Network Working Group   J. Jeong
Internet-Draft   Y. Shen
Intended status: Standards Track   Y. Jo
Expires: September 6, 2018   Sungkyunkwan University
                                                               J. Jeong
                                                    Samsung Electronics
                                                                 J. Lee
                                                 Sangmyung University
                                                          March 5, 2018

       IPv6 Neighbor Discovery for Prefix and Service Discovery in Vehicular
                                   Networks
             draft-jeong-ipwave-vehicular-neighbor-discovery-02

Abstract

   This document specifies an extension of IPv6 Neighbor Discovery (ND)
   for rapid network prefix and service discovery in vehicular networks.
   It is assumed that a vehicle or a Road-Side Unit (RSU) have an
   external network interface and their internal network. The extended
   IPv6 ND called vehicular ND can support vehicle-to-infrastructure
   communications as well as vehicle-to-vehicle communications. This
   document defines new ND options to allow a vehicle to announce the
   network prefixes and services inside its internal network to another
   vehicle or RSU.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   Vehicular Ad Hoc Networks (VANET) have been researched for the
   networking on intelligent services in road networks, such as driving
   safety, efficient driving, and entertainment. To enable this VANET
   in road networks, Dedicated Short-Range Communications (DSRC)
   [DSRC-WAVE] has been standardized as IEEE 802.11p [IEEE-802.11p],
   which is an extension of IEEE 802.11a [IEEE-802.11a], considering the
   characteristics of vehicular networks, such as high-speed mobility
   and network fragmentation. Note that IEEE 802.11p was renamed IEEE
   802.11 Outside the Context of a Basic Service Set (OCB)
   [IEEE-802.11-OCB] in 2012. For Wireless Access in Vehicular
   Environments (WAVE) [DSRC-WAVE][WAVE-1609.0], the IEEE has
   standardized IEEE 1609 family standards, such as IEEE 1609.2, 1609.3,

and 1609.4 [WAVE-1609.2][WAVE-1609.3][WAVE-1609.4]. The IEEE 1609
standards specify IPv6 as the network-layer protocol [WAVE-1609.3].

Many automobile vendors are replacing Controller Area Networks (CANs)
with Ethernet for high-speed interconnectivity among Electronic
Control Units (ECUs) in a vehicle. The sensing information of the
ECUs can be delivered to the service centers of those automobile
ventors for remote diagnosis for driving safety using DSRC between
vehicles and Road-Side Units (RSUs) having the Internet connectivity
toward the service centers in a vehicular cloud.

With this trend, it is time to enable vehicular networking with IPv6
to let various Internet-based applications (e.g., remote vehicle
diagnosis) run on top of transport-layer protocols, such as TCP, UDP,
and SCTP. IPv6 [RFC2460] is suitable for a network layer in
vehicular networks in that the protocol has abundant address space,
autoconfiguration features, and protocol extension ability through
extension headers.

To support the interaction between vehicles or between a vehicle and
an RSU, this document specifies an extension of IPv6 ND [RFC4861] for
rapid network prefix and service discovery in vehicular networks with
new ND options. That is, the extended IPv6 ND in this document,
which is called vehicular ND, can support not only vehicle-to-
infrastructure (V2I) communications but also vehicle-to-vehicle (V2V)
communications.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in RFC 2119 [RFC2119].

3. Terminology

This document uses the terminology described in [RFC4861] and
[RFC4862]. In addition, four new terms are defined below:

o Road-Side Unit (RSU): A node that has a Dedicated Short-Range
   Communications (DSRC) device for wireless communications with the
   vehicles and is connected to the Internet. Every RSU is usually
   deployed at an intersection so that it can provide vehicles with
   the Internet connectivity.

o Vehicle: A node that has the DSRC device for wireless
   communications with vehicles and RSUs. Every vehicle may also
   have a GPS-navigation system for efficient driving.

   o Traffic Control Center (TCC): A node that maintains road
      infrastructure information (e.g., RSUs and traffic signals),
      vehicular traffic statistics (e.g., average vehicle speed and
      vehicle inter-arrival time per road segment), and vehicle
      information (e.g., a vehicle's identifier, position, direction,
      speed, and trajectory). TCC is included in a vehicular cloud for
      vehicular networks.

4. Overview

   This document specifies an IPv6 ND extension for vehicle-to-vehicle
   (V2V) or vehicle-to-infrastructure (V2I) networking.

