Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 4, 2018

A. Petrescu
CEA, LIST
N. Benamar
Moulay Ismail University
J. Haerri
Eurecom
J. Lee
Sangmyung University
T. Ernst
YoGoKo

March 3, 2018

Transmission of IPv6 Packets over IEEE 802.11 Networks operating in mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB)

draft-ietf-ipwave-ipv6-over-80211ocb-21.txt

Abstract

In order to transmit IPv6 packets on IEEE 802.11 networks running outside the context of a basic service set (OCB, earlier "802.11p") there is a need to define a few parameters such as the supported Maximum Transmission Unit size on the 802.11-OCB link, the header format preceding the IPv6 header, the Type value within it, and others. This document describes these parameters for IPv6 and IEEE 802.11-OCB networks; it portrays the layering of IPv6 on 802.11-OCB similarly to other known 802.11 and Ethernet layers - by using an Ethernet Adaptation Layer.

Status of This Memo

Table of Contents

1. Introduction

This document describes the transmission of IPv6 packets on IEEE Std 802.11-OCB networks [IEEE-802.11-2016] (a.k.a "802.11p" see Appendix B). This involves the layering of IPv6 networking on top of the IEEE 802.11 MAC layer, with an LLC layer. Compared to running IPv6 over the Ethernet MAC layer, there is no modification expected to IEEE Std 802.11 MAC and Logical Link sublayers: IPv6 works fine directly over 802.11-OCB too, with an LLC layer.

The IPv6 network layer operates on 802.11-OCB in the same manner as operating on Ethernet, but there are two kinds of exceptions:

- Exceptions due to different operation of IPv6 network layer on 802.11 than on Ethernet. To satisfy these exceptions, this document describes an Ethernet Adaptation Layer between Ethernet headers and 802.11 headers. The Ethernet Adaptation Layer is described Section 4.2.1. The operation of IP on Ethernet is described in [RFC1042], [RFC2464] and [I-D.hinden-6man-rfc2464bis].

- Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure and handover behaviour. For security and privacy recommendations see Section 5 and Section 4.5. The subnet structure is described in Section 4.6. The handover behaviour on OCB links is not described in this document.

In the published literature, many documents describe aspects and problems related to running IPv6 over 802.11-OCB: [I-D.ietf-ipwave-vehicular-networking-survey].

2. Terminology

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].

IP-OBU (Internet Protocol On-Board Unit): an IP-OBU is a computer situated in a vehicle such as an automobile, bicycle, or similar. It has at least one IP interface that runs in mode OCB of 802.11, and that has an "OBU" transceiver. See the definition of the term "OBU" in section Appendix I.

IP-RSU (IP Road-Side Unit): an IP-RSU is situated along the road. An IP-RSU has at least two distinct IP-enabled interfaces; at least one interface is operated in mode OCB of IEEE 802.11 and is IP-enabled. An IP-RSU is similar to a Wireless Termination Point (WTP), as defined in [RFC5415], or an Access Point (AP), as defined in IEEE documents, or an Access Network Router (ANR) defined in [RFC3753], with one key particularity: the wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. The IP-RSU communicates with the IP-OBU in the vehicle over 802.11 wireless link operating in OCB mode.

OCB (outside the context of a basic service set - BSS): A mode of operation in which a STA is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality.

802.11-OCB: mode specified in IEEE Std 802.11-2016 when the MIB attribute dot11OCBActivited is true. Note: compliance with standards and regulations set in different countries when using the 5.9GHz frequency band is required.

3. Communication Scenarios where IEEE 802.11-OCB Links are Used

The IEEE 802.11-OCB Networks are used for vehicular communications, as ’Wireless Access in Vehicular Environments’. The IP communication scenarios for these environments have been described in several documents; in particular, we refer the reader to [I-D.ietf-ipwave-vehicular-networking-survey], that lists some scenarios and requirements for IP in Intelligent Transportation Systems.

The link model is the following: STA --- 802.11-OCB --- STA. In vehicular networks, STAs can be IP-RSUs and/or IP-OBUs. While 802.11-OCB is clearly specified, and the use of IPv6 over such link is not radically new, the operating environment (vehicular networks) brings in new perspectives.

The mechanisms for forming and terminating, discovering, peering and mobility management for 802.11-OCB links are not described in this document.

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

The default MTU for IP packets on 802.11-OCB MUST be 1500 octets. It is the same value as IPv6 packets on Ethernet links, as specified in [RFC2464]. This value of the MTU respects the recommendation that every link on the Internet must have a minimum MTU of 1280 octets (stated in [RFC8200], and the recommendations therein, especially with respect to fragmentation).

