IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases (draft-ietf-ipwave-vehicular-networking-11)

IETF 105, Montreal

July 23, 2019

Jaehoon (Paul) Jeong [Editor], Nabil Benamar, Sandra Cespedes, Jerome Haerri, Dapeng Liu, Tae (Tom) Oh, Charles E. Perkins, Alexandre Petrescu, Yiwen (Chris) Shen, and Michelle Wetterwald

Updates from -09 and -10 Versions

- This document (-11) is updated from
  - draft-ietf-ipwave-vehicular-networking-09
  - draft-ietf-ipwave-vehicular-networking-10

- Major Updates
  - Review of Volunteer Reviewers
    - Charlie Perkins (Done)
    - Sri Gundavelli (Done)
  - Key Work Items for IPWAVE Problem Statement
    - Neighbor Discovery (with Vehicular Link Model)
    - Mobility Management
    - Security and Privacy

Updates from -09 Version (1/2)

- **Major Updates**
  - **Reflection** of the Comments from Charlie Perkins
  - For the question on the preference on a multi-link subnet model, the revision does not suggest the multi-link subnet model as a possible solution, focusing on the characteristics and requirements for a vehicular link model.
  - The motivation about DNS in a vehicle network is addressed clearly.
  - The timing importance of ND is addressed with a reference to [NHTSA-ACAS-Report].

Updates from -09 Version (2/2)

- **Major Updates**
  - The Security Considerations are expanded with cross references to other parts of the document such as IPv6 ND and mobility management.
  - 2001:DB8::/32 is a reserved prefix for use in documentation [RFC3849]. Any routable IPv6 address needs to be routable in a VANET and a vehicular network including RSUs.
  - With an example in Figure 1, it is suggested that two separate VANETs can merge into one network.
  - A suggestion is made about how to distinguish good nodes from bad nodes with an authentication process.

Updates from -10 Version

- **Major Updates**
  - **Reflection** of the Comments from Charlie Perkins and Sri Gundavelli.
  - Many editorial comments and questions from Charlie Perkins are addressed in this document.
  - According to Sri Gundavelli's comments, the solution text and RFC 8505 reference for the vehicular ND are deleted from Section 5.1.

Next Steps

- **WG Last Call**
  - First, Request for Carlos Bernardos' Review
  - Next, Request for WGLC this August
- **IESG Submission and RFC Publication**
  - We aim at submitting it to IESG this September so that it can be published as an RFC before the IETF-106 Singapore meeting.
- **Rechartering of IPWAVE WG**
  - After the RFC approval of IESG, IPWAVE WG can start the **Rechartering for IPWAVE Basic Protocols:**
    - Vehicular Neighbor Discovery
    - Vehicular Mobility Management
    - Vehicular Security and Privacy Management.

Appendices

- Changes from -09

- Changes from -10

Changes from -09
(Revision based on Comments)

Changes from -09 (1/8)

Changes: Section 4.2. V2I-based Internetworking

-OLD: DNS services should be supported to enable name resolution for hosts or servers residing either in the vehicle's moving network or the RSU's fixed network.

Comments: The discussions about DNS need better motivation.

Reply: I put a motivation for DNS for the DNS name resolution of in-vehicle devices within a vehicle’s internal network as well as for the DNS name resolution of those devices from a remote host in the Internet for on-line diagnosis (e.g., an automotive service center server).

-NEW: A DNS service should be supported for the DNS name resolution of in-vehicle devices within a vehicle’s internal network as well as for the DNS name resolution of those devices from a remote host in the Internet for on-line diagnosis (e.g., an automotive service center server).

Changes from -09 (2/8)

Changes: Section 5.1.1. Link Model

Comments: It is not at all clear to me why a multi-link subnet model is better than simply a routing protocol between moving networks.

Reply: A multi-link subnet model is a possible approach, so I let the PS document mention the problem for a vehicular link model rather than a possible solution such as a multi-link subnet as follows.

Changes from -09 (2/8)

-NEW:

The vehicular link model needs to support the multihop routing in a connected VANET where the vehicles with the same global-scope IPv6 prefix are connected in one hop or multiple hops. It also needs to support the multhop routing in multiple connected VANETs via an RSU that has the wireless connectivity with each VANET. For example, assume that Vehicle1, Vehicle 2, and Vehicle3 are configured with their IPv6 addresses based on the same global-scope IPv6 prefix. Vehicle1 and Vehicle3 can also communicate with each other via either multi-hop V2V or multi-hop V2I2V. When two vehicles (e.g., Vehicle1 and Vehicle3 in Figure 1) are connected in a VANET, it will be more efficient for them to communicate with each other via VANET rather than RSUs. On the other hand, when two vehicles (e.g., Vehicle1 and Vehicle3) are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V. Thus, two separate VANETs can merge into one network via RSU(s). Also, newly arriving vehicles can merge two separate VANETs into one VANET if they can play a role of a relay node for those VANETs.

Changes from -09 (3/8)

Changes: Section 5.1. Neighbor Discovery

-OLD: When ND is used in vehicular networks, the communication delay (i.e., latency) between two vehicles should be bounded to a certain threshold (e.g., 500 ms) for collision-avoidance message exchange [CASD].

Comments: I had asked for a more detailed analysis about the timing requirements and latency bounds. The inclusion of numbers like 1 second, .5 second, and 500ms is not at all convincing, especially without citations. Given some knowledge of DSRC range and typical speeds for motor vehicles, you should be able to get better numbers by some basic arithmetic.

Reply: I add a reference from a report from the National Highway Traffic Safety Administration (NHTSA) that addresses the importance of 0.5-second interval. That is, an extra 0.5 seconds of warning time can prevent about 60% of rear-end collisions of vehicles moving closely in a roadway.

