Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 10, 2017

J. Jeong
Sungkyunkwan University
A. Petrescu
CEA, LIST
T. Oh
Rochester Institute of Technology
D. Liu
Alibaba
C. Perkins
Futurewei Inc.
June 8, 2017

Problem Statement for IP Wireless Access in Vehicular Environments
draft-jeong-ipwave-problem-statement-00

Abstract

This document provides a problem statement for IP Wireless Access in Vehicular Environments (IPWAVE), that is, vehicular networks. This document addresses the extension of IPv6 as the network layer protocol in vehicular networks. It deals with networking issues in one-hop communication between a Road-Side Unit (RSU) and a vehicle, that is, "vehicle-to-infrastructure" (V2I) communication. It also deals with one-hop communication between two neighboring vehicles, that is, "vehicle-to-vehicle" (V2V) communication. Major issues about IPv6 in vehicular networks include neighbor discovery protocol, stateless address autoconfiguration, and DNS configuration for Internet connectivity. When a vehicle and an RSU have an internal network (respectively), the document discusses internetworking issues between two internal networks through either V2I or V2V communication. Those issues include prefix discovery, prefix exchange, service discovery, security, and privacy.

Copyright Notice

Table of Contents

1. Introduction 3
2. Requirements Language 4
3. Terminology 4
4. Overview 5
5. Internetworking between Vehicle Network and RSU Network . . . 6
  5.1. V2I-Based Internetworking 6
  5.2. The Use Cases of V2I-Based Internetworking 8
6. Internetworking between Two Vehicle Networks 8
  6.1. V2V-Based Internetworking 8
  6.2. The Use Cases of V2V-Based Internetworking 9
7. IPv6 Addressing 10
8. Neighbor Discovery 10
9. IP Address Autoconfiguration 11
10. DNS Naming Service 11
11. IP Mobility Management 12
12. Service Discovery 12
13. Security Considerations 13
14. Contributors 13
15. Acknowledgments 13
16. References 14
  16.1. Normative References 14
  16.2. Informative References 15

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 VANET, Dedicated Short-Range Communications (DSRC) [DSRC-WAVE] was standardized as Wireless Access in Vehicular Environments (WAVE) standards by IEEE. The WAVE standards include IEEE 802.11p [IEEE-802.11p] for WAVE Media Access Control (MAC) and Physical Layer (PHY), IEEE 1609.0 for WAVE architecture [WAVE-1609.0], IEEE 1609.2 for WAVE security services [WAVE-1609.2], IEEE 1609.3 for WAVE networking services [WAVE-1609.3], and IEEE 1609.4 for WAVE multi-channel operation [WAVE-1609.4]. 802.11p extends IEEE 802.11a [IEEE-802.11a] by consideration of vehicular characteristics such as a vehicle's velocity and collision avoidance. IEEE 802.11p has been published as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012.

Now the deployment of VANET is indicated in 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) now consider automobiles as computer systems instead of mechanical machines, since many current vehicles are operating with many sensors and software. Google has advanced 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.

Vehicular networking research is enabling vehicles to communicate with each other and infrastructure nodes in the Internet by using TCP/IP, IP address autoconfiguration, routing, handover, and mobility management [ID-VN-Survey]. IPv6 [RFC2460] is suitable for vehicular networks since the protocol has abundant address space and autoconfiguration features, and can be extended by way of new protocol headers.

This document identifies issues of IPv6-based vehicle-to-infrastructure (V2I) networking and vehicle-to-vehicle (V2V) networking, such as IPv6 addressing [RFC4291], neighbor discovery [RFC4861], address autoconfiguration [RFC4862], and DNS naming service [RFC8106][RFC3646][ID-DNSNA]. This document also identifies issues of internetworking between two internal networks when a vehicle and/or an RSU have an internal network. Those issues include prefix discovery, prefix exchange, and service discovery in the inter-connected internal networks. In addition, the document analyzes the characteristics of vehicular networks to consider the design of V2I or V2V 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, five new terms are defined below:

- Road-Side Unit (RSU): A node that has a wireless communication device (e.g., DSRC) to communicate with vehicles and is connected to the Internet as a router. An RSU is deployed either at an intersection or in a road segment.

- On-Board Unit (OBU): A node that has a wireless communication device (e.g., DSRC) to communicate with other OBUs and RSUs. An OBU is mounted on a vehicle. It is assumed that a Global Positioning System (GPS) is included in a vehicle with an OBU for efficient navigation.

- Fixed Network: An RSU can have an internal network consisting of multiple subnets. This internal network is a fixed network since the RSU is fixed in the road network.