   Figure 1 shows the V2V networking of two vehicles whose internal
   networks are Moving Network1 and Moving Network2, respectively.
   Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and
   Host2), and the two routers (Router1 and Router2). Vehicle2 has the
   DNS Server (RDNSS2), the two hosts (Host3 and Host4), and the two
   routers (Router3 and Router4).

   It is assumed that Host1 and Host3 are running a Cooperative Adaptive
   Cruise Control (C-ACC) program for physical collision avoidance.
   Also, it is assumed that Host2 and Host4 are running a Cooperative
   On-board Camera Sharing (C-OCS) program for sharing road hazards or
   obstacles to avoid road accidents. Vehicle1's Router1 and Vehicle2's
   Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for
   V2V networking for various vehicular services. The vehicular
   applications, such as C-ACC and C-BCS, can be registered into the DNS
   Server (i.e., RDNSS) through DNSNA protocol in [ID-DNSNA] along with
   IPv6 ND DNS options in [RFC6106].

   Vehicle1's Router1 and Vehicle2's Router3 can know what vehicular
   applications exist in their internal network by referring to their
   own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know
   what network prefixes exist in their internal network through an
   intra-domain routing protocoli, such as OSFP. Each vehicle announces
   its network prefixes and services through ND options defined in
   Section 5.

```
                        (*)<..........>(*)
                         |             | 2001:DB8:1:1::/64
    .-----------------------------.  .-----------------------------.
    |                  |          |  |         |                   |
    | .-------. .-------. .-------. |  | .-------. .-------. .-------. |
    | | Host1 | |RDNSS1| |Router1| |  | |Router3| |RDNSS2| | Host3 | |
    | .-------. .-------. .-------. |  | .-------. .-------. .-------. |
    |     ^        ^        ^      |  |     ^        ^        ^      |
    |     |        |        |      |  |     |        |        |      |
    |     v        v        v      |  |     v        v        v      |
    | --------------------------- |  | --------------------------- |
    | 2001:DB8:10:1::/64 ^        |  |    ^ 2001:DB8:20:1::/64     |
    |                    |        |  |    |                        |
    |                    v        |  |    v                        |
    | .-------.      .-------.    |  | .-------.      .-------.    |
    | | Host2 |      |Router2|    |  | |Router4|      | Host4 |    |
    | .-------.      .-------.    |  | .-------.      .-------.    |
    |     ^              ^        |  |     ^              ^        |
    |     |              |        |  |     |              |        |
    |     v              v        |  |     v              v        |
    | --------------------------- |  | --------------------------- |
    |  2001:DB8:10:2::/64        |  |     2001:DB8:20:2::/64      |
    ._____.  ._____.
       Vehicle1 (Moving Network1)     Vehicle2 (Moving Network2)

       <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 1: Internetworking between Vehicle Networks

Figure 2 shows the V2I networking of a vehicle and an RSU whose
internal networks are Moving Network1 and Fixed Network1,
respectively. Vehicle1 has the DNS Server (RDNSS1), the two hosts
(Host1 and Host2), and the two routers (Router1 and Router2). RSU1
has the DNS Server (RDNSS2), one host (Host3), the two routers
(Router3 and Router4).

It is assumed that RSU1 has a collection of servers (Server1 to
ServerN) for various services in the road networks, such as road
emergency notification and navigation services. Vehicle1's Router1
and RSU1's Router3 use 2001:DB8:1:1::/64 for an external link (e.g.,
DSRC) for I2V networking for various vehicular services. The
vehicular applications, such as road emergency notification and
navigation services, can be registered into the DNS Server (i.e.,
RDNSS) through DNSNA protocol in [ID-DNSNA] along with IPv6 ND DNS
options in [RFC6106].

Vehicle1's Router1 and RSU1's Router3 can know what vehicular
applications exist in their internal network by referring to their

own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know
what network prefixes exist in their internal network through an
intra-domain routing protocoli, such as OSFP. Each vehicle and each
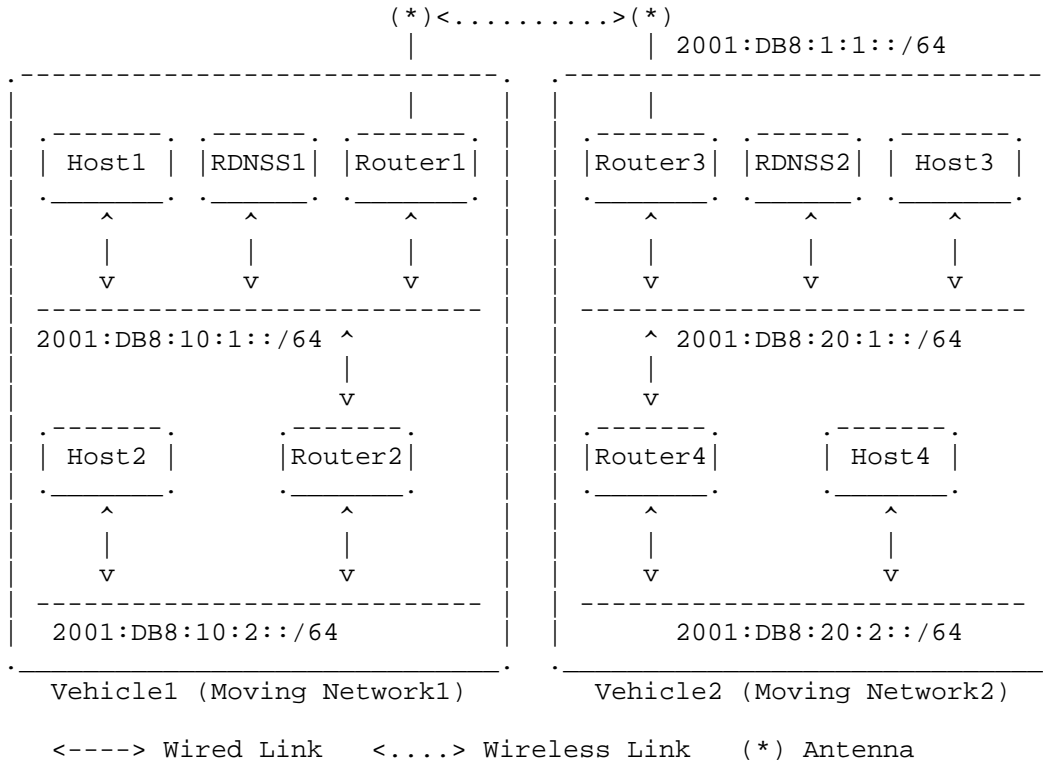RSU announce their network prefixes and services through ND options
defined in Section 5.

