IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: November 11, 2021

Z. Yan
CNNIC
J. Weng
G. Geng
Jinan University
J. Lee
Sejong University
J. Jeong
Sungkyunkwan University
May 10, 2021

Service and Neighbor Vehicle Discovery in IPv6-Based Vehicular Networks

draft-yan-ipwave-nd-08.txt

Abstract

For Cooperative Adaptive Cruise Control (C-ACC), platooning and other typical use cases in Intelligent Transportation System (ITS), IPv6 communication between neighbor vehicles and between vehicle and server pose the following two issues: 1) how to discover a neighbor vehicle and the demanded service; and 2) how to discover the link-layer address and other metadata of the neighbor vehicle and selected server. This document presents a solution to these problems based on DNS-SD/mDNS [RFC6762][RFC6763].

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.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

As illustrated in [DNS-Autoconf], a naming scheme is needed for the vehicle devices to support the unique name auto-configuration. This can support the location based communication and scalable information organization in Intelligent Transportation Systems (ITS). Based on the naming scheme like this and the widely-used DNS-SD/mDNS protocol, this document illustrates how to discover a neighbor vehicle or the required services with DNS resolution logic. Before this, we make the following assumptions:

- o Name: A vehicle SHOULD have at least one temporary name which may be related with its geo-location or provided services. This name is related with the service or identifier of the particular vehicle.

- o Address: A vehicle SHOULD have at least one global IP address which is routable for the IPv6 communications. This address acts as the Home Address (HoA) of vehicle to facilitate its mobility.

In this way, a standardized, efficient and scalable scheme should be used to retrieve the necessary information of the corresponding node (domain name, IP address, geo-location, link-layer address, key and so on) for the further communications based on the DNS-SD/mDNS functions. In addition, the IPv6 Neighbor Discovery (ND)'s messages (e.g., RA and RS messages) can also be used to exchange some required information (e.g., mobile network prefixes) in ITS in combination with DNS-SD/mDNS [MNPP].

2. Name and address configurations

Typically, the Road-Side Unit (RSU) acts as an Access Router (AR) to serve for the static and moving vehicles which want to be connected into the networks locally or publically.

Based on [RFC3646], [RFC6106] or extended WAVE Service Announcement (WSA) message, the RSU can announce its location based name prefix to the vehicles covered by the RSU. This location based prefix may contain information such as country, city, street and so on, which will act as the "domain_name" of the vehicle device name as specified in [DNS-Autoconf].

The RSU may also advertise the IPv6 prefix to support the IPv6 Stateless Address Auto-configuration (SLAAC) operation of vehicle devices and movement detection (in the IP layer). If the DHCPv6 is used for the address configuration, RSU also acts as functional entity such as a DHCP proxy and DHCP server.

3. Service and neighbor vehicle discovery

Vehicular network is a dynamic environment, then the following two modes should be supported based on different connection conditions of the vehicle.

(1) RSU based

Vehicles may have direct connection with the serving RSU and join the same link with the serving RSU. Then the RSU can maintain the registered vehicles and services in its serving domain. Otherwise, the RSU acts as a proxy node for discovering in a proxy manner [DNSSD-Hybrid].

When a vehicle wants to locate the potential service or the nearby neighbor and further establish the communication, the vehicle will trigger the direct unicast query to port 5353 or legacy unicast DNS query to the RSU. RSU may respond directly if it has the related information, otherwise, the RSU multicasts the DNS query to the multicast group to retrieve the related information. A unicast

response is the first recommendation here because it can suppress the flooding, but of course, the DNS response message can also be multicasted as an active announcement of the vehicle or service existence.

(2) Ad-hoc based

Vehicles may communicate with each other or sense the front and rear neighbor vehicles with DSRC, WiFi, Bluetooth or other short-distance communication technologies, connecting each other in the Ad-hoc manner. Then the discovery can also be executed in an infrastructure-less manner with the following phases, as specified in the plain mDNS.

o Probing: When a vehicle starts up, wakes up from sleeping mode or the Vehicular Ad Hoc Networks (VANET) topology changes (after configuration of the name and address), it should probe the availability of the service with which it can provide other vehicles. Then the vehicle periodically announces the service and its existence with unsolicited multicast DNS response containing, in the Answer Section, all of its service name, DNS name, IP address and other information. The vehicle also updates the related information actively if there is any change.

o Discovering: To support the service and neighbor vehicle discovery in the dynamic and fragmentation-possible environment in VANET, different query modes of mDNS can be used for different scenarios: 1) One-Short Multicast DNS Query can be used to locate a specific vehicle. 2) Continuous Multicast DNS Query can be used to locate the nearby vehicles which are moving.

o Refreshing: After the neighbor discovery as illustrated above, the vehicles should continually exchange their DNS name, IP address, geo-location and other information in order to refresh the established communications. For example, the Multiple Questions Multicast Responses can be used to update the caches of receivers efficiently and Multiple Questions Unicast Responses can be used to support the fast bootstrapping when a new vehicle joins.

o Goodbye: When the vehicle arrives at its destination, stops temporarily or shuts down its communication or sensing devices, it will announce the service suspending and its inexistence with an unsolicited multicast DNS response packet, giving the same Resource Records (RRs) (containing its DNS name and IP address), but with zero Time-To-Live (TTL).