4.2. Frame Format

IP packets are transmitted over 802.11-OCB as standard Ethernet packets. As with all 802.11 frames, an Ethernet adaptation layer MUST be used with 802.11-OCB as well. This Ethernet Adaptation Layer performing 802.11-to-Ethernet is described in Section 4.2.1. The Ethernet Type code (EtherType) for IPv6 MUST be 0x86DD (hexadecimal 86DD, or otherwise #86DD).

The Frame format for transmitting IPv6 on 802.11-OCB networks MUST be the same as transmitting IPv6 on Ethernet networks, and is described in section 3 of [RFC2464].

4.2.1. Ethernet Adaptation Layer

An 'adaptation' layer is inserted between a MAC layer and the Networking layer. This is used to transform some parameters between their form expected by the IP stack and the form provided by the MAC layer.

An Ethernet Adaptation Layer makes an 802.11 MAC look to IP Networking layer as a more traditional Ethernet layer. At reception, this layer takes as input the IEEE 802.11 header and the Logical-Link Layer Control Header and produces an Ethernet II Header. At sending, the reverse operation is performed.

The operation of the Ethernet Adaptation Layer is depicted by the double arrow in Figure 1.

```
+------------------+-----------+------------+---------+-----------+
|  802.11 header   | LLC Header | IPv6 Header | Payload |.11 Trailer|
+------------------+-----------+------------+---------+-----------+
 \                             /                         \         /
   ---------------------------                             --------
             \---------------------------------------------/
                              ^
                              |
               802.11-to-Ethernet Adaptation Layer
                              |
                              v
+---------------------+------------+---------+
| Ethernet II Header  | IPv6 Header | Payload |
+---------------------+------------+---------+
```

Figure 1: Operation of the Ethernet Adaptation Layer

The Receiver and Transmitter Address fields in the 802.11 header MUST contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header MUST be the same as the value of the Type field in the Ethernet II Header.

The ".11 Trailer" contains solely a 4-byte Frame Check Sequence.

The specification of which type or subtype of 802.11 headers are used to transmit IP packets is left outside the scope of this document.

The placement of IPv6 networking layer on Ethernet Adaptation Layer is illustrated in Figure 2.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 IPv6                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Ethernet Adaptation Layer         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             802.11 MAC                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             802.11 PHY                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Ethernet Adaptation Layer stacked with other layers

(in the above figure, a 802.11 profile is represented; this is used also for 802.11 OCB profile.)

Other alternative views of layering are EtherType Protocol Discrimination (EPD), see Appendix E, and SNAP see [RFC1042].

4.3. Link-Local Addresses

The link-local address of an 802.11-OCB interface is formed in the same manner as on an Ethernet interface. This manner is described in section 5 of [RFC2464]. Additionally, if stable identifiers are needed, it is RECOMMENDED to follow the Recommendation on Stable IPv6 Interface Identifiers [RFC8064]. Additionally, if semantically opaque Interface Identifiers are needed, a potential method for generating semantically opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration is given in [RFC7217].

4.4. Address Mapping

Unicast and multicast address mapping MUST follow the procedures specified for Ethernet interfaces in sections 6 and 7 of [RFC2464].

4.4.1. Address Mapping -- Unicast

The procedure for mapping IPv6 unicast addresses into Ethernet link-layer addresses is described in [RFC4861].

4.4.2. Address Mapping -- Multicast

The multicast address mapping is performed according to the method specified in section 7 of [RFC2464]. The meaning of the value "3333" mentioned in that section 7 of [RFC2464] is defined in section 2.3.1 of [RFC7042].

Transmitting IPv6 packets to multicast destinations over 802.11 links proved to have some performance issues [I-D.perkins-intarea-multicast-ieee802]. These issues may be exacerbated in OCB mode. Solutions for these problems should consider the OCB mode of operation.

4.5. Stateless Autoconfiguration

The Interface Identifier for an 802.11-OCB interface is formed using the same rules as the Interface Identifier for an Ethernet interface; this is described in section 4 of [RFC2464]. No changes are needed, but some care must be taken when considering the use of the Stateless Address Auto-Configuration procedure.

The bits in the interface identifier have no generic meaning and the identifier should be treated as an opaque value. The bits 'Universal' and 'Group' in the identifier of an 802.11-OCB interface are significant, as this is an IEEE link-layer address. The details of this significance are described in [RFC7136].