```
                      (*)<...........>(*)
                       |               | 2001:DB8:1:1::/64
  .---------------------------.   .---------------------------------.
  |            |              |   | |       |                       |
  | .-------. .------. .-------. | | .-------. .------. .-------.    |
  | | Host1 | |RDNSS1| |Router1| | | |Router3| |RDNSS2| | Host3 |   |
  | ._____. ._____. ._____. | | ._____. ._____. ._____.     |
  |    ^        ^        ^      |   |    ^        ^        ^         |
  |    |        |        |      |   |    |        |        |         |
  |    v        v        v      |   |    v        v        v         |
  | -------------------------   |   | ------------------------------ |
  | 2001:DB8:10:1::/64 ^        |   |  ^ 2001:DB8:20:1::/64          |
  |                    |        |   |  |                            |
  |                    v        |   |  v                            |
  | .-------.     .-------.     |   | .-------. .-------.  .-------. |
  | | Host2 |     |Router2|     |   | |Router4| |Server1|...|ServerN| |
  | ._____.     ._____.      |   | ._____. ._____.  ._____.   |
  |    ^            ^           |   |    ^        ^          ^       |
  |    |            |           |   |    |        |          |       |
  |    v            v           |   |    v        v          v       |
  | -------------------------   |   | ------------------------------ |
  |  2001:DB8:10:2::/64         |   |     2001:DB8:20:2::/64         |
  ._____.   ._____.
     Vehicle1 (Moving Network1)        RSU1 (Fixed Network1)