4. Mobility support

During the movement of the vehicle, it may cross different RSUs. When a vehicle enters the coverage of a new RSU, the new domain prefix and new IPv6 prefix may be learned. Generally, there are the following three main cases for the mobility:

- o The domain name changes and the IP prefix remains. The vehicle will configure a new DNS name from the new RSU. Then the vehicle should update the new DNS name in the local database (e.g., RSU) with DNS Update [RFC2136], DNS Push Notifications [DNSSD-Push], Service Registration Protocol (SRP) [DNSSD-SRP] or just actively announce its new name information with plain mDNS notification scheme. If the service is registered in the RSU, then the stale service should be withdrawn in order to reduce the management load [DNSSD-Lease].

- o The domain name remains and the IP prefix changes. The vehicle will configure a new IPv6 temporary address (e.g., CoA) form the new RSU. Then the IP-layer mobility management protocols should be used to update the binding entry of the vehicle (e.g., Mobile IPv6 [RFC6275]).

- o Both the domain name and IP prefix change, the name information should be updated as in the first case and then the IP-layer mobility management protocols (e.g., Mobile IPv6 [RFC6275] and Proxy Mobile IPv6 [RFC5213]) as in the second case should also be triggered.

5. Signaling messages

To facilitate the further communication, the link-layer address, public Key, geo-information and other metadata may be included in the DNS message in a piggyback manner. Specially, the TXT RR in DNS-SD can be used to include these information with multiple key: value pairs.

Besides, this kind of information may be obtained through the following IPv6 Neighbor Discovery Protocol (NDP) or other procedures (e.g., DHCP and WSA).

6. Security considerations

In order to reduce the DNS traffic on the wireless link and avoid the unnecessary flooding, the related schemes in mDNS can be used, such as: Known-Answer Suppression, Multipacket Known-Answer Suppression, Duplicate Question Suppression and Duplicate Answer Suppression.

In order to guarantee the origination of the DNS message and avoid the DNS message tampering, the security consideration in mDNS should also be adopted.

7. References

7.1. 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>.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, DOI 10.17487/RFC2136, April 1997, <https://www.rfc-editor.org/info/rfc2136>.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, DOI 10.17487/RFC3646, December 2003, <https://www.rfc-editor.org/info/rfc3646>.

[RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <https://www.rfc-editor.org/info/rfc5213>.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, DOI 10.17487/RFC6106, November 2010, <https://www.rfc-editor.org/info/rfc6106>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

[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>.

7.2. Informative References

[DNS-Autoconf]
Jeong, J., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks", draft-jeong-ipwave-iot-dns-autoconf-07, November 2019.

[DNSSD-Hybrid]
Cheshire, S., "Discovery Proxy for Multicast DNS-Based Service Discovery", draft-ietf-dnssd-hybrid-10, March 2019.

[DNSSD-Lease]
Cheshire, S. and T. Lemon, "Dynamic DNS Update Leases", draft-sekar-dns-ul-02, August 2018.

[DNSSD-Push]
Pusateri, T. and S. Cheshire, "DNS Push Notifications", draft-ietf-dnssd-push-25, October 2019.

[DNSSD-SRP]
Cheshire, S. and T. Lemon, "Service Registration Protocol for DNS-Based Service Discovery", draft-ietf-dnssd-srp-02, July 2019.

[MNPP] Lee, J., Tsukada, M., and T. Ernst, "Mobile Network Prefix Provisioning", draft-jhlee-mext-mnpp-00, October 2009.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing 100190
China

EMail: yan@cnnic.cn

Jian Weng
Jinan University
No.601, West Huangpu Avenue
Guangzhou 510632
China

EMail: cryptjweng@gmail.com

Guanggang Geng
Jinan University
No.601, West Huangpu Avenue
Guangzhou 510632
China

EMail: gggeng@jnu.edu.cn

Jong-Hyouk Lee
Sejong University
209, Neungdong-ro, Gwangjin-gu
Seoul 05006
Republic of Korea

EMail: jonghyouk@sejong.ac.kr

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

EMail: pauljeong@skku.edu