Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 20, 2017
J. Jeong
Sungkyunkwan University
T. Oh
Rochester Institute of Technology
July 19, 2016

Problem Statement for Vehicle-to-Infrastructure Networking
draft-jeong-its-v2i-problem-statement-02

Abstract

This document specifies the problem statement for IPv6-based vehicle-to-infrastructure networking. Dedicated Short-Range Communications (DSRC) is standardized as IEEE 802.11p for the wireless media access in vehicular networks. This document addresses the extension of IPv6 as the network layer protocol in vehicular networks and is focused on the networking issues in one-hop communication between a Road-Side Unit (RSU) and vehicle. The RSU is connected to the Internet and allows vehicles to have the Internet access if connected. The major issues of including IPv6 in vehicular networks are neighbor discovery protocol, stateless address autoconfiguration, and DNS configuration for the Internet connectivity over DSRC. Also, when a vehicle and an RSU have an internal network, respectively, the document discusses the issues of the internetworking between the vehicle's internal network and the RSU's internal network, such as prefix discovery, prefix exchange, and service discovery.

Table of Contents

1. Introduction

Recently, Vehicular Ad Hoc Networks (VANET) have been focusing on intelligent services in road networks, such as driving safety, efficient driving, and entertainment. For this VANET, 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] with a consideration of the vehicular network's characteristics such as a vehicle's velocity and collision avoidance.

Now the deployment of VANET is demanded into real road environments along with the popularity of smart devices (e.g., smartphone and tablet). Many automobile vendors (e.g., Benz, BMW, Ford, Honda, and Toyota) started to consider automobiles as computers instead of mechanical machines since many current vehicles are operating with many sensors and software. Also, Google made a great advancement in self-driving vehicles with many special software modules and hardware devices to support computer-vision-based object recognition, machine-learning-based decision-making, and GPS navigation.

With this trend, vehicular networking has been researched to enable vehicles to communicate with other vehicles and infrastructure nodes in the Internet by using TCP/IP technologies [ID-VN-Survey], such as IP address autoconfiguration, routing, handover, and mobility management. IPv6 [RFC2460] is suitable for vehicular networks since the protocol has abundant address space, autoconfiguration features, and protocol extension ability through extension headers.

This document specifies the problem statement of IPv6-based vehicle-to-infrastructure (V2I) networking, such as IPv6 addressing [RFC4291], neighbor discovery [RFC4861], address autoconfiguration [RFC4862], and DNS naming service [RFC6106][RFC3646][ID-DNSNA]. This document also specifies the problem statement of the internetworking between a vehicle's internal network and an RSU's internal network, such as prefix discovery, prefix exchange, and service discovery, in the case where the vehicle and the RSU have their own internal network. In addition, the document analyzes the characteristics of vehicular networks to consider the design of V2I networking.

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:

- 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.

- 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.

- 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 the problem statement of vehicle-to-infrastructure (V2I) networking based on IPv6. The main focus is one-hop networking between a vehicle and an RSU or between vehicles via an RSU. However, this document does not address multi-hop networking scenarios of vehicles and RSUs. Also, the problems focus on the network layer (i.e., IPv6 protocol stack) rather than the media access control (MAC) layer and the transport layer (e.g., TCP, UDP, and SCTP).

Figure 1 shows the network configuration for V2I networking in a road network. The two RSUs (RSU1 and RSU2) are deployed in the road network and are connected to the Vehicular Cloud through the Internet. The TCC is connected to the Vehicular Cloud and the two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and the last vehicle (Vehicle3) is wirelessly connected to RSU2. Vehicle1 can communicate with Vehicle2 via RSU1. Vehicle1 can communicate with Vehicle3 via RSU1 and RSU2.

```
                               *-------------*
                              *               *         .-------.
                             * Vehicular Cloud *<------>|  TCC  |
                              *               *         ._______.
                               *-------------*
                              ^               ^
                              |               |
                              |               |
                              v               v
                      .--------.             .--------.
                      |  RSU1  |<----------->|  RSU2  |
                      .________.             .________.
                      ^        ^                  ^
                      .        .                  .
                      .        .                  .
                      v        v                  v
               .--------.    .--------.         .--------.
               |Vehicle1|=>  |Vehicle2|=>       |Vehicle3|=>
               .________.    .________.         .________.

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

Figure 1: The Network Configuration for V2I Networking

Figure 2 shows internetworking between the vehicle's moving network and the RSU's fixed network. There exists an internal network (Moving Network1), which is located inside Vehicle1. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). The internal network (Fixed Network1) is located inside RSU1. RSU1 has the DNS Server (RDNSS2), one host (Host3), the two routers (Router3 and Router4), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1's Router1 and RSU1's Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for I2V networking.

This document addresses the internetworking between the vehicle's moving network and the RSU's fixed network in Figure 2 and the required enhancement of IPv6 protocol suite for the V2I networking service.

