Revision Letter for IPWAVE PS Document

Editor: Jaehoon Paul Jeong

Date: 3/9/2020

OLD: draft-ietf-ipwave-vehicular-networking-13

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

Hi Carlos,

I answer your comments and questions as follows. Your comments use a bold font and my answers use a regular font along with the prefix of [PAUL].

Hi Paul,

I've checked version -13, and it has certainly improved compared to -12. However, there are still comments that have not been completely addressed. Please find below the main ones I still have.

- Page 4 (but also later in different parts of the doc): Mobility Anchor (MA): is this term coined somewhere you can reference? It is mentioned as a component of a vehicular architecture, but it is not discussed why, not even why an IPv6 mobility solution is needed in a vehicular scenario. It might seem like straightforward, but you need to present that need. This comment still applies. The term MA is not a standard one and the need for it is not properly explained.

=> [PAUL] I clarify the definition of MA and refer to Local Mobility Anchor that has similar functionality as follows.

[NEW] Section 2. Terminology

> o Mobility Anchor (MA): A node that maintains IPv6 addresses and mobility information of vehicles in a road network to support their IPv6 address autoconfiguration and mobility management with a binding table. An MA has End-to-End (E2E) connections (e.g., tunnels) with IP-RSUs under its control for the address autoconfiguration and mobility management of the vehicles. This MA is similar to a Local Mobility Anchor (LMA) in PMIPv6 [RFC5213] for network-based mobility management.

- The use cases section still does not help much on identifying requirements. Vehicular Neighbor Discovery (VND), Vehicular Mobility Management (VMM), and Vehicular Security and Privacy (VSP) in vehicular networks appear as “new” functions, but what the use cases should reflect is the gaps of current IPv6 mechanisms that

need to be addressed. We don’t need to define new “vehicular-specific” functions, but rather to identify the extensions to existing protocols that vehicular scenarios bring.
=> [PAUL] I use the adjective “Vehicular” to represent an extension of the existing protocol such as IPv6 Neighbor Discovery, IPv6 Mobility Management (e.g., PMIPv6 and DMM), and IPv6 Security and Privacy Mechanisms rather than new “vehicular-specific” functions.
The existing IPv6 protocol does not support wireless single-hop V2V communications as well as wireless multi-hop V2V communications. Thus, the IPv6 needs to be extended for both single-hop V2V communications and multi-hop V2V communications.

[NEW] Section 3. Use Cases

Since IP is widely used among various computing devices in the Internet, it is expected that the use cases in this section need to work on top of IPv6 as the network layer protocol. Thus, the IPv6 for these use cases should be extended for vehicular IPv6 such that the IPv6 can support the functions of the network layer protocol such as Vehicular Neighbor Discovery (VND), Vehicular Mobility Management (VMM), and Vehicular Security and Privacy (VSP) in vehicular networks. Note that the adjective "Vehicular" in this document is used to represent extensions of existing protocols such as IPv6 Neighbor Discovery, IPv6 Mobility Management (e.g., PMIPv6 [RFC5213] and DMM [RFC7429]), and IPv6 Security and Privacy Mechanisms rather than new "vehicular-specific" functions. Refer to Section 5 for the problem statement of the requirements of the vehicular IPv6.

[NEW] Section 3.1. V2V

3.1. V2V

The use cases of V2V networking discussed in this section include

o Context-aware navigation for driving safety and collision avoidance;

o Cooperative adaptive cruise control in an urban roadway;

o Platooning in a highway;

o Cooperative environment sensing.

These four techniques will be important elements for self-driving vehicles.

The existing IPv6 protocol does not support wireless single-hop V2V communications as well as wireless multi-hop V2V communications. Thus, the IPv6 needs to be extended for both single-hop V2V communications and multi-hop V2V communications.

[NEW] Section 3.2. V2I

3.2. V2I

The use cases of V2I networking discussed in this section include o Navigation service;

o Energy-efficient speed recommendation service;

o Accident notification service.

The existing IPv6 protocol does not support wireless multi-hop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an RSU through the multi- hop data forwarding of intermediate vehicles. Thus, the IPv6 needs to be extended for multi-hop V2I communications.

[NEW] Section 3.3. V2X

3.3. V2X

The use case of V2X networking discussed in this section is pedestrian protection service.

The existing IPv6 protocol does not support wireless multi-hop 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 multi-hop data forwarding of intermediate vehicles (or pedestrians' smartphones). Thus, the IPv6 needs to be extended for multi-hop V2X (or V2I2X) communications.

