Workgroup: IPWAVE Working Group
Internet-Draft:
draft-jeong-ipwave-vehicular-neighbor-discovery-13
Published: 21 February 2022
Intended Status: Standards Track
Expires: 25 August 2022
Authors: J. Jeong, Ed. — Sungkyunkwan University
Y. Shen — Sungkyunkwan University
Z. Xiang — Sungkyunkwan University
S. Cespedes — NIC Chile Research Labs

Vehicular Neighbor Discovery for IP-Based Vehicular Networks

Abstract

This document specifies a Vehicular Neighbor Discovery (VND) as an extension of IPv6 Neighbor Discovery (ND) for IP-based vehicular networks. An optimized Address Registration and a multihop Duplicate Address Detection (DAD) mechanism are performed for having operation efficiency and also saving both wireless bandwidth and vehicle energy. In addition, three new ND options for prefix discovery, service discovery, and mobility information report are defined to announce the network prefixes and services inside a vehicle (i.e., a vehicle's internal network).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Vehicular Ad Hoc Networks (VANET) have been researched for Intelligent Transportation System (ITS) such as driving safety, efficient driving and entertainment. Considering the high-speed mobility of vehicular network based on Dedicated Short-Range Communications (DSRC) [DSRC-WAVE], IEEE has standardized IEEE 802.11p [IEEE-802.11p] as a MAC protocol for vehicles in Wireless

Access in Vehicular Environments (WAVE). IEEE 802.11p was renamed IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB]. In addition, IEEE has also standardized a family standard suite of WAVE as IEEE 1609. This IEEE 1609 standard suite is considered as a key component for ITS. IEEE 1609 standards include IEEE 1609.0 [WAVE-1609.0], 1609.2 [WAVE-1609.2], 1609.3 [WAVE-1609.3], and 1609.4 [WAVE-1609.4], which provide a low-latency and alternative network for vehicular communications. What is more, IP-based vehicular networks specialized as IP Wireless Access in Vehicular Environments (IPWAVE) [I-D.ietf-ipwave-vehicular-networking] can enable many use cases over vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. IETF has standardized an IPv6 packet delivery protocol over IEEE 802.11-OCB [RFC8691].

VANET features high mobility dynamics, asymmetric and lossy connections, and moderate power constraint (e.g., electric cars and unmanned aerial vehicles). Links among hosts and routers in VANET can be considered as undetermined connectivities with constantly changing neighbors described in [RFC5889]. IPv6 [RFC8200] is selected as the network-layer protocol for Internet applications by IEEE 1609.0 and 1609.3. However, the relative long-time Neighbor Discovery (ND) process in IPv6 [RFC4861] is not suitable in VANET scenarios.

To better support the interaction between vehicles or between vehicles and Rode-Side Units (RSUs), this document specifies a Vehicular Neighbor Discovery (VND) procedure as an extension of IPv6 ND for IP-based vehicular networks. VND provides vehicles with an optimized Address Registration and a multihop Duplicate Address Detection (DAD) mechanism. In addition, an efficient mobility management scheme is specified to support efficient V2V, V2I, and V2X communications. Detailed statements of the mobility management are addressed in [I-D.jeong-ipwave-vehicular-mobility-management] .

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], [RFC4862], [RFC6775], and [RFC8691]. In addition, the following new terms are defined as below:

* WAVE: Acronym for "Wireless Access in Vehicular Environments" [WAVE-1609.0].

* Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support the address autoconfiguration and mobility management of them. It has end-to-end connections with RSUs under its control. It maintains a DAD Table recording the IP addresses of vehicles moving within the communication coverage of its RSUs.

* Vehicular Cloud: A cloud infrastructure for vehicular networks, including compute nodes, storage nodes, and network nodes.

* Traffic Control Center (TCC): A node that maintains road infrastructure information (e.g., RSUs, traffic signals, and loop detectors), 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 as a navigation path). TCC is included in a vehicular cloud for vehicular networks and has MAs under its management.

