Revision Letter for Editorial Comments for IPWAVE PS Document

Editor: Jaehoon Paul Jeong

Date: 10/3/2019

OLD: draft-ietf-ipwave-vehicular-networking-11

NEW: draft-ietf-ipwave-vehicular-networking-12

Hi Charlie and Sandra,

I answer your comments and questions as follows. Your comments use a bold font and my answers use a regular font.

Hello folks,

I made a review of the document draft-ietf-ipwave-vehicular-networking-11.txt. Besides editorial comments, I had some other more substantive comments on the document, as follows.

First, I thought that the document should contain an easily identifiable problem statement. Here is some text that I devised for that purpose, which could fit naturally at the beginning of Section 5.

=> I reflect you suggested problem statement on the text as follows.

o Section 5. Problem-Statement: The first paragraph

OLD:

This section presents key topics such as neighbor discovery, mobility management, and security & privacy.

NEW:

In order to specify protocols using the abovementioned architecture for VANETs, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively small compared to the lifetime of a link between

a vehicle and an RSU, or between two vehicles. This has a major impact on IPv6 neighbor discovery. Mobility management is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communications. Finally, and perhaps most importantly, proper authorization for vehicular protocol messages must be assured in order to prevent false reports of accidents or other mishaps on the road, which would cause horrific misery in modern urban environments. This section presents key topics such as neighbor discovery and mobility management.

Although geographic routing is mentioned early in the document, it is not discussed in later sections. This makes me wonder whether the early mention is really relevant. In fact, for fast moving objects, I think it is already questionable whether geographic routing has value. For the RSUs, it is a lot easier to imagine a good use for geographic routing, or perhaps some other use of geographic information to establish links between application endpoints. If geographic algorithms are mentioned at all, a lot more development is needed to establish relevance to the problem statement.

=> Since the geographic routing is not relevant to the IPWAVE's use cases, I remove the text related to the geographic routing as follows.

o Section 1. Introduction

OLD:

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC5944], MIPv6 [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213][RFC5844]) can be applied to vehicular networks. In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. GN protocols are useful to route an event or notification message to vehicles around a geographic position, such as an accident area in a roadway. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].

NEW:

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC5944], MIPv6 [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213][RFC5844]) can be applied to vehicular networks. ~~In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. GN protocols are useful to route an event or notification message to vehicles around a geographic position, such as an accident area in a roadway.~~

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

More description is needed for OCB in the Terminology section. It would also be a good idea to include definitions for "context-aware" and for platooning.

=> We add the description of OCB to the Terminology section as follows.

Section 2: Terminology

NEW:

OCB: "Outside the Context of a Basic Service Set". It is differentiated from the Basic Service Set (BSS) mode in IEEE 802.11 standard. A node in OCB mode can directly transmit packets to other nodes in its wireless range without the authentication or association process defined in BSS mode.

=> We add the definition of Context-Awareness.

NEW:

Context-Awareness: A vehicle can be aware of spatial-temporal mobility information (e.g., position, speed, direction, and acceleration/deceleration) of surrounding vehicles for both safety and non-safety uses through sensing or communication [CASD].

=> We add the definition of Platooning.

NEW:

Platooning: Moving vehicles can be grouped together to reduce air-resistance for energy efficiency and reduce the number of drivers such that only the leading vehicle has a driver and the other vehicles are autonomous vehicles without a driver and closely following the leading vehicle [Truck-Platooning].

---

class-based safety plan needs a definition and a list of classes.

=> We add the definition of class-based safety plain and a list of classes as follows.

NEW:

Class-Based Safety Plan: A vehicle can make safety plan by classifying the surrounding vehicles into different groups for safety purposes according to the geometrical relationship among them. The vehicle groups can be classified as Line-of-Sight Unsafe, Non-Line-of-Sight Unsafe, and Safe groups [CASD].

As a general comment, it seems to me that a proposed architecture is usually considered to be part of the solution, not the problem statement. In the case of this document, the architecture is really a depiction of IPv6 as it might be normally considered to live in a multi-network deployment (e.g., between a lot of cars and RSUs). But anyway some care has to be taken so that the proposed architecture doesn't otherwise place strong limits on acceptable solutions. So, for example, in section 4.1, it needs to be clear whether or not a single subnet prefix can span multiple vehicles. This is an important choice.

=> The vehicular architecture is described as a general one with possible components. Some components in the vehicular network architecture may not be needed such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor. As shown in Figure 1, a single subnet prefix can span multiple vehicles. In this figure, three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle5) constructs a connected Vehicular Ad Hoc Networks (VANET).