     <----> Wired Link   <....> Wireless Link   (*) Antenna
```
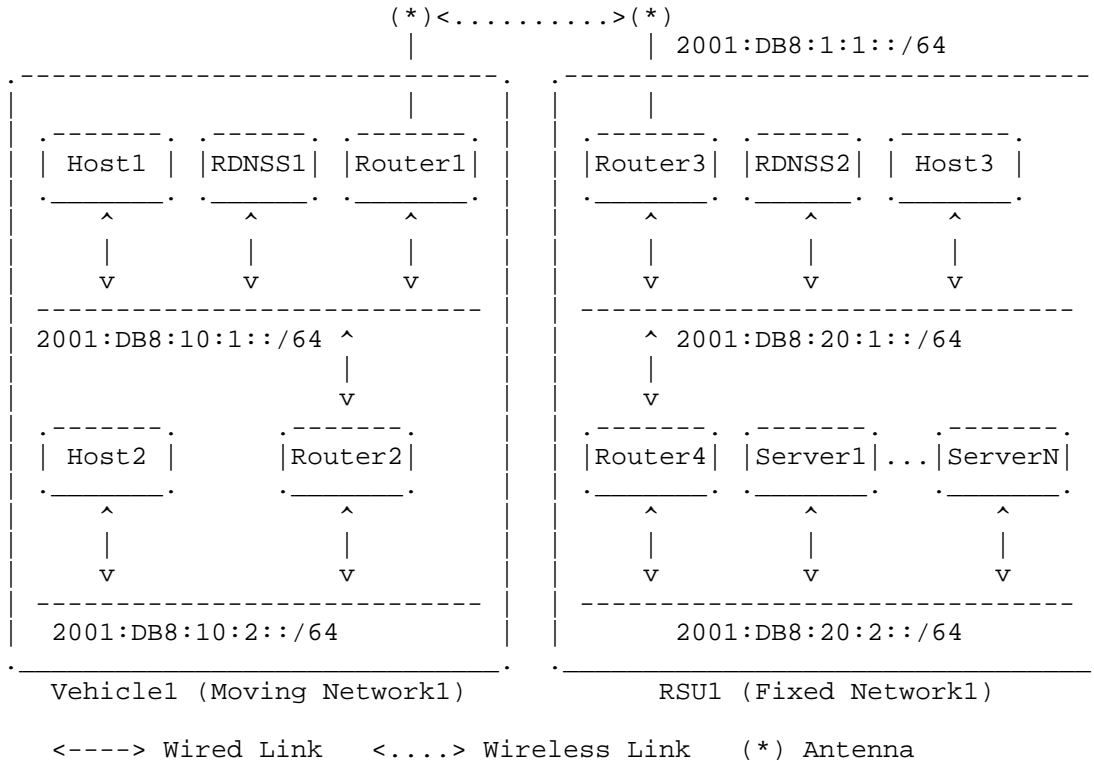
       Figure 2: Internetworking between Vehicle Network and RSU Network

5. ND Extension for Prefix and Service Discovery

   This section defines two new ND options for prefix and service
   discovery: (i) the Vehicular Prefix Information (VPI) option and (ii)
   the Vehicular Service Information (VSI) option. It also describes
   the ND protocol for such prefix and service discovery.

5.1. Vehicular Prefix Information Option

   The VPI option contains one IPv6 prefix in the internal network.
   Figure 3 shows the format of the VPI option.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |     Length    | Prefix Length |   Distance    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Reserved                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                            Prefix                             :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

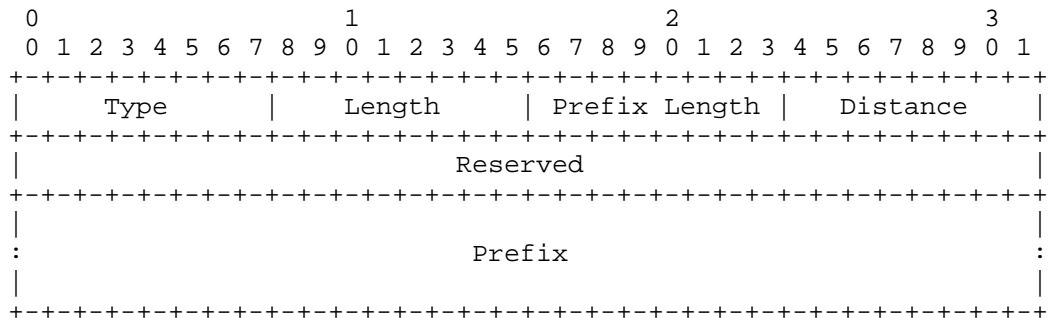   Figure 3: Vehicular Prefix Information (VPI) Option Format

   Fields:
   Type   8-bit identifier of the VPI option type as assigned
                 by the IANA: TBD

   Length   8-bit unsigned integer. The length of the option
                 (including the Type and Length fields) is in units of
                 8 octets. The value is 3.

   Prefix Length 8-bit unsigned integer. The number of leading bits
                 in the Prefix that are valid. The value ranges
                 from 0 to 128.

   Distance   8-bit unsigned integer. The distance between the
                 subnet announcing this prefix and the subnet
                 corresponding to this prefix in terms of the number
                 of hops.

   Reserved   This field is unused. It MUST be initialized to
                 zero by the sender and MUST be ignored by the
                 receiver.

   Prefix   An IP address or a prefix of an IP address. The
                 Prefix Length field contains the number of valid
                 leading bits in the prefix. The bits in the prefix
                 after the prefix length are reserved and MUST be
                 initialized to zero by the sender and ignored by
                 the receiver.

5.2. Vehicular Service Information Option

   The VSI option contains one vehicular service in the internal
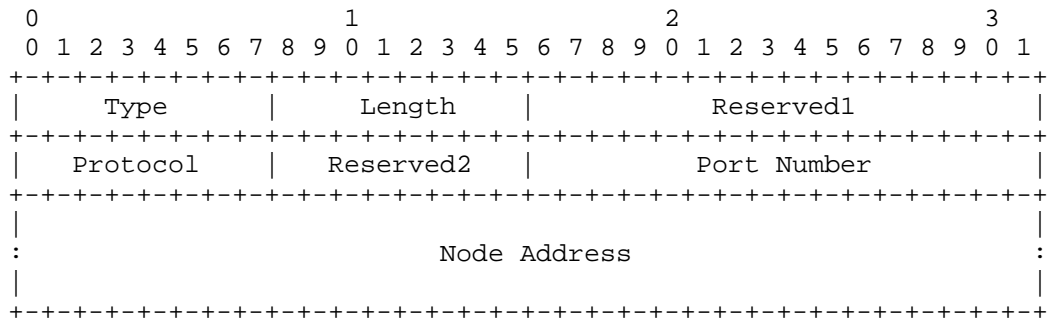   network. Figure 4 shows the format of the VSI option.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |     Length    |            Reserved1          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Protocol   |    Reserved2  |          Port Number          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
:                        Node Address                           :
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

        Figure 4: Vehicular Service Information (VSI) Option Format

   Fields:
    Type   8-bit identifier of the VSI option type as assigned
                  by the IANA: TBD

    Length   8-bit unsigned integer. The length of the option
                  (including the Type and Length fields) is in units of