4. Overview

This document proposes an optimized ND with a more adaptive structure for vehicular networks compared to [RFC4861] by considering dynamic vehicle mobility and overhead of control message traffic in wireless environments. Furthermore, prefix and service discovery can be implemented as part of the ND's process along with an efficient Address Registration procedure and a DAD mechanism for moving vehicles. This document specifies a set of behaviors between vehicles and RSUs to accomplish these goals.

4.1. Link Model

There is a relationship between a link and a network prefix along with reachability scopes, such as link-local and global scopes. The legacy IPv6 ND protocol [RFC4861] has the following link model. All IPv6 nodes in the same on-link subnet, which use the same subnet prefix with the on-link bit set, are reachable with each other by one-hop links. The symmetry of the connectivity among the nodes is assumed, that is, bidirectional connectivity between two on-link nodes. However, a link model in vehicular networks (called vehicular link model) should consider the asymmetry of the connectivity that unidirectional links can exist due to interference in wireless channels and the different levels of transmission power employed by wireless network interfaces.

The on-link subnet can be constructed by one link (as a basic service set) or multiple links (as an extended service set) called a multi-link subnet [RFC6775]. In this multi-link subnet, an all-node-multicasted packet is copied and related to other links by an ND proxy. On the other hand, in vehicular networks having fast moving vehicles, multiple links can share the same subnet prefix for operation efficiency. For example, if two wireless links under two adjacent RSUs are in the same subnet, a vehicle as an IPv6 host does not need to reconfigure its IPv6 address during handover between those RSUs. However, the packet relay by an RSU as an ND proxy is not required because such a relay can cause a broadcast storm in the extended subnet. Thus, in the multi-link subnet, all-node-multicasting needs to be well-calibrated to either being confined to multicasting in the current link or being disseminated to other links in the same subnet.

In a connected multihop VANET, for efficient communication, vehicles in the same link of an RSU can communicate directly with each other, not through the serving RSU. This direct wireless communication is similar to the direct wired communication in an on-link subnet using Ethernet as a wired network. The vehicular link model needs to accommodate both the ad-hoc communication between vehicles and infrastructure communication between a vehicle and an RSU in an efficient and flexible way. Therefore, the IPv6 ND should be extended to accommodate the concept of a new IPv6 link model in vehicular networks.

To support multi-link subnet, this specification employs the Shared-Prefix model for prefix assignments. A Shared-Prefix model refers to an addressing model where the prefix(es) are shared by more than one node. In this document, we assume that in a specified subnet, all interfaces of RSUs responding for prefix assignments to vehicles hold the same prefix, which ensure vehicles obtain and maintain the same prefix in this subnet scope.

4.2. ND Optimization

This document takes advantage of the optimized ND for Low-Power Wireless Personal Area Network (6LoWPAN) [RFC6775] because vehicular environments have common parts with 6LoWPAN, such as the reduction of unnecessary wireless traffic by multicasting and the energy saving in battery. Note that vehicles tend to be electric vehicles whose energy source is from their battery.

In the optimized IPv6 ND for 6LoWPAN, the connections among nodes are assumed to be asymmetric and unidirectional because of changing radio environment and loss signal. The authors proposed an optimized IPv6 ND which greatly eliminates link-scope multicast to save energy by constructing new options and a new scheme for address configurations. Similarly, this document proposes an improved IPv6 ND by eliminating many link-scope-multicast-based ND operations, such as DAD for IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. Thus, this document suggests an extension of IPv6 ND as vehicular ND tailored for vehicular networks along with new ND options (e.g., prefix discovery, service discovery, and mobility information options).