- Section 4 should introduce a generic vision of what vehicular networks architectures might look like, again to help the purpose of identifying requirements. Current section is still making quite a lot of assumptions about how the architecture looks like without properly justifying them. The text now mentions that it is "an exemplary architecture" to support the use cases, which might be OK, but I'm afraid it might raise many questions on why we don't try to use existing known architectures and pinpointing where there are gaps.

=> [PAUL] The existing known architecture such as PMIPv6 can be extended such that it can support wireless multi-hop V2I, multi-hop V2V, and multi-hop V2I2V (or V2I2X) as follows.

[NEW] Section 4.1. Vehicular Network Architecture

4.1. Vehicular Network Architecture

Figure 1 shows an exemplary vehicular network architecture for V2I and V2V in a road network. The vehicular network architecture contains vehicles, IP-RSUs, Vehicular Cloud, Traffic Control Center, and Mobility Anchor as components. However, some components in the vehicular network architecture may not be needed for vehicular networks, such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor.

The existing, well-known architecture such as PMIPv6 [RFC5213] can be extended to a vehicular network architecture (as shown in Figure 1) such that it can support wireless multi-hop V2I, multi-hop V2V, and multi-hop V2X (or V2I2X).

- "For an IPv6 communication between an IP-OBU and an IP-RSU or between two neighboring IP-OBUs, network parameters need to be shared among them, such as MAC layer and IPv6 layer information. The MAC layer information includes wireless link layer parameters, transmission power level, the MAC address of an external network interface for the internetworking with another IP-OBU or IP-RSU. The IPv6 layer information includes the IPv6 address and network prefix of an external network interface for the internetworking with another IP-OBU or IP-RSU." --> I still don't see a clear justification on the need for exchanging prefix information... I'm not judging if this is needed or not, just saying that the draft does not really backs that need.

=> [PAUL] I revised the above paragraph to focus on the requirements of knowing the network parameters for V2I or V2V communications rather than the network parameter sharing.

[NEW] Section 4.2. V2I-based Internetworking

For the IPv6 communication between an IP-OBU and an IP-RSU or between two neighboring IP-OBUs, they need to know the network parameters, which include MAC layer and IPv6 layer information. The MAC layer information includes wireless link layer parameters, transmission power level, the MAC address of an external network interface for the internetworking with another IP-OBU or IP-RSU. The IPv6 layer information includes the IPv6 address and network prefix of an external network interface for the internetworking with another IP- OBU or IP-RSU.

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.

- There are multiple assumptions in the draft about the way IPv6 addressing will be used (e.g., multiple vehicles sharing a prefix in Figure 1, control and data separation, certain network topologies in Figure 2) that are not explained. Why those assumptions and not others? Any reference supporting them? The document kind of assumes a prefix model that is not properly introduced. Issues cannot be derived from the use of a prefix model that is not well introduced.

=> [PAUL] Multiple vehicles share a prefix such that mobile nodes share a prefix of a WiFi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks.

[NEW] Section 4.1. Vehicular Network Architecture

Multiple vehicles under the coverage of an RSU share a prefix such that mobile nodes share a prefix of a WiFi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks. For example, in Figure 1, two vehicles (i.e., Vehicle2, and Vehicle5) can use Prefix 1 to configure their IPv6 global addresses for V2I communication.

A single subnet prefix announced by an RSU can span multiple vehicles in VANET. For example, in Figure 1, for Prefix 1, three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle5) can construct a connected VANET. Also, for Prefix 2, two vehicles (i.e., Vehicle3 and Vehicle6) can construct another connected VANET, and for Prefix 3, two vehicles (i.e., Vehicle4 and Vehicle7) can construct another connected VANET.

=> [PAUL] The separation of the control plane and data plane is explained as follows.

[NEW] Section 4.1. Vehicular Network Architecture

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

=> The internal network of a vehicle is constructed by Ethernet by automotive vendors as follows.

[NEW] Section 4.2. V2I-based Internetworking

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle's internal network (i.e., moving network) and an EN's internal network (i.e., fixed network) via V2I communication. The internal network of a vehicle is nowadays constructed with Ethernet by many automotive vendors [In-Car-Network].

[NEW] Section 7. Informative References

[In-Car-Network]
Lim, H., Volker, L., and D. Herrscher, "Challenges in a Future IP/Ethernet-based In-Car Network for Real-Time Applications", ACM/EDAC/IEEE Design Automation Conference (DAC), June 2011.

- All the discussion on ND timers is again very much solution specific and should be avoided.

=> [PAUL] The discussion on ND timers is modified, focusing on a problem rather than a solution as follows.

[NEW] Section 5.1. Neighbor Discovery

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.

Thanks,

Carlos

Thanks for your valuable comments.

Best Regards,

Jaehoon (Paul) Jeong