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11-OCB interface may involve privacy, MAC address spoofing and IP address hijacking risks. A vehicle embarking an OBU or an IP-OBU whose egress interface is 802.11-OCB may expose itself to eavesdropping and subsequent correlation of data; this may reveal data considered private by the vehicle owner; there is a risk of being tracked; see the privacy considerations described in Appendix F.

If stable Interface Identifiers are needed in order to form IPv6 addresses on 802.11-OCB links, it is recommended to follow the recommendation in [RFC8064]. Additionally, if semantically opaque Interface Identifiers are needed, a potential method for generating semantically opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration is given in [RFC7217].

4.6. Subnet Structure

A subnet is formed by the external 802.11-OCB interfaces of vehicles that are in close range (not their on-board interfaces). This ephemeral subnet structure is strongly influenced by the mobility of vehicles: the 802.11 hidden node effects appear. On another hand, the structure of the internal subnets in each car is relatively stable.

The 802.11 networks in OCB mode may be considered as 'ad-hoc' networks. The addressing model for such networks is described in [RFC5889].

The operation of the Neighbor Discovery protocol (ND) over 802.11 OCB links is different than over 802.11 links. In OCB, the link layer does not ensure that all associated members receive all messages, because there is no association operation. The operation of ND over 802.11 OCB is not specified in this document.

The operation of the Mobile IPv6 protocol over 802.11 OCB links is different than on other links. The Movement Detection operation (section 11.5.1 of [RFC6275]) can not rely on Neighbor Unreachability Detection operation of the Neighbor Discovery protocol, for the reason mentioned in the previous paragraph. Also, the 802.11 OCB link layer is not a lower layer that can provide an indication that a link layer handover has occured. The operation of the Mobile IPv6 protocol over 802.11 OCB is not specified in this document.

5. Security Considerations

Any security mechanism at the IP layer or above that may be carried out for the general case of IPv6 may also be carried out for IPv6 operating over 802.11-OCB.

The OCB operation is stripped off of all existing 802.11 link-layer security mechanisms. There is no encryption applied below the network layer running on 802.11-OCB. At application layer, the IEEE 1609.2 document [IEEE-1609.2] does provide security services for certain applications to use; application-layer mechanisms are out-of-scope of this document. On another hand, a security mechanism provided at networking layer, such as IPsec [RFC4301], may provide data security protection to a wider range of applications.

802.11-OCB does not provide any cryptographic protection, because it operates outside the context of a BSS (no Association Request/ Response, no Challenge messages). Any attacker can therefore just sit in the near range of vehicles, sniff the network (just set the interface card's frequency to the proper range) and perform attacks without needing to physically break any wall. Such a link is less protected than commonly used links (wired link or protected 802.11).

The potential attack vectors are: MAC address spoofing, IP address and session hijacking and privacy violation.

Within the IPsec Security Architecture [RFC4301], the IPsec AH and ESP headers [RFC4302] and [RFC4303] respectively, its multicast extensions [RFC5374], HTTPS [RFC2818] and SeND [RFC3971] protocols can be used to protect communications. Further, the assistance of proper Public Key Infrastructure (PKI) protocols [RFC4210] is necessary to establish credentials. More IETF protocols are available in the toolbox of the IP security protocol designer. Certain ETSI protocols related to security protocols in Intelligent Transportation Systems are described in [ETSI-sec-archi].

As with all Ethernet and 802.11 interface identifiers, there may exist privacy risks in the use of 802.11-OCB interface identifiers. Moreover, in outdoors vehicular settings, the privacy risks are more important than in indoors settings. New risks are induced by the possibility of attacker sniffers deployed along routes which listen for IP packets of vehicles passing by. For this reason, in the 802.11-OCB deployments, there is a strong necessity to use protection tools such as dynamically changing MAC addresses. This may help mitigate privacy risks to a certain level. On another hand, it may have an impact in the way typical IPv6 address auto-configuration is performed for vehicles (SLAAC would rely on MAC addresses and would hence dynamically change the affected IP address), in the way the IPv6 Privacy addresses were used, and other effects.

6. IANA Considerations

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

Romain Kuntz contributed extensively about IPv6 handovers between links running outside the context of a BSS (802.11-OCB links).

Tim Leinmueller contributed the idea of the use of IPv6 over 802.11-OCB for distribution of certificates.