4.3. Design Goals

The vehicular ND in this document has the following design goals:

* To perform prefix and service discovery through ND procedure;

* To implement host-initiated refresh of Router Advertisement (RA) and remove the necessity for routers to use periodic or unsolicited multicast RA to find hosts;

* To replace Neighbor Unreachable Detection(NUD) and create Neighbor Cache Entries (NCE) for all registered vehicles in RSUs and MA by appending Address Registration Option (ARO) in Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages;

* To support a multihop DAD by conveying ND messages received from vehicles to MA to eliminate multicast storms and save energy; and

* To support multihop communication for vehicles outside the coverage of RSUs to communicate with the serving RSU via a relay neighbor.

5. Vehicular Network Architecture

A vehicular network architecture for V2I and V2V is illustrated in Figure 1. Three RSUs are deployed along roadsides and are connected to an MA through wired links. There are two subnets such as Subnet1 and Subnet2. The wireless links of RSU1 and RSU2 belong to the same subnet named Subnet1, but the wireless link of RSU3 belongs to another subnet named Subnet2. Vehicle2 is wirelessly connected to RSU1 while Vehicle3 and Vehicle4 are connected to RSU2 and RSU3, respectively. Vehicles can directly communicate with each other through V2V connection (e.g., Vehicle1 and Vehicle2) to share driving information. In addition, vehicles not in the range of any RSU may connect with RSU in multihop connection via relay vehicle (e.g., Vehicle1 can contact RSU1 via Vehicle2). Vehicles are assumed to start the connection to an RSU when they entered the coverage of the RSU.

This document recommends a multi-link subnet involving multiple RSUs as shown in Figure 1. This recommendation aims at the reduction of the frequency with which vehicles have to change their IP address during handover between two adjacent RSUs. To construct this multi-link subnet, a Shared-Prefix model is proposed. That is, for RSUs in the same subnet, the interfaces responsible for prefix assignment for vehicles should hold the same prefix in their global address.

This also promises vehicles achieve the same prefix in this scope. When they pass through RSUs in the same subnet, vehicles do not need to perform the Address Registration and DAD again because they can use their current IP address in the wireless coverage of the next RSU. Moreover, this proposal accords with the assumption that nodes belonging to the same IP prefix domain are able to communicate with each other directly without the intervention of RSUs if they are within the wireless communication range of each other. On the other hand, if vehicles enter the wireless coverage of an RSU belonging to another subnet with a different prefix, they repeat the Address Registration and DAD procedure to update their IP address with the new prefix.

In Figure 1, RSU1 and RSU2 are deployed in a multi-link subnet with the same prefix address in their interfaces responding for connection with vehicles. When vehicle2 leaves the coverage of RSU1 and enters RSU2, it maintains its address configuration and ignores Address Registration and DAD steps. If vehicle2 moves into the coverage of RSU3, since RSU3 belongs to another subnet and holds a different prefix from RSU1 and RSU2, so vehicle2 must do Address Registration and DAD just as connecting to a new RSU. Note that vehicles and RSUs have their internal networks including in-vehicle devices and servers, respectively. The structures of the internal networks are described in [I-D.ietf-ipwave-vehicular-networking].

```
                     Traffic Control Center in Vehicular Cloud
                    *-----------------------------------------*
                   *                                           *
                  *             +----------------+              *
                 *              | Mobility Anchor|               *
                 *              +----------------+               *
                  *                    ^                        *
                   *                   |                       *
                    *------------------v----------------------*
                    ^                  ^                     ^
                    |                  |                     |
                    |                  |                     |
                    v                  v                     v
               +--------+ Ethernet +--------+            +--------+
               |  RSU1  |<-------->|  RSU2  |<---------->|  RSU3  |
               +--------+          +--------+            +--------+
                  ^                     ^                    ^
                  :                     :                    :
           +-------------------------------------+   +-----------------+
           |      : V2I             V2I :        |   |   V2I :         |
           |      v                     v        |   |       v         |
+--------+ |   +--------+          +--------+    |   |   +--------+    |
|Vehicle1|===> |Vehicle2|===>      |Vehicle3|===>|   |   |Vehicle4|===>|
|        |<...>|        |<........>|        |    |   |   |        |    |
+--------+ V2V +--------+    V2V   +--------+    |   |   +--------+    |
           |                                     |   |                 |
           +-------------------------------------+   +-----------------+
                           Subnet1                         Subnet2

        <----> Wired Link   <....> Wireless Link   ===> Moving Direction
```