NEW: Figure 1

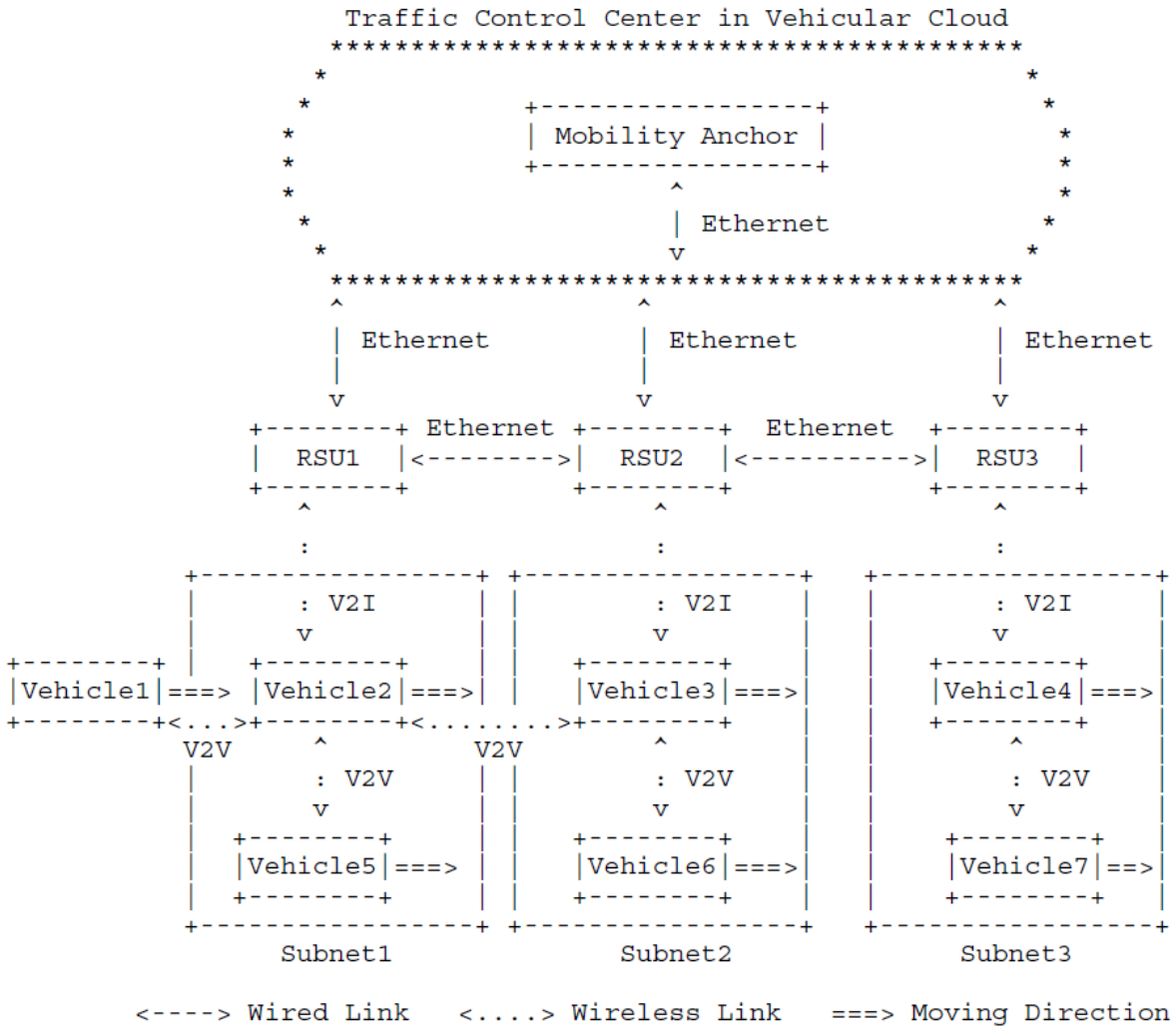

Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

OLD: Section 4.1

Figure 1 shows an architecture for V2I and V2V networking in a road network. As shown in this figure, RSUs as routers and vehicles with 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 RSUs.

NEW: Section 4.1

Figure 1 shows an architecture for V2I and V2V networking in a road network. The vehicular network architecture contains vehicles, 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 networking, such as Vehicular Cloud, Traffic Control Center, and Mobility Anchor.

As shown in this figure, RSUs as routers and vehicles with 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 RSUs.