                  8 octets. The value is 3.

    Reserved1   This field is unused. It MUST be initialized to
                  zero by the sender and MUST be ignored by the
                  receiver.

    Protocol   8-bit unsigned integer to indicate the upper-layer
                  protocol, such as transport-layer protocol (e.g.,
                  TCP, UDP, and SCTP).

    Reserved2   This field is unused. It MUST be initialized to
                  zero by the sender and MUST be ignored by the
                  receiver.

    Port Number   16-bit unsigned integer to indicate the port number
                  for the protocol.

    Service Address
                  128-bit IPv6 address of a node proving this vehicular
                  service.

5.3. Vehicular Neighbor Discovery

   With VPI and VSI options, a node (e.g., vehicle or RSU) can announce
   the network prefixes and services in its internal network via ND
   messages, such as Neighbor Solicitation (NS) and Neighbor
   Advertisement (NA) [RFC4861].

A node periodically announces an NS message containing the VPI and
VSI options with its prefixes and services in all-nodes multicast
address to reach all neighboring nodes. When another neighboring
node receives this NS message, it responds to this NS message by
sending an NA message containing the VPI and VSI options with its
prefixes and services via unicast toward the NS-originating node.

Through this procedure, vehicles and RSUs can rapidly discover the
network prefixes and services of the other party without any
additional service discovery protocol.

6. Security Considerations

This document shares all the security issues of the neighbor
discovery protocol. This document can get benefits from secure
neighbor discovery (SEND) [RFC3971] in order to protect ND from
possible security attacks.

7. Acknowledgments

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
           Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6
           (IPv6) Specification", RFC 2460, December 1998.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
           "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861,
           September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
           Address Autoconfiguration", RFC 4862, September 2007.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli,
           "IPv6 Router Advertisement Options for DNS Configuration",
           RFC 6106, November 2010.

8.2. Informative References

   [DSRC-WAVE]
             Morgan, Y., "Notes on DSRC & WAVE Standards Suite: Its
             Architecture, Design, and Characteristics",
             IEEE Communications Surveys & Tutorials, 12(4), 2012.

   [ID-DNSNA]
             Jeong, J., Ed., Lee, S., and J. Park, "DNS Name
             Autoconfiguration for Internet of Things Devices", draft-
             jeong-ipwave-iot-dns-autoconf-02 (work in progress), March
             2018.

   [IEEE-802.11-OCB]
             IEEE 802.11 Working Group, "Part 11: Wireless LAN Medium
             Access Control (MAC) and Physical Layer (PHY)
             Specifications", IEEE Std 802.11-2012, February 2012.

   [IEEE-802.11a]