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

6. ND Extension for Prefix and Service Discovery

This section specifies an IPv6 ND extension for vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) networking. This section also defines three new ND options for prefix discovery, service discovery, and mobility information report: (i) Vehicular Prefix Information (VPI) option, (ii) Vehicular Service Information (VSI) option, and (iii) Vehicular Mobility Information (VMI) option. It also describes the procedure of the ND protocol with those options.

6.1. Vehicular Prefix Information Option

The VPI option contains IPv6 prefix information in the internal network. Figure 2 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 2: 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.

6.2. Vehicular Service Information Option

The VSI option contains vehicular service information in the internal network. Figure 3 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 3: 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 this protocol.

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

6.3. Vehicular Mobility Information Option

The VMI option contains one vehicular mobility information of a vehicle or an RSU. Figure 4 shows the format of the VMI 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           |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                            Reserved2                          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 :                       Mobility Information                    :
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: Vehicular Mobility Information (VMI) Option Format

Fields:

Type: 8-bit identifier of the VMI 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.

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

Mobility Information: 128-bit mobility information, such as position, speed, acceleration/deceleration, and direction.

6.4. Vehicular Neighbor Discovery

Prefix discovery enables hosts (e.g., vehicles and in-vehicle devices) to distinguish destinations on the same link from those only reachable via RSUs. A vehicle (or its in-vehicle devices) can directly communicate with on-link vehicles (or their in-vehicle devices) without the relay of an RSU, but through V2V communications along with VPI ND option. This VPI option contains IPv6 prefixes in a vehicle's internal network.

Vehicles announce services in their internal networks to other vehicles through an VSI ND option. The VSI option contains a list of vehicular services in a vehicle's or an RSU's internal network.

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

Therefore, prefix and service discovery can be achieved via ND messages (e.g., NS and NA) by vehicular ND with VPI and VSI options. This VND-based discovery eliminates an additional prefix and service discovery scheme, such as DNS-based Service Discovery [RFC6763] (e.g., Multicast DNS (mDNS) [RFC6762] and DNSNA [I-D.jeong-ipwave-iot-dns-autoconf]), other than ND. That is, vehicles and RSUs can rapidly discover the network prefixes and services of the other party without any additional service discovery protocol.

6.5. Message Exchange Procedure for V2I Networking

This subsection explains a message exchange procedure for VND in V2I networking, where a vehicle communicates with its corresponding node in the Internet via an RSU.

Figure 5 shows an example of message exchange procedure in V2I networking. Detailed steps of the procedure are explained in Section 7. The mobility management part is described in [I-D.jeong-ipwave-vehicular-mobility-management].

Note that a vehicle could also perform the prefix and service discovery simultaneously along with Address Registration procedure, as shown in Figure 7.

This document specified that RSUs as routers do not transmit periodical and unsolicited multicast RA messages including a prefix for energy saving in vehicular networks. Vehicles as hosts periodically initiate an RS message according to a time interval (considering its position and an RSU's coverage). Since they have a digital road map with the information of RSUs (e.g., position and communication coverage), vehicles can know when they will go out of the communication range of an RSU along with the signal strength (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]) from the RSU. RSUs replies with a solicited RA in unicast only when they receive an RS message.

```
          Vehicle                    RSU                     MA
             |                        |                        |
             |-RS with Mobility Info->|                        |
             |         [VMI]          |                        |
             |                        |                        |
             |                        |-----------PBU--------->|
             |                        |                        |
             |                        |                        |
             |                        |<----------PBA----------|
             |                        |                        |
             |                        |                        |
             |                        |======Bi-Dir Tunnel=====|
             |                        |                        |
             |                        |                        |
             |<----RA with prefix-----|                        |
             |                        |                        |
             |                        |                        |
             |                        |                        |
             |--NS with Address Reg-->|                        |
             |     [ARO+VPI+VSI]      |                        |
             |                        |                        |
             |                        |---Forward NS for DAD-->|
             |                        |                        |
             |                        |                        |
             |                        |<--NA with DAD result---|
             |                        |    [ARO+VPI+VSI]       |
             |<------Forward NA-------|                        |
             |                        |                        |
```

