Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 28, 2017

Z. Yan
CNNIC
J. Lee
Sangmyung University
October 25, 2016

Neighbor discovery to support direct communication in ITS
draft-yan-its-nd-01.txt

Abstract

For C-ACC, Platooning and other typical use cases in ITS, how to establish direct IP communication paths between neighbor vehicles poses two issues : how to discover the neighbor vehicle and the nearby service (from the upper layer); how to discover the link-layer address of the selected vehicle (from the lower layer). This draft aims to solve these problems based on mDNS.

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 28, 2017.

Table of Contents

1. Introduction

As illustrated in [DNS-Autoconf] draft, a naming scheme is proposed for the vehicle devices to support the unique name auto-configuration. This can be used to support the location based communicaton and scalable information organization in ITS. Based on the naming scheme like this and the mature mDNS protocol, this draft illustrates how to discover the neighbor vehicle or services with the infrastructure-less DNS resolution. Before this, we have the following assumptions:

- Name: vehicle SHOULD have a temporary name which is related to its location.

- Address: vehicle SHOULD have a global IP address which is stable.

In this way, a standardized and efficient scheme can be used to retrieve the necessary information of the neighbor vehicles (domain name, IP address, goe-location and so on) for the further direct communications based on the mDNS function.

2. Name configuration

The RSU acts as an access router for the static and moving vehicles who want to be connected. Based on RFC3646, RFC6106 or extended WSA message, the RSU can announce its location based name prefix to the vehicles covered by it. 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 spefified in the [DNS-Autoconf] document.

3. Address configuration

The RSU may advertise the IP prefix to support the SLAAC operation of vehicle devices and movement detection (in the IP layer). However, the DHCP may also be used for the address configuration.

The network architecture which illustrates the prefix management of name and address should be discussed in depth in this WG.

4. Neighbor discovery

- RSU based: Vehicles may have direct connection with the serving RSU and join the same link-local multicast group with the serving RSU. Then the RSU can maintain the registered vehicle or service in its serving domain. Otherwise, the RSU acts as a relay node for discovering in a proxy manner. When a vehicle wants to locate the potential nearby neighbor and further establish the communication with it, the vehicle will trigger the direct unicast query to port 5353 or legacy unicast DNS query to the RSU. RSU may response directly if it has the related information, otherwise, the RSU multicasts the DNS query to multicast group to retrieve the related information. 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 existence.

- AD-hoc based: Vehicles may communicate with each other or sense the front and rear neighbors with DSRC, WiFi, blue-tooth or other short-distance communication technologies. When a vehicle discovers the neighbor vehicles through the periodic scanning, a L2 connection will be established. Then they can join the same link-local multicast group, and the discovery can be executed in an infrastructure-less manner with the following phases.

Probing: When a vehicle starts up, wakes up from stalls or topology changes (after configuration of the name and address), it should probe the availability of the service it announced. Then the vehicle periodically announces the service and its existence with unsolicited

multicast DNS response containing, in the Answer Section, all of its service and name and address. The vehicle also updates the related information actively if there is any change.

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:

- One-Short Multicast DNS Query can be used to locate a specific service (for example).

- Continuous Multicast DNS Query can be used to locate the nearby vehicles which are moving (for example).

Refreshing: After the neighbor discovery illustrated above, the vehicles should continually exchange their domain name, IP address and geo-location 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 new vehicle joins.

Goodbye: When the vehicle arrives at its destination, stalls temporarily or shuts down its communication or sensing devices, it will announce the service suspending and its inexistence with unsolicited multicast DNS response packet, giving the same RRs (containing its name and address), but TTL of zero.

5. Handover

During the movement of the vehicle, it may cross different RUSes. When attaching into a new RSU, the new domain prefix may be learned. But the vehicle should keep its previous name for some time until that all the communicating neighbors learned its new name. During this period, the vehicle will contain both previous and new domain names in the DNS response message. We assume that the IP prefix is available in a much larger domain than the name prefix.

6. Signaling messages

To facilitate the further communication, the link-layer address and geo-information may be included in the DNS message in a piggyback manner. Otherwise, these information may be obtained through the following NDP or other procedures.

7. 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.

8. References

8.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3640] van der Meer, J., Mackie, D., Swaminathan, V., Singer, D., and P. Gentric, "RTP Payload Format for Transport of MPEG-4 Elementary Streams", RFC 3640, DOI 10.17487/RFC3640, November 2003, <http://www.rfc-editor.org/info/rfc3640>.

[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, <http://www.rfc-editor.org/info/rfc6106>.

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

8.2. Informative References

[DNS-Autoconf] Jeong, J., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-its-iot-dns-autoconf-00, March 2016.

Authors' Addresses

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

EMail: yan@cnnic.cn

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

EMail: jonghyouk@smu.ac.kr