Marios Makassikis, Jose Santa Lozano, Albin Severinson and Alexey Voronov provided significant feedback on the experience of using IP messages over 802.11-OCB in initial trials.

Michelle Wetterwald contributed extensively the MTU discussion, offered the ETSI ITS perspective, and reviewed other parts of the document.

8. Acknowledgements

The authors would like to thank Witold Klaudel, Ryuji Wakikawa, Emmanuel Baccelli, John Kenney, John Moring, Francois Simon, Dan Romascanu, Konstantin Khait, Ralph Droms, Richard 'Dick' Roy, Ray Hunter, Tom Kurihara, Michal Sojka, Jan de Jongh, Suresh Krishnan, Dino Farinacci, Vincent Park, Jaehoon Paul Jeong, Gloria Gwynne, Hans-Joachim Fischer, Russ Housley, Rex Buddenberg, Erik Nordmark, Bob Moskowitz, Andrew Dryden, Georg Mayer, Dorothy Stanley, Sandra Cespedes, Mariano Falcitelli, Sri Gundavelli, Abdussalam Baryun, Margaret Cullen, Erik Kline, Carlos Jesus Bernardos Cano, Ronald in 't Velt, Katrin Sjoberg, Roland Bless and William Whyte. Their valuable comments clarified particular issues and generally helped to improve the document.

Pierre Pfister, Rostislav Lisovy, and others, wrote 802.11-OCB drivers for linux and described how.

For the multicast discussion, the authors would like to thank Owen DeLong, Joe Touch, Jen Linkova, Erik Kline, Brian Haberman and participants to discussions in network working groups.

The authors would like to thank participants to the Birds-of-a-Feather "Intelligent Transportation Systems" meetings held at IETF in 2016.

9. References

9.1. Normative References

[RFC1042] Postel, J. and J. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", STD 43, RFC 1042, DOI 10.17487/RFC1042, February 1988, <https://www.rfc-editor.org/info/rfc1042>.

[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>.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <https://www.rfc-editor.org/info/rfc2464>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <https://www.rfc-editor.org/info/rfc3753>.

[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>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, DOI 10.17487/RFC4210, September 2005, <https://www.rfc-editor.org/info/rfc4210>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[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>.

[RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, DOI 10.17487/RFC5374, November 2008, <https://www.rfc-editor.org/info/rfc5374>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[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>.

[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>.

[RFC7042] Eastlake 3rd, D. and J. Abley, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 7042, DOI 10.17487/RFC7042, October 2013, <https://www.rfc-editor.org/info/rfc7042>.

[RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <https://www.rfc-editor.org/info/rfc7136>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <https://www.rfc-editor.org/info/rfc7721>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[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>.

9.2. Informative References

[ETSI-sec-archi] "ETSI TS 102 940 V1.2.1 (2016-11), ETSI Technical Specification, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, November 2016. Downloaded on September 9th, 2017, freely available from ETSI website at URL http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf".

[I-D.hinden-6man-rfc2464bis] Crawford, M. and R. Hinden, "Transmission of IPv6 Packets over Ethernet Networks", draft-hinden-6man-rfc2464bis-02 (work in progress), March 2017.

[I-D.ietf-ipwave-vehicular-networking-survey] Jeong, J., Cespedes, S., Benamar, N., Haerri, J., and M. Wetterwald, "Survey on IP-based Vehicular Networking for Intelligent Transportation Systems", draft-ietf-ipwave-vehicular-networking-survey-00 (work in progress), July 2017.

[I-D.perkins-intarea-multicast-ieee802]
Perkins, C., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-perkins-intarea-multicast-ieee802-03 (work in progress), July 2017.

[IEEE-1609.2]
"IEEE SA - 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Security Services for Applications and Management Messages. Example URL http://ieeexplore.ieee.org/document/7426684/ accessed on August 17th, 2017.".

[IEEE-1609.3]
"IEEE SA - 1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services. Example URL http://ieeexplore.ieee.org/document/7458115/ accessed on August 17th, 2017.".

[IEEE-1609.4]
"IEEE SA - 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation. Example URL http://ieeexplore.ieee.org/document/7435228/ accessed on August 17th, 2017.".

[IEEE-802.11-2016]
"IEEE Standard 802.11-2016 - IEEE Standard for Information Technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Status - Active Standard. Description retrieved freely on September 12th, 2017, at URL https://standards.ieee.org/findstds/standard/802.11-2016.html".