```
                           (*)<..........>(*)
                            |              | 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. Internetworking between the Vehicle and RSU Networks

This section discusses the internetworking between the vehicle's moving network and the RSU's fixed network. As shown in Figure 2, it is assumed that the prefix assignment for each subnet inside the vehicle's mobile network and the RSU's fixed network through a prefix delegation protocol. Problems are a prefix discovery and prefix exchange. The prefix discovery is defined as how routers in a moving network discover the prefixes of the subnets in the moving network, as shown in Figure 2. The prefix exchange is defined as how a vehicle and an RSU exchange their prefixes with each other. Once these prefix discovery and prefix exchange are established, the unicast of packets should be supported between the vehicle's moving network and the RSU's fixed network. Also, the DNS naming service should be supported for the DNS name resolution for a host or server in either the vehicle's moving network or the RSU's fixed network.

6. IPv6 Addressing

This section discusses IP addressing for V2I networking. There are two policies for IPv6 addressing in vehicular networks. The one policy is to use unique local IPv6 unicast addresses (ULAs) for vehicular networks [RFC4193]. The other policy is to use global IPv6 addresses for the interoperability with the Internet [RFC4291]. The former approach is usually used by Mobile Ad Hoc Networks (MANET) for a separate multi-link subnet. This approach can support the emergency notification service and navigation service in road networks. However, for general Internet services (e.g., email access, web surfing and entertainment services), the latter approach is required.

For the global IP addresses, there are two policies, which are a multi-link subnet approach for multiple RSUs and a single subnet approach per RSU. In the multi-link subnet approach, which is similar to ULA for MANET, RSUs play a role of L2 switches and the router interconnected with the RSUs is required. The router maintains the location of each vehicle belonging to an RSU for L2 switching. In the single subnet approach per RSU, which is similar to the legacy subnet in the Internet, RSUs play a role of L3 router.

7. Neighbor Discovery

The Neighbor Discovery (ND) is a core part of IPv6 protocol suite [RFC4861]. This section discusses the extension of ND for V2I networking. The vehicles are moving fast within the communication coverage of an RSU. The external link between the vehicle and the RSU can be used for V2I networking, as shown in Figure 2.

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval should be adjusted for high-speed vehicles and vehicle density. As vehicles move faster, the NA interval should decrease for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase for the NA messages to collide with other NA messages with lower collision probability.

8. IP Address Autoconfiguration

This section discusses the IP address autoconfiguration for V2I networking. For the IP address autoconfiguration, the high-speed vehicles should also be considered. The legacy IPv6 stateless address autoconfiguration [RFC4862], as shown in Figure 1, may not perform well because vehicles can pass through the communication coverage of the RSU before the address autoconfiguration with the Router Advertisement and Duplicate Address Detection (DAD)

procedures.

To mitigate the impact of vehicle speed on the address configuration, RSU can perform IP address autoconfiguration includig the DAD proactively for the sake of the vehicles as an ND proxy. If vehicles periodically report their mobility information (e.g., position, trajectory, speed, and direction) to TCC, TCC can coordinate RSUs under its control for the proactive IP address configuration of the vehicles with the mobility information of the vehicles. DHCPv6 (or Stateless DHCPv6) can be used for the IP address autoconfiguration [RFC3315][RFC3736].

In the case of a single subnet per RSU, the delay to change IPv6 address through DHCPv6 procedure is not suitable since vehicles move fast. Some modifications are required for the high-speed vehicles that quickly crosses the communication coverages of multiple RSUs. Some modifications are required for both stateless address autoconfiguration and DHCPv6.

9. DNS Naming Service

This section discusses a DNS naming service for V2I networking. The DNS naming service can consist of the DNS name resolution and DNS name autoconfiguration.

The DNS name resolution translates a DNS name into the corresponding IPv6 address through a recursive DNS server (RDNSS) within the vehicle's moving network and DNS servers in the Internet [RFC1034][RFC1035], which are distributed in the world. The RDNSSes can be advertised by RA DNS Option or DHCP DNS Option into the subnets within the vehicle's moving network.

The DNS name autoconfiguration makes a unique DNS name for hosts within a vehicle's moving network and registers it into a DNS server within the vehicle's moving network [ID-DNSNA]. With Vehicle Identification Number (VIN), a unique DNS suffix can be constructed as a DNS domain for the vehicle's moving network. Each host can generate its DNS name and register it into the local RDNSS in the vehicle's moving network.