             IEEE Std 802.11a, "Part 11: Wireless LAN Medium Access
             Control (MAC) and Physical Layer (PHY) specifications:
             High-speed Physical Layer in the 5 GHZ Band", September
             1999.

   [IEEE-802.11p]
             IEEE Std 802.11p, "Part 11: Wireless LAN Medium Access
             Control (MAC) and Physical Layer (PHY) Specifications
             Amendment 6: Wireless Access in Vehicular Environments",
             June 2010.

   [RFC3971] Arkko, J., Ed., "SEcure Neighbor Discovery (SEND)",
             RFC 3971, March 2005.

   [WAVE-1609.0]
             IEEE 1609 Working Group, "IEEE Guide for Wireless Access
             in Vehicular Environments (WAVE) - Architecture", IEEE Std
             1609.0-2013, March 2014.

   [WAVE-1609.2]
             IEEE 1609 Working Group, "IEEE Standard for Wireless
             Access in Vehicular Environments - Security Services for
             Applications and Management Messages", IEEE Std
             1609.2-2016, March 2016.

   [WAVE-1609.3]
             IEEE 1609 Working Group, "IEEE Standard for Wireless
             Access in Vehicular Environments (WAVE) - Networking
             Services", IEEE Std 1609.3-2016, April 2016.

   [WAVE-1609.4]
              IEEE 1609 Working Group, "IEEE Standard for Wireless
              Access in Vehicular Environments (WAVE) - Multi-Channel
              Operation", IEEE Std 1609.4-2016, March 2016.

Appendix A.   Changes from draft-jeong-ipwave-vehicular-neighbor-
              discovery-01

   The following changes are made from draft-jeong-ipwave-vehicular-
   neighbor-discovery-01:

   o In Section 1, the following sentence is added: Note that IEEE
      802.11p was renamed IEEE 802.11 Outside the Context of a Basic
      Service Set (OCB) [IEEE-802.11-OCB] in 2012.

   o In Section 1, references for WAVE are added as follows: For
      Wireless Access in Vehicular Environments (WAVE) [DSRC-WAVE]
      [WAVE-1609.0], the IEEE has standardized IEEE 1609 family
      standards, such as IEEE 1609.2, 1609.3, and 1609.4
      [WAVE-1609.2][WAVE-1609.3][WAVE-1609.4]. The IEEE 1609 standards
      specify IPv6 as the network-layer protocol [WAVE-1609.3].

Authors' Addresses

   Jaehoon Paul Jeong
   Department of Software
   Sungkyunkwan University
   2066 Seobu-Ro, Jangan-Gu
   Suwon, Gyeonggi-Do 16419
   Republic of Korea

   Phone: +82 31 299 4957
   Fax: +82 31 290 7996
   EMail: pauljeong@skku.edu
   URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

   Yiwen Chris Shen
   Department of Computer Science and Engineering
   Sungkyunkwan University
   2066 Seobu-Ro, Jangan-Gu
   Suwon, Gyeonggi-Do 16419
   Republic of Korea

   Phone: +82 31 299 4106
   Fax: +82 31 290 7996
   EMail: chrisshen@skku.edu

Younghwa Jo
Department of Software Platform
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: movie_jo@naver.com

Junsik Jeong
Software R&D Center
Samsung Electronics
Seoul R&D Campus D-Tower, 56, Seongchon-Gil, Seocho-Gu
Seoul 06765
Republic of Korea

EMail: jun.jeong@samsung.com

Jong-Hyouk Lee
Sangmyung University
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan, NY 31066
Republic of Korea

EMail: jonghyouk@smu.ac.kr