-NEW: According to a report from the National Highway Traffic Safety Administration (NHTSA) [NHTSA-ACAS-Report], an extra 0.5 second of warning time can prevent about 60% of the collisions of vehicles moving closely in a roadway. A warning message should be exchanged every 0.5 seconds. Thus, if the ND messages (e.g., NS and NA) are used as warning messages, they should be exchanged every 0.5 second.

Changes from -09 (4/8)

Changes: Section 5.3. Security and Privacy

Comments: The Security Considerations needs to be significantly expanded, with cross references to other parts of the document.

Reply:

Since the IPWAVE PS document focuses on three subjects such as IPv6 Neighbor Discovery (ND), mobility management, and security & privacy, I add security issues of IPv6 ND and mobility management.

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 RSU and the Mobility Anchor (MA). The vehicles and RSUs need to filter out suspicious ND traffic in advance.

For the mobility management, a malicious vehicle constructs 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.

Changes from -09 (4/8)

-NEW:

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 RSU and the MA. The vehicles and RSUs need to filter out suspicious ND traffic in advance.

For the mobility management, a malicious vehicle constructs 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.

Changes from -09 (5/8)

Changes: Section 4.1. Vehicular Network Architecture

-OLD: 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. Also, it is assumed that such 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.

Comments: I am not sure whether or not you intended to have a specific global prefix range (e.g., 2001:DB8:) set aside for VANETs. I think this would be a bad idea. Any routable IPv6 address ought to be routable in a VANET.

Reply: According to RFC 3849, 2001:DB8::/32 is a reserved prefix for use in documentation. This prefix is used for the example prefix in the PS document. As you said, any routable IPv6 address needs to be routable in a VANET and a vehicular network including RSUs.

-NEW: 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. Also, it is assumed that such 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 [RFC 3849] 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.

Changes from -09 (6/8)

Changes: Section 5.1.4. Routing

Comments: In section 5.1, you might cite draft-ietf-mboned-ieee802-mcast-problems, our draft that discusses various kinds of problems faced by multicast-based protocols over wireless media.

Reply: I cite draft-ietf-mboned-ieee802-mcast-problems in the document.

-NEW: For multihop V2V communications in a VANET (or a multi-link subnet), a vehicular ad hoc routing protocol (e.g., AODV and OLSRv2) may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead [ID-Multicast-Problems].

Changes from -09 (7/8)

Changes: Section 5.1.1. Link Model

-OLD: On the other hand, when two vehicles (e.g., Vehicle1 and Vehicle3) are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V.

Comments: In section 5.1.1, it is suggested that two separate VANETs can merge into one network. An example is needed for this.

Reply: Two separate VANETs can merge into one network through an RSU. Also, newly arriving vehicles can merge two separate VANETs into one VANET if they can play a role of a relay node for those VANETs. I clarify this mergence in the text.

-NEW: On the other hand, when two vehicles (e.g., Vehicle1 and Vehicle3) are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V. Thus, two separate VANETs can merge into one network via RSU(s). Also, newly arriving vehicles can merge two separate VANETs into one VANET if they can play a role of a relay node for those VANETs.

Changes from -09 (8/8)

Changes: Section 5.3. Security and Privacy

Comments: In section 5.3, the discussion indicates that malicious actions should be prevented by cooperation between good nodes. But no suggestion is made about how to distinguish good nodes from bad nodes, or how to reduce the likelihood that a good node might be misused by a malicious operator, or be compromised. Similarly, it is not suggested how to identify authorized vehicles.

Reply: Since this document focuses on the problems rather than possible solutions, suggestion about such solutions is left as future work of IPWAVE WG. However, I add some text as a direction of possible solutions.

-NEW: 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.

Changes from -10
(Revision based on Comments)

Changes from -10 (1/5)

Changes: Section 2. Terminology

-OLD: Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network nodes.

Comments: What does "network node" mean here?

Reply: “Network node” means “network forwarding elements (e.g., switch)”.

-NEW: Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network forwarding elements (e.g., switch and router).

Changes from -10 (2/5)

Changes: Section 3.1. V2V

-OLD: Through the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the context.

Comments: What is the context?

Reply: The context is replaced with “the other vehicles and environment”

-NEW: Through the cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment.

Changes from -10 (3/5)

Changes: Section 3.3. V2X

-OLD: 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.

Comments: The next sentence is hard to parse and should be broken up.

Reply: The next sentence is broken up for easy parsing as follows.

-NEW: For Vehicle-to-Pedestrian (V2P), a vehicle and a pedestrian's smartphone can directly communicate with each other using V2X. In this V2X communication, an RSU as a relay node is not required because the pedestrian's smartphone can communicate with another vehicle with its wireless media interface.

Changes from -10 (4/5)

Changes: Section 3.3. V2X

-OLD: In Vehicle-to-Device (V2D), a device can be a mobile node such as bicycle and motorcycle, and can communicate directly with a vehicle for collision avoidance.

Comments: a motorcycle is a vehicle, so should be V2V.

Reply: Yes, the communication between a vehicle and a light-weight mobile node (e.g., bicycle and motorcycle) can be regarded as V2V.

-NEW: There are light-weight mobile nodes such as bicycle and motorcycle, and they can communicate directly with a vehicle for collision avoidance using V2V.

Changes from -10 (5/5)

Changes: Section 5.1.1. Link Model

-OLD: For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces.

Comments: Citations needed

Reply: For a reference for the assumption of symmetry in the connectivity, RFC 6250 (Evolution of the IP Model) is cited.

-NEW: For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces [RFC6250].