Figure 5: Message Interaction for Vehicular Neighbor Discovery

7. Address Registration and Duplicate Address Detection

This section explains address configuration, consisting of IP Address Autoconfiguration, Address Registration, and multihop DAD via V2I or V2V.

This document recommends a new Address Registration and DAD scheme in order to avoid multicast flooding and decrease link-scope multicast for energy and wireless channel conservation on a large-scale vehicular network. Host-initiated refresh of RA removes the necessity for routers to use frequent and unsolicited multicast RAs to accommodate hosts. This also enables the same IPv6 address prefix(es) to be used across a subnet.

There are three scenarios feasible in Address Registration scheme:

1. Vehicle enters the subnet for the first time or the current RSU belongs to another subnet: Vehicles need to perform the Address

Registration and multihop DAD as described in the following subsections.

2. Vehicle has already configured its IP addresses with prefix obtained from the previous RSU, and the current RSU located in the same subnet: This means RSUs have the same prefix and the vehicle has no need to repeat the Address Registration and multihop DAD.

3. Vehicle is not in the coverage of RSU but has a neighbor registered in RSU: This document proposes a new V2V scenario for vehicles which are currently not in the range of the RSU. If a user vehicle failed to find an on-link RSU, it starts to look for adjacent vehicle neighbors which can work as a relay neighbor to share the prefix obtained from RSU and undertake DAD of the user vehicle by forwarding DAD messages to RSU.

7.1. Address Autoconfiguration

A vehicle as an IPv6 host creates its link-local IPv6 address and global IPv6 address as follows [RFC4862]. When they receive RS messages from vehicles, RSUs send back RA messages containing prefix information. The vehicle makes its global IPv6 addresses by combining the prefix for its current link and its link-layer address.

The address autoconfiguration does not perform the legacy DAD as defined in [RFC4862]. Instead, a new multihop DAD is performed in Section 7.3.

7.2. Address Registration

After its IP tentative address autoconfiguration with the known prefix from an RSU and its link-layer address, a vehicle starts to register its IP address to the serving RSU along with multihop DAD. Address Register Option (ARO) is used in this step and its format is defined in [RFC6775].

ARO is always host-initiated by vehicles. Information such as registration time and registration status contained in ARO are applied to indicate the registration duration and result. ARO will also be forwarded to MA together with NS by RSUs.

An example message exchange procedure of Address Registration is presented in Figure 6. Since Address Registration is performed simultaneously with the multihop DAD, the specific procedure is together described with the DAD mechanism in Section 7.3.

```
             Vehicle                       RSU
                |                           |
                |                           |
         1.     |----NS with Address Reg--->|
                |            [ARO]          |
                |                           |
                |                           |
                |                           |
         2.     |<---NA with Address Reg----|
                |            [ARO]          |
```

Figure 6: Neighbor Discovery Address Registration

7.3. Multihop Duplicate Address Detection

Before it can exchange data, a node should determine whether its IP address is already used by another node or not. In the legacy IPv6 ND, hosts multicast NS messages to all nodes in the same on-link subnet for DAD. Instead of this, an optimized multihop DAD is designed to eliminate multicast messages for energy-saving purpose. For this multihop DAD, Neighbor Cache and DAD Table are maintained by each RSU and an MA, respectively, for the duplicate address inspection during the multihop DAD process. That is, each RSU makes Neighbor Cache Entries (NCE) of all the on-link hosts in its Neighbor Cache. Similarly, the MA stores all the NCEs reported by the RSUs in its DAD Table.