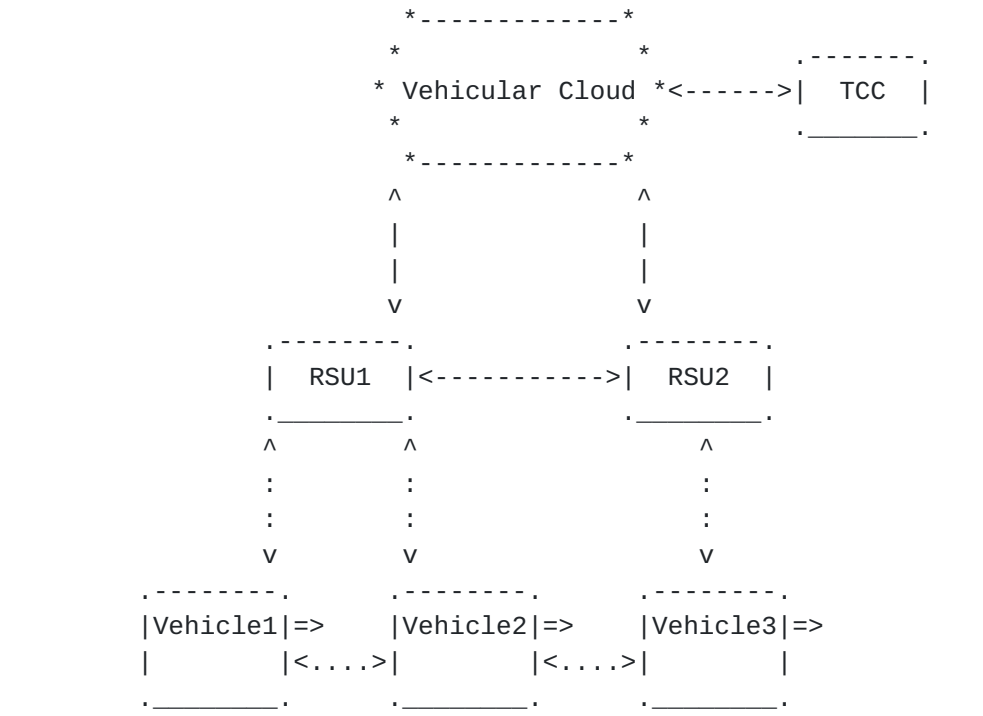
- Moving Network: A vehicle can have an internal network consisting of multiple subnets. This internal network is called a moving network since the vehicle is moving in the road network.

- 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 as a navigation path). TCC is included in a vehicular cloud for vehicular networks. Exemplary functions of TCC include the management of evacuation routes, the monitoring of pedestrians and bike traffic, the monitoring of real-time transit operations, and real-time responsive traffic signal systems. Thus, TCC is the nerve center of most freeway management sytems such that data is collected, processed, and fused with other operational and control data, and is also synthesized to produce "information" distributed to stakeholders, other agencies, and traveling public. TCC is called Traffic Management Center (TMC) in the US.

4. Overview

This document provides a problem statement of IPv6-based V2I and V2V networking. The main focus is one-hop networking between a vehicle and an RSU or between two neighboring vehicles. However, this document does not address all multi-hop networking scenarios of vehicles and RSUs. Also, the problems focus on the network layer (i.e., IPv6 protocol stack) rather than the MAC layer and the transport layer (e.g., TCP, UDP, and SCTP).

Figure 1 shows a network configuration for V2I and V2V networking in a road network. The two RSUs (RSU1 and RSU2) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. 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 V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication. Vehicle1 can communicate with Vehicle3 via RSU1 and RSU2 via V2I communication.



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

Figure 1: The Network Configuration for Vehicular Networking

5. Internetworking between Vehicle Network and RSU Network

This section discusses the internetworking between a vehicle's moving network and an RSU's fixed network.

5.1. V2I-Based Internetworking

As shown in Figure 2, the vehicle's moving network and the RSU's fixed network are internal networks having multiple subnets and having an edge router for the communication with another vehicle or RSU. The method of prefix assignment for each subnet inside the vehicle's mobile network and the RSU's fixed network is out of scope for this document. The internetworking between two internal networks via either V2I or V2V communication requires an exchange of network prefix and other parameters.

The network parameter discovery collects networking information for an IP communication between a vehicle and an RSU or between two neighboring vehicles, such as link layer, MAC layer, and IP layer information. The link layer information includes wireless link layer parameters, such as wireless media (e.g., IEEE 802.11 OCB, LTE D2D, Bluetooth, and LiFi) and a transmission power level. The MAC layer information includes the MAC address of an external network interface for the internetworking with another vehicle or RSU. The IP layer information includes the IP address and prefix of an external network interface for the internetworking with another vehicle or RSU.