NEW: Section 4.1

A single subnet prefix 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.

In section 5.1.1., a claim is made that a new link model is required. I think this is a very ambitious claim, and I am not even quite sure what is meant. IPv6 already provides for "on-link" and "off-link" variations on subnet operation. Unless I am missing something here, the claim should be made much more clear (or else retracted).

=> The vehicular link model for vehicular networks is clarified, considering “on-link” and “off-link” in subnet operation as follows.

Section 5.1.1. Link Model

OLD:

A VANET can have multiple links between pairs of vehicles within wireless communication range, as shown in Figure 4. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Suppose that a global-scope IPv6 prefix is assigned to VANETs in vehicular networks. 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 a one hop in the same VANET because of the multihop network connectivity. Thus, in this case, the concept of an on-link IPv6 prefix does not hold because two vehicles with the same on-link IPv6 prefix cannot communicate directly with each other. Also, when two vehicles are located in two different VANETs with the same IPv6 prefix, they cannot communicate with each other. When these two VANETs are converged to one VANET, the two vehicles can communicate with each other in a multihop fashion. Therefore, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility.

NEW:

A VANET can have multiple links between pairs of vehicles within wireless communication range, as shown in Figure 4. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Suppose that a global-scope IPv6 prefix is assigned to VANETs in vehicular networks. 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 a one hop in the same VANET because of the multihop network connectivity. Thus, in this case, the concept of an on-link IPv6 prefix does not hold because two vehicles with the same on-link IPv6 prefix cannot communicate directly with each other. Also, when two vehicles are located in two different VANETs with the same IPv6 prefix, they cannot communicate with each other. When these two VANETs converge to one VANET, the two vehicles can communicate with each other in a multihop fashion.

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 one-hop reachability among the vehicles in an appropriate way. If the vehicles with the same prefix are reachable with 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 with each other in one hop due to either the multi-hop topology in the VANET or multiple partitions, the prefix should be off-link.

Similarly, the suggestion that VANETs need to be merging and partitioning as part of the problem statement seems at least ambitious and might present a very high bar that could disqualify otherwise suitable solutions.

=> The merging and partitioning of VANETs occurs frequently in vehicular networks. This merging and partitioning should be considered for the IPv6 Neighbor Discovery (e.g., SLAAC). The requirements of the IPv6 ND are addressed for the merging and partitioning as follows.

Section 5.1 Neighbor Discovery

OLD:

The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks.

NEW:

The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks. The merging and partitioning of VANETs occurs frequently in vehicular networks. This merging and partitioning should be considered for the IPv6 Neighbor Discovery (e.g., SLAAC). Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. Also, SLAAC should be extended to prevent IPv6 address duplication due to the merging of VANETs. According to the merging and partitioning, a destination vehicle (as an IP host) should be distinguished as either an on-link host or off-link host even though the source vehicle uses the same prefix with the destination vehicle.

It would be nice to have a citation about why current implementations of address pseudonyms are insufficient for the purposes described in section 5.1.2.

=> A citation of [Scrambler-Attack], which uses the scrambler seed in the IEEE 802.11-OCB frames as fingerprint information, is added to show the insufficiency of the MAC address pseudonym for privacy.

Section 5.1.2 MAC-Address-Pseudonym

OLD:

For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used, so that the MAC address can be changed periodically. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP) session with an IPv6 address pair. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

NEW:

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

7. Informative References

NEW:

...

[Scrambler-Attack]

Bloessl, B., Sommer, C., Dressier, F., and D. Eckhoff, “The Scrambler Attack: A Robust Physical Layer Attack on Location Privacy in Vehicular Networks”, IEEE 2015 International Conference on Computing, Networking and Communications (ICNC), February 2015.

...

It seems to me that the discussion in section 5.1.3 lives almost entirely in solution space.

=> We remove Section 5.1.3 “Prefix Dissemination/Exchange” since this section discusses a solution.

Section 5.1.3 Prefix Dissemination/Exchange (Removed)

OLD:

5.1.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes within the internal networks of two vehicles (or within the internal networks of a vehicle and an RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is

required. Either a vehicle or an RSU needs an external network interface for its internal network, as shown in Figure 2 and Figure 3. The vehicular ND (VND) [ID-Vehicular-ND] can support the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) with a vehicular prefix information option. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without a vehicular ad hoc routing protocol (e.g., AODV [RFC3561] or OLSRv2 [RFC7181]).