With the multihop DAD, a vehicle can skip the multicast-based DAD in its current wireless link whenever it enters the coverage of another RSU in the same subset, leading to the reduction of traffic overhead in vehicular wireless links.

For the multihop DAD, we take advantage of the procedure of [RFC6775] but simplified the message flows by canceling the two new ICMPv6 message types such as Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC). Instead, NS and NA containing ARO are directly forwarded between RSU and MA. This idea is raised because DAR and DAC

7.3.1. DAD without Intermediate Vehicle

Figure 7 presents the procedure of Address Registration and multihop DAD. The detailed steps are explained as follows.

```
        Vehicle                     RSU                MA
           |                         |                  |
           |                         |                  |
    1.     |--NS with Address Reg--> |                  |
           |     [ARO+VPI+VSI]       |                  |
           |                         |                  |
    2.     |                         |----Forward NS--->|
           |                         |                  |
           |                         |                  |
    3.     |                         |<---Forward NA----|
           |                         |                  |
           |                         |                  |
    4.     |<--NA with Address Reg--|                   |
           |     [ARO+VPI+VSI]       |                  |
```

Figure 7: Neighbor Discovery Address Registration with Multihop DAD

1. A vehicle sends an NS message to the current RSU in unicast, containing the ARO to register its address.

2. The RSU receives the NS message, and then inspects its Neighbor Cache to check whether it is duplicate or not. If there is no duplicate NCE, a tentative NCE is created for this address, and then the RSU forward the NS message containing the ARO to the MA for the multihop DAD.

3. When the MA receives NS from an RSU, it checks whether the register-requested address exists in its DAD Table or not. If an entry with the same address exists in the DAD Table, which means that the address is considered "Duplicate Address", then MA returns a NA message containing the registration status in ARO to notify the RSU of the address duplication. If no entry with the same address exists in the DAD Table, which means that an entry for the address is created, then MA replies a NA message to the RSU to confirm the uniqueness of the register-requested address to the RSU.

4. If the address duplication is notified by the MA, the RSU deletes the tentative NCE, and forward NA with to the address-registration vehicle to notify the registration failure. Otherwise, the RSU changes the tentative NCE into a registered NCE in its Neighbor Cache, and then forward NA to the vehicle to notify the registration success.

Thus, the multihop DAD is processed simultaneously with the Address Registration. Note that the tentative address is not considered assigned to the vehicle until the MA confirms the uniqueness of the register-requested address in the multihop DAD.

7.3.2. DAD with one Intermediate Vehicle

If a vehicle failed to register a default router, it triggers neighbor discovery to look for vehicle neighbors which can provide relay service using multihop communication. In this specification, we assumed vehicles would not emulate V2V communication and trigger relay scenario only if Router Discovery(RD) failed.

```
User Vehicle          Relay Vehicle                RSU               MA
   |                        |                       |                 |
   |------------------------|                       |                 |
   |        RD failed       |                       |                 |
   |------------------------|                       |                 |
   |                        |                       |                 |
   |                        |                       |                 |
   |-----------NS---------->|                       |                 |
   |                        |                       |                 |
   |<--NA with Prefix Info--|                       |                 |
   |                        |                       |                 |
   |                        |                       |                 |
   |--NS with Address Reg-->|                       |                 |
   |    [ARO+VPI+VSI]       |                       |                 |
   |                        |----- Forward NS ----->|                 |
   |                        |                       |                 |
   |                        |                       |-----------------|
   |                        |                       | Same as Figure 9|
   |                        |                       |-----------------|
   |                        |                       |                 |
   |                        |<--NA with Address Reg-|                 |
   |                        |     [ARO+VPI+VSI]     |                 |
   |<------ Forward NA -----|                       |                 |
   |                        |                       |                 |
```

Figure 8: Address Registration and Multihop DAD via V2V Relay

Since vehicles have a digital road map with the information of RSUs (e.g., position and communication coverage), they can determine if they are available to serve as a relay vehicle. Only vehicles with the ability to serve as temporary relays will take action when they receive relay service requests. The user vehicle can process global address configuration, Address Registration and DAD through its relay vehicle before it enters the coverage of RSUs. See Figure 8.