Once the network parameter discovery and prefix exchange operations are performed, unicast of packets can be supported between the vehicle's moving network and the RSU's fixed network. The DNS naming service should be supported for the DNS name resolution for hosts or servers residing either in the vehicle's moving network or the RSU's fixed network.

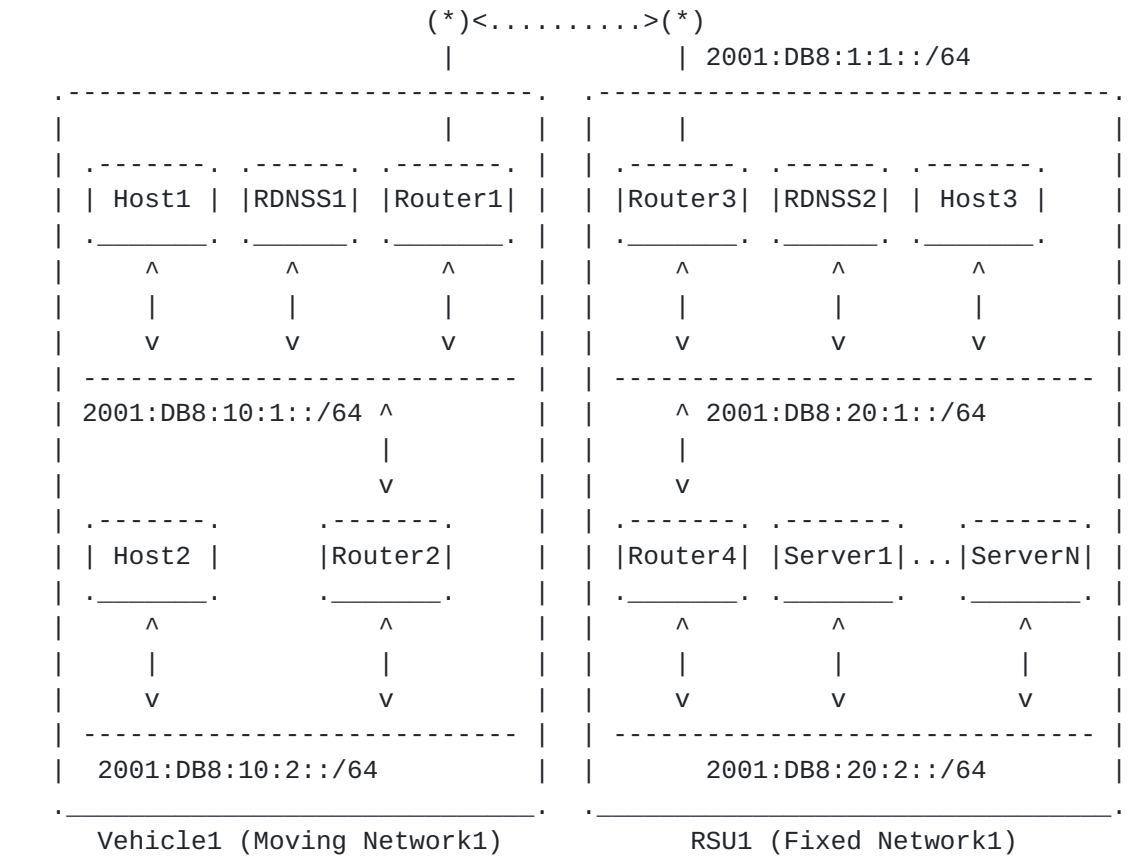


Figure 2: Internetworking between Vehicle Network and RSU Network

Figure 2 shows internetworking between the vehicle's moving network and the RSU's fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Fixed Network1) 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.

5.2. The Use Cases of V2I-Based Internetworking

The use cases for V2I networking include navigation service, fuel-efficient speed recommendation service, and accident notification service.

A navigation service, such as Self-Adaptive Interactive Navigation Tool [SAINT], using V2I networking interacts with TCC for the global road traffic optimization and can guide individual vehicles for appropriate navigation paths in real time.

A pedestrian protection service, such as Safety-Aware Navigation Application [SANA], using V2I networking can reduce the collision of a pedestrian and a vehicle, which have a smartphone, in a road network.

6. Internetworking between Two Vehicle Networks

This section discusses the internetworking between the moving networks of two neighboring vehicles.

6.1. V2V-Based Internetworking

In Figure 3, the prefix assignment for each subnet inside each vehicle's mobile network is done through a prefix delegation protocol.