NEW:

~~5.1.3. Prefix Dissemination/Exchange~~

~~A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes within the internal networks of two vehicles (or within the internal networks of a vehicle and an RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is required. Either a vehicle or an RSU needs an external network interface for its internal network, as shown in Figure 2 and Figure 3. The vehicular ND (VND) [ID-Vehicular-ND] can support the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) with a vehicular prefix information option. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without a vehicular ad hoc routing protocol (e.g., AODV [RFC3561] or OLSRv2 [RFC7181]).~~

In section 5.1.4, it was not clear to me about why Neighbor Discovery really needs to be extended into being a routing protocol.

=> The motivation of merging the IPv6 Neighbor Discovery and a VANET routing protocol is the efficient wireless channel utilization described as follows.

Section 5.1.4 Routing

NEW:

The merging of the IPv6 Neighbor Discovery and a VANET routing protocol allows the efficient wireless channel utilization. A routing protocol for VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in VANET with a dynamic network topology if the IPv6 ND is used to check the neighborhood of each vehicle, and can be extended to compute each vehicle's

routing table in VANET.

It seems to me that section 5.3 really belongs in section 6.

=> The contents of Section 5.3 are moved to Section 6.

NEW: Section 6

This section discusses security and privacy for IP-based vehicular networking. The security and privacy are one of key components in IP-based vehicular networking, such as neighbor discovery and mobility management, so they need to be analyzed in depth.

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe. Sybil attack, which tries to confuse a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. This sybil attack should be prevented through the cooperation between good vehicles and RSUs. Note that good vehicles are ones with valid certificates that are determined by the authentication process with an authentication server in the vehicular network. Applications on IP-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and
mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., RSU) connected to an authentication server in TCC. Also, Transport Layer Security (TLS) certificates can be used for secure E2E vehicle communications.

For secure V2I communication, a secure channel between a mobile router in a vehicle and a fixed router in an RSU should be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC

address pseudonym should be provided to the vehicle; that is, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an RSU) in terms of transport layer for a long-living higher-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IP addresses, because an adversary can see the change of the MAC and IP addresses and track the vehicle with those addresses.

For the IPv6 ND, the vehicular-network-wide DAD is required for the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that makes the DAD-related ND packets are disseminated over the VANET and vehicular network including the RSUs and the MA. The vehicles and RSUs need to filter out suspicious ND traffic in advance.

For the mobility management, a malicious vehicle can construct multiple virtual bogus vehicles, and register them with the RSU and the MA. This registration makes the RSU and MA waste their resources. The RSU and MA need to determine whether a vehicle is genuine or bogus in the mobility management.

Also, even a perfectly authorized and legitimate vehicle might be persuaded somehow to run malicious applications. I think that this point is not sufficiently covered in the current text.

=> The compromise of a perfectly authorized and legitimate vehicle is described as a security problem to be considered as follows.

Section 6. Security Considerations

OLD: Section 5.3

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

NEW: Section 6

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

Even a perfectly authorized and legitimate vehicle may be hacked to run malicious applications to track and collect other vehicles' information. For this case, an attack mitigation process may be required to reduce the aftermath of the malicious behaviors.

In addition to your comments, I revised a sentence about V2X for clear explanation in Section 3.3 as follows.

OLD: Section 3.3

For Vehicle-to-Pedestrian (V2P), a vehicle and a pedestrian's smartphone can directly communicate with each other via V2X without the relaying of an RSU as in the V2V scenario that the pedestrian's smartphone is regarded as a vehicle with a wireless media interface to be able to communicate with another vehicle. There are light-weight mobile nodes such as bicycle and motorcycle, and they can communicate directly with a vehicle for collision avoidance using V2V.

NEW: Section 3.3

For Vehicle-to-Pedestrian (V2P), a vehicle can directly communicate with a pedestrian's smartphone by V2X, without RSU relaying. There are light-weight mobile nodes such as bicycle, and they can communicate directly with a vehicle for collision avoidance using V2V.

Based on the comments from Sandra Cespedes, I revised the definition of an RSU in Section 2 so that it can accommodate multiple routers (or switches) and servers (including DNS server and edge computing server) as an edge computing system because the RSU is regularly a router or switch as follows.

OLD: Section 2. Terminology

Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in a car parking area.

NEW: Section 2. Terminology

Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-

OCB and C-V2X) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU can accommodate multiple routers (or switches) and servers (e.g., DNS server and edge computing server) in its internal network as an edge computing system. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in a car parking area.

Charlie and Sandra,

Thanks a lot for your detailed comments.

Best Regards,

Jaehoon (Paul) Jeong