When a user vehicle failed to directly register to an RSU, it initiates neighbor discovery to detect vehicle neighbors through V2V communication. Vehicle sends NS messages to connect with neighbors in range. If neighbor can provide relay service, it creates a NCE for user vehicle, setting its own address as relay address, and sends back NA with prefix information received from RSU.

To guarantee vehicles could find the nearest neighbor from multiple neighbors which can act as relay vehicles, a new time-out mechanism is presented to select the nearest neighbor by hop distance parameter carried in Prefix Information Option. That is, a user vehicle multicast NS messages to look for relay vehicles after RD failed and wait for 1.5 seconds to receive all NA replies from neighbors. Each NA carries its own global prefix(es) and the hop distance(s) in Prefix Information Option. The user vehicle preserves every NA reply in a temporary router list and select the one with least hop counts as its relay vehicle after time out.

With receipt of NA, user vehicle configures its global address with prefix information as mentioned in Section 7.1. After this, user vehicle takes up to initiate the Address Registration along with DAD process via relay vehicle. NS message is configured as specified in Section 7.2 but indicate the relay vehicle's address as next-hop to reach the RSU. In such a case, when relay vehicle receives relay request message, it will forward NS message to RSU. The procedure sets up on the rails except MA will include the relay vehicle's address as relay address in NCE to indicate that at this moment, it is not a directly attached vehicle, and sets the relay address as next-hop address. Relay vehicle forwards DAD result information message to user vehicle as soon as it received.

7.3.3. DAD with multiple Intermediate Vehicles

This document supports multihop communications (e.g., multihop DAD and UDP/TCP transmission) for remote vehicles through multiple relay vehicles. Vehicles which have already finished DAD process can serve as temporary routers and forward packets for remote vehicles.

A new routing mechanism is specified to accomplish route selections among user vehicles and serving RSUs when multiple vehicles act as relay vehicles. Taking advantage of the Destination-Sequenced Distance-Vector routing protocol (DSDV) [DSDV], this new routing approach supposes that each vehicle holds a Neighbor Routing Table which integrates the neighbor information in Neighbor Cache and forwarding records for remote vehicles. Each vehicle which acts as a relay vehicle for this remote vehicle will make records in its Neighbor Routing Table.

Figure 9 specifies an example of parameters in Neighbor Routing Table when more than one vehicle work as intermediate relay vehicles. In Figure 9, Vehicle3 connects RSU1 indirectly via Vehicle2 and Vehicle1. When Vehicle1 and Vehicle2 forward messages for Vehicle3, they make records in its Neighbor Routing Table including the next-hop node to indicate the route to Vehicle3. This can ensure that the packets from a source vehicle can be successfully transmitted to an RSU as well as the reverse packet path exists from the RSU to the source vehicle.

```
+--------+       +--------+         +--------+         +--------+
|Vehicle3|<......>|Vehicle2|<........>|Vehicle1|<.......> |  RSU1  |
|  (V3)  |   V2V  |  (V2)  |    V2V   |  (V1)  |   V2I    |        |
+--------+       +--------+         +--------+         +--------+

+------------+    +------------+      +------------+      +------------+
|Node|NextHop|    |Node|NextHop|      |Node|NextHop|      |Node|NextHop|
+------------+    +------------+      +------------+      +------------+
| V2 |   V2  |    | V1 |   V1  |      |RSU1| RSU1  |      |  V1  |  V1 |
+------------+    | V3 |   V3  |      | V2 |  V2   |      |  V2  |  V1 |
                  +------------+      | V3 |  V2   |      |  V3  |  V1 |
                                      +------------+      +------------+
```