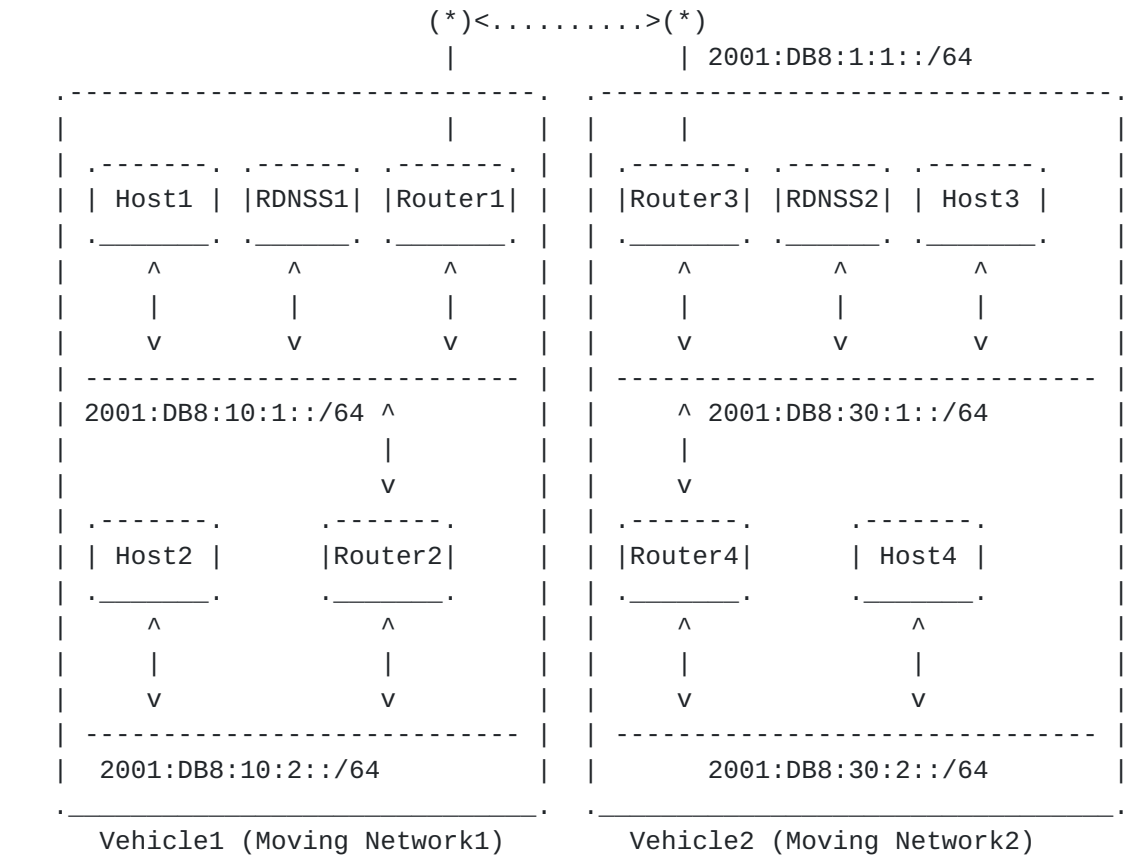


Figure 3: Internetworking between Two Vehicle Networks

Figure 3 shows internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (RDNSS2), the two hosts (Host3 and Host4), and the two routers (Router3 and Router4). Vehicle1's Router1 and Vehicle2's Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking.

This document describes the internetworking between the moving networks of two neighboring vehicles in Figure 3 and the required enhancement of IPv6 protocol suite for the V2V networking service.

6.2. The Use Cases of V2V-Based Internetworking

The use cases for V2V networking include context-aware navigator for driving safety, cooperative adaptive cruise control in an urban roadway, and platooning in a highway. These are three techniques

that will be important elements for self-driving.

Context-aware navigator can help drivers to drive safely by letting the drivers recognize dangerous obstacles and situations, including neighboring vehicles that might cause a collision [CASD].

Cooperative adaptive cruise control helps vehicles to adapt their speed autonomously according to the mobility of their predecessor and successor vehicles in an urban roadway.

Platooning allows a series of vehicles (e.g., trucks) to move together with a very short inter-distance. This platooning can maximize the throughput of vehicular traffic in a highway.

7. IPv6 Addressing

This section discusses IP addressing for the V2I and V2V networking. There are two approaches for IPv6 addressing in vehicular networks. The first is to use unique local IPv6 unicast addresses (ULAs) for vehicular networks [RFC4193]. The other is to use global IPv6 addresses for the interoperability with the Internet [RFC4291]. The former approach is often used by Mobile Ad Hoc Networks (MANET) for an isolated 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 global IP addresses, there are two choices: 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 layer-2 (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, each RSU plays the role of a (layer-3) router.

