Thus, the vehicles and IP-RSUs need to filter out suspicious ND traffic in advance.

*** NEW ***
For the IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. Thus, the vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. Based on the SEND [RFC 3971] mechanism, 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 to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based mechanism [Vehicular-BlockChain] can be used.

Thanks for your valuable input and comments.

Best Regards,
Jaehoon (Paul) Jeong
--
==========
Mr. Jaehoon (Paul) Jeong, Ph.D.
Associate ProfessorDepartment Head
Department of Computer Science and Engineering
Sungkyunkwan University
Office: +82-31-299-4957
Email: pauljeong@skku.edu, jaehoon.paul@gmail.com
Personal Homepage: http://iotlab.skku.edu/people-jaehoon-jeong.php