[IEEE-802.11p-2010]
"IEEE Std 802.11p (TM)-2010, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments; document freely available at URL http://standards.ieee.org/getieee802/download/802.11p-2010.pdf retrieved on September 20th, 2013.".

Appendix A. ChangeLog

The changes are listed in reverse chronological order, most recent changes appearing at the top of the list.

From draft-ietf-ipwave-ipv6-over-80211ocb-20 to draft-ietf-ipwave-ipv6-over-80211ocb-21

- o Corrected a few nits and added names in Acknowledgments section.
- o Removed unused reference to old Internet Draft tsvwg about QoS.

From draft-ietf-ipwave-ipv6-over-80211ocb-19 to draft-ietf-ipwave-ipv6-over-80211ocb-20

- o Reduced the definition of term "802.11-OCB".
- o Left out of this specification which 802.11 header to use to transmit IP packets in OCB mode (QoS Data header, Data header, or any other).
- o Added 'MUST' use an Ethernet Adaptation Layer, instead of 'is using' an Ethernet Adaptation Layer.

From draft-ietf-ipwave-ipv6-over-80211ocb-18 to draft-ietf-ipwave-ipv6-over-80211ocb-19

- o Removed the text about fragmentation.
- o Removed the mentioning of WSMP and GeoNetworking.
- o Removed the explanation of the binary representation of the EtherType.
- o Rendered normative the paragraph about unicast and multicast address mapping.
- o Removed paragraph about addressing model, subnet structure and easiness of using LLs.
- o Clarified the Type/Subtype field in the 802.11 Header.
- o Used RECOMMENDED instead of recommended, for the stable interface identifiers.

From draft-ietf-ipwave-ipv6-over-80211ocb-17 to draft-ietf-ipwave-ipv6-over-80211ocb-18

o Improved the MTU and fragmentation paragraph.

From draft-ietf-ipwave-ipv6-over-80211ocb-16 to draft-ietf-ipwave-ipv6-over-80211ocb-17

o Susbtituted "MUST be increased" to "is increased" in the MTU section, about fragmentation.

From draft-ietf-ipwave-ipv6-over-80211ocb-15 to draft-ietf-ipwave-ipv6-over-80211ocb-16

o Removed the definition of the 'WiFi' term and its occurences. Clarified a phrase that used it in Appendix C "Aspects introduced by the OCB mode to 802.11".

o Added more normative words: MUST be 0x86DD, MUST fragment if size larger than MTU, Sequence number in 802.11 Data header MUST be increased.

From draft-ietf-ipwave-ipv6-over-80211ocb-14 to draft-ietf-ipwave-ipv6-over-80211ocb-15

o Added normative term MUST in two places in section "Ethernet Adaptation Layer".

From draft-ietf-ipwave-ipv6-over-80211ocb-13 to draft-ietf-ipwave-ipv6-over-80211ocb-14

o Created a new Appendix titled "Extra Terminology" that contains terms DSRC, DSRCS, OBU, RSU as defined outside IETF. Some of them are used in the main Terminology section.

o Added two paragraphs explaining that ND and Mobile IPv6 have problems working over 802.11 OCB, yet their adaptations is not specified in this document.

From draft-ietf-ipwave-ipv6-over-80211ocb-12 to draft-ietf-ipwave-ipv6-over-80211ocb-13

o Substituted "IP-OBU" for "OBRU", and "IP-RSU" for "RSRU" throughout and improved OBU-related definitions in the Terminology section.

From draft-ietf-ipwave-ipv6-over-80211ocb-11 to draft-ietf-ipwave-ipv6-over-80211ocb-12

- o Improved the appendix about "MAC Address Generation" by expressing the technique to be an optional suggestion, not a mandatory mechanism.

From draft-ietf-ipwave-ipv6-over-80211ocb-10 to draft-ietf-ipwave-ipv6-over-80211ocb-11

- o Shortened the paragraph on forming/terminating 802.11-OCB links.

- o Moved the draft tsvwg-ieee-802-11 to Informative References.

From draft-ietf-ipwave-ipv6-over-80211ocb-09 to draft-ietf-ipwave-ipv6-over-80211ocb-10

- o Removed text requesting a new Group ID for multicast for OCB.

- o Added a clarification of the meaning of value "3333" in the section Address Mapping -- Multicast.

- o Added note clarifying that in Europe the regional authority is not ETSI, but "ECC/CEPT based on ENs from ETSI".

- o Added note stating that the manner in which two STAtions set their communication channel is not described in this document.

- o Added a time qualifier to state that the "each node is represented uniquely at a certain point in time."