8. Neighbor Discovery

Neighbor Discovery (ND) is a core part of IPv6 protocol suite [RFC4861]. This section discusses an 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.

9. IP Address Autoconfiguration

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

To mitigate the impact of vehicle speed on address configuration, the RSU can perform IP address autoconfiguration including the DAD proactively as an ND proxy on behalf of the vehicles. If vehicles periodically report their movement information (e.g., position, trajectory, speed, and direction) to TCC, TCC can coordinate the 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. Mobile IPv6 (MIPv6) can be used for the fast update of a vehicle's care-of address for the current RSU to communicate with the vehicle [RFC6275].

10. DNS Naming Service

This section suggests a DNS naming service for V2I networking. The DNS naming service consists 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 located outside the VANET. 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.

11. IP Mobility Management

This section discusses an IP mobility support in V2I networking. In a single subnet per RSU, vehicles continually cross the communication coverages of adjacent RSUs. During this crossing, TCP/UDP sessions can be maintained through IP mobility support, such as MIPv6 [RFC6275], Proxy MIPv6 [RFC5213][RFC5949], and Distributed Mobility Management (DMM) [RFC7333][RFC7429]. Since vehicles move fast along roadways, high speed should be enabled by the parameter configuration in the IP mobility management. With the periodic reports of the movement 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 MIPv6, the high speed of vehicles should be considered for a parameter configuration in NEMO.

12. Service Discovery

Vehicles need to discover services (e.g., road condition notification, navigation service, and entertainment) 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.

13. Security Considerations

Security and privacy are paramount in the V2I and V2V networking in VANET. Only authorized vehicles should be allowed to use the V2I and V2V networking in VANET. A Vehicle Identification Number (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. Transport Layer Security (TLS) certificates can also 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 security and privacy can be supported for safe and reliable data services in vehicular networks.

To prevent an adversary from tracking a vehicle by with its MAC address or IPv6 address, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the communications between a vehicle and an RSU.

To protect packets exchanged between a vehicle and an RSU, packets should be encrypted. To assure confidentiality, efficient encryption and decryption algorithms can be used along with a key management scheme such as Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [Securing-VCOMM].

14. Contributors

IPWAVE is a group effort. The following people actively contributed to the problem statement text: Nabil Benamar (Moulay Ismail University), Sandra Cespedes (Universidad de Chile), Thierry Ernst (YoGoKo), Jerome Haerri (Eurecom), Richard Roy (MIT), and Francois Simon (Pilot).

15. Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2017R1B1A1B03035885). 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.

16. References

16.1. 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.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, March 2017.

[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.

[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.

16.2. 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.

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

[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 1609.2 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 1609.3 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services", IEEE Std 1609.3-2016, April 2016.

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

[ID-VN-Survey] Jeong, J., Ed., Cespedes, S., Benamar, N., Haerri, J., and M. Wetterwald, "Survey on IP-based Vehicular Networking for Intelligent Transportation Systems", draft-jeong-ipwave-vehicular-networking-survey-03 (work in progress), June 2017.

[ID-DNSNA] Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-00 (work in progress), March 2017.

[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-ipwave-vehicular-neighbor-discovery-00 (work in progress), March 2017.

[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.

[Securing-VCOMM] Fernandez, P., Santa, J., Bernal, F., and A. Skarmeta, "Securing Vehicular IPv6 Communications", IEEE Transactions on Dependable and Secure Computing, January 2016.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", RFC 4086, June 2005.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[SAINT] Jeong, J., Jeong, H., Lee, E., Oh, T., and D. Du, "SAINT: Self-Adaptive Interactive Navigation Tool for Cloud-Based Vehicular Traffic Optimization", IEEE Transactions on Vehicular Technology, Vol. 65, No. 6, June 2016.

[SANA] Hwang, T. and J. Jeong, "SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks", Springer Lecture Notes in Computer Science (LNCS), Vol. 9502, December 2015.

[CASD] Shen, Y., Jeong, J., Oh, T., and S. Son, "CASD: A Framework of Context-Awareness Safety Driving in Vehicular Networks", International Workshop on Device Centric Cloud (DC2), March 2016.

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

Alex
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
France

Phone: +33169089223
EMail: Alexandre.Petrescu@cea.fr

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

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

Phone: +86 13911788933
EMail: max.ldp@alibaba-inc.com

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4586
EMail: charliep@computer.org