Figure 9: An Example of Neighbor Routing Table when multiple Vehicles act as Relay Vehicles

7.4. Pseudonym Handling

Considering the privacy protection of a vehicle, a pseudonym mechanism for its link-layer address is requested. This mechanism periodically modifies the link-layer address, leading to the update of the corresponding IP address. A random MAC Address Generation mechanism is proposed in Appendix F.4 of [IEEE-802.11-OCB] by generating the 46 remaining bits of MAC address using a random number generator. When it changes its MAC address, a vehicle should ask the serving RSU to update its own NCE, and to register its IP address into the MA again.

8. Security Considerations

This document shares all the security issues of the neighbor discovery protocol and 6LoWPAN protocol. This document can get benefits from secure neighbor discovery (SEND) [RFC3971] in order to protect ND from possible security attacks.

9. Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government, Ministry of Science and ICT (MSIT) (No. 2020R1F1A1048263).

This work was supported in part by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea MSIT (Ministry of Science and ICT) (R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning).

This work was supported in part by the MSIT under the ITRC (Information Technology Research Center) support program (IITP-2021-2017-0-01633) supervised by the IITP.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <https://www.rfc-editor.org/info/rfc5889>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013, <https://www.rfc-editor.org/info/rfc6763>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC8200]
Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8691] Benamar, N., Härri, J., Lee, J., and T. Ernst, "Basic Support for IPv6 Networks Operating Outside the Context of a Basic Service Set over IEEE Std 802.11", RFC 8691, DOI 10.17487/RFC8691, December 2019, <https://www.rfc-editor.org/info/rfc8691>.

[I-D.ietf-ipwave-vehicular-networking]
(editor), J. (. J., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", Work in Progress, Internet-Draft, draft-ietf-ipwave-vehicular-networking-25, 13 February 2022, <https://www.ietf.org/archive/id/draft-ietf-ipwave-vehicular-networking-25.txt>.

10.2. Informative References

[I-D.jeong-ipwave-iot-dns-autoconf] Jeong, J. P., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks", Work in Progress, Internet-Draft, draft-jeong-ipwave-iot-dns-autoconf-11, 21 August 2021, <https://www.ietf.org/archive/id/draft-jeong-ipwave-iot-dns-autoconf-11.txt>.

[I-D.jeong-ipwave-vehicular-mobility-management]
Jeong, J. (., Mugabarigira, B. A., Shen, Y. (., and Z. Xiang, "Vehicular Mobility Management for IP-Based Vehicular Networks", Work in Progress, Internet-Draft, draft-jeong-ipwave-vehicular-mobility-management-06, 21

August 2021, <https://www.ietf.org/archive/id/draft-jeong-ipwave-vehicular-mobility-management-06.txt>.

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

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

[IEEE-802.11-OCB] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, December 2016.

[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.

[VIP-WAVE] Cespedes, S., Lu, N., and X. Shen, "VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks", IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, March 2013.

[DSDV] Perkins, C. and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers", ACM SIGCOMM, August 1994.

Appendix A. Changes from draft-jeong-ipwave-vehicular-neighbor-discovery-12

The following changes are made from draft-jeong-ipwave-vehicular-neighbor-discovery-12:

* Several sentences are rephrased to more clearly describe the goal and the motivations of this draft. In addition, several typos are

corrected and one author's affiliation information is also updated.

*This version also updates the references to synchronize with the referred I.-D.s.

Authors' Addresses

Jaehoon (Paul) Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4957
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
Email: chrisshen@skku.edu
URI: https://chrisshen.github.io

Zhong Xiang
Department of Electrical and Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 10 9895 1211
Email: xz618@skku.edu

Sandra Cespedes
NIC Chile Research Labs
Universidad de Chile
Av. Blanco Encalada 1975

Santiago
Chile

Phone: +56 2 29784093
Email: scespede@niclabs.cl