10. IP Mobility Management

This section discusses an IP mobility support in V2I networking. In a single subnet per RSU, vehicles keep crossing the communication coverages of adjacent RSUs. During this crossing, TCP/UDP sessions can be maintained through IP mobility support, such as Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 [RFC5213][RFC5949], and Distributed Mobility Management (DMM) [RFC7333][RFC7429]. Since vehicles move

fast along roadways, this high speed should be considered for a parameter configuration in the IP mobility management. With the periodic reports of the mobility information from the vehicles, TCC can coordinate RSUs and other network compoments under its control for the proactive mobility management of the vehicles along the movement of the vehicles.

To support the mobility of a vehicle's moving network, Network Mobility Basic Support Protocol (NEMO) can be used [RFC3963]. Like Mobile IPv6, the high speed of vehicles should be considered for a parameter configuration in NEMO.

11. Service Discovery

Vehicles need to discover services (e.g., road condition notification, navigation service, and infotainment) provided by infrastructure nodes in a fixed network via RSU, as shown in Figure 2. During the passing of an intersection or road segment with an RSU, vehicles should perform this service discovery quickly.

Since with the existing service discovery protocols, such as DNS-based Service Discovery (DNS-SD) [RFC6763] and Multicast DNS (mDNS) [RFC6762], the service discovery will be performed with message exchanges, the discovery delay may hinder the prompt service usage of the vehicles from the fixed network via RSU. One feasible approach is a piggyback service discovery during the prefix exchange of network prefixes for the networking between a vehicle's moving network and an RSU's fixed network. That is, the message of the prefix exchange can include service information, such as each service's IP address, transport layer protocol, and port number.

IPv6 ND can be extended for the prefix and service discovery [ID-Vehicular-ND]. Vehicles and RSUs can announce the network prefixes and services in their internal network via ND messages containing ND options with the prefix and service information. Since it does not need any additional service discovery protocol in the application layer, this ND-based approach can provide vehicles and RSUs with the rapid discovery of the network prefixes and services.

12. Security Considerations

The security and privacy are very important in secure vehicular networks for V2I networking. Only valid vehicles should be allowed to use V2I networking in vehicular networks. VIN and a user certificate along with in-vehicle device's identifier generation can be used to authenticate a vehicle and the user through a road infrastructure node, such as an RSU connected to an authentication server in TCC. Also, TLS certificates can be used for secure vehicle

communications.

A security scheme providing authentication and access control should be provided in vehicular networks [VN-Security]. With this scheme, the secuirty and privacy can be supported for safe and reliable data services in vehicular networks.

This document shares all the security issues of the neighbor discovery protocol. This document can get benefits from secure neighbor discovery (SEND) [RFC3971].

13. Acknowledgements

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning). This work was supported in part by ICT R&D program of MSIP/IITP (14-824-09-013, Resilient Cyber-Physical Systems Research) and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning.

This document has greatly benefited from inputs by Alexandre Petrescu, Thierry Ernst, Nabil Benamar, Jerome Haerri, Richard Roy, and Sandra Cespedes. The authors sincerely appreciate their contributions.

14. References

14.1. 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.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[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.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC7333] Chan, H., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

[RFC7429] Liu, D., Zuniga, JC., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, January 2015.

[RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", RFC 1035, November 1987.

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

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, February 2013.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, February 2013.

14.2. Informative References

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

[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.

[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.

[ID-VN-Survey] Jeong, J., Ed., Cespedes, S., Benamar, N., and J. Haerri, "Survey on IP-based Vehicular Networking for Intelligent Transportation Systems", draft-jeong-its-vehicular-networking-survey-01 (work in progress), July 2016.

[ID-DNSNA] Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-its-iot-dns-autoconf-01 (work in progress), July 2016.

[ID-Vehicular-ND] Jeong, J., Ed., Shen, Y., Jo, Y., Jeong, J., and J. Lee, "IPv6 Neighbor Discovery for Prefix and Service Discovery in Vehicular Networks", draft-jeong-its-vehicular-neighbor-discovery-00 (work in progress), July 2016.

[VN-Security] Moustafa, H., Bourdon, G., and Y. Gourhant, "Providing Authentication and Access Control in

Vehicular Network Environment", IFIP TC-11 International Information Security Conference, May 2006.

Appendix A. Changes from draft-jeong-its-v2i-problem-statement-01

The following changes were made from draft-jeong-its-v2i-problem-statement-01:

- In Section 11, an extension of IPv6 ND is added for service discovery along with prefix discovey.

Authors' Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 440-746
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

Tae (Tom) Oh
Department of Information Sciences and Technologies
Rochester Institute of Technology
One Lomb Memorial Drive
Rochester, NY 14623-5603
USA

Phone: +1 585 475 7642
EMail: Tom.Oh@rit.edu