- o Removed text "This section may need to be moved" (the "Reliability Requirements" section). This section stays there at this time.

- o In the term definition "802.11-OCB" added a note stating that "any implementation should comply with standards and regulations set in the different countries for using that frequency band."

- o In the RSU term definition, added a sentence explaining the difference between RSU and RSRU: in terms of number of interfaces and IP forwarding.

- o Replaced "with at least two IP interfaces" with "with at least two real or virtual IP interfaces".

- o Added a term in the Terminology for "OBU". However the definition is left empty, as this term is defined outside IETF.

- o Added a clarification that it is an OBU or an OBRU in this phrase "A vehicle embarking an OBU or an OBRU".

- Checked the entire document for a consistent use of terms OBU and OBRU.

- Added note saying that "’p’ is a letter identifying the Ammendment".

- Substituted lower case for capitals SHALL or MUST in the Appendices.

- Added reference to RFC7042, helpful in the 3333 explanation. Removed reference to individual submission draft-petrescu-its-scenario-reqs and added reference to draft-ietf-ipwave-vehicular-networking-survey.

- Added figure captions, figure numbers, and references to figure numbers instead of ’below’. Replaced "section Section" with "section" throughout.

- Minor typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-08 to draft-ietf-ipwave-ipv6-over-80211ocb-09

- Significantly shortened the Address Mapping sections, by text copied from RFC2464, and rather referring to it.

- Moved the EPD description to an Appendix on its own.

- Shortened the Introduction and the Abstract.

- Moved the tutorial section of OCB mode introduced to .11, into an appendix.

- Removed the statement that suggests that for routing purposes a prefix exchange mechanism could be needed.

- Removed refs to RFC3963, RFC4429 and RFC6775; these are about ND, MIP/NEMO and oDAD; they were referred in the handover discussion section, which is out.

- Updated a reference from individual submission to now a WG item in IPWAVE: the survey document.

- Added term definition for WiFi.

- Updated the authorship and expanded the Contributors section.

- Corrected typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-07 to draft-ietf-ipwave-ipv6-over-80211ocb-08

- Removed the per-channel IPv6 prohibition text.

- Corrected typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-06 to draft-ietf-ipwave-ipv6-over-80211ocb-07

- Added new terms: OBRU and RSRU ('R' for Router). Refined the existing terms RSU and OBU, which are no longer used throughout the document.

- Improved definition of term "802.11-OCB".

- Clarified that OCB does not "strip" security, but that the operation in OCB mode is "stripped off of all .11 security".

- Clarified that theoretical OCB bandwidth speed is 54mbits, but that a commonly observed bandwidth in IP-over-OCB is 12mbit/s.

- Corrected typographical errors, and improved some phrasing.

From draft-ietf-ipwave-ipv6-over-80211ocb-05 to draft-ietf-ipwave-ipv6-over-80211ocb-06

- Updated references of 802.11-OCB document from -2012 to the IEEE 802.11-2016.

- In the LL address section, and in SLAAC section, added references to 7217 opaque IIDs and 8064 stable IIDs.

From draft-ietf-ipwave-ipv6-over-80211ocb-04 to draft-ietf-ipwave-ipv6-over-80211ocb-05

- Lengthened the title and cleanded the abstract.

- Added text suggesting LLs may be easy to use on OCB, rather than GUAs based on received prefix.

- Added the risks of spoofing and hijacking.

- Removed the text speculation on adoption of the TSA message.

- Clarified that the ND protocol is used.

- Clarified what it means "No association needed".

- o Added some text about how two STAs discover each other.

- o Added mention of external (OCB) and internal network (stable), in the subnet structure section.

- o Added phrase explaining that both .11 Data and .11 QoS Data headers are currently being used, and may be used in the future.

- o Moved the packet capture example into an Appendix Implementation Status.

- o Suggested moving the reliability requirements appendix out into another document.

- o Added a IANA Consiserations section, with content, requesting for a new multicast group "all OCB interfaces".

- o Added new OBU term, improved the RSU term definition, removed the ETTC term, replaced more occurences of 802.11p, 802.11 OCB with 802.11-OCB.

- o References:

  * Added an informational reference to ETSI's IPv6-over-GeoNetworking.

  * Added more references to IETF and ETSI security protocols.

  * Updated some references from I-D to RFC, and from old RFC to new RFC numbers.

  * Added reference to multicast extensions to IPsec architecture RFC.

  * Added a reference to 2464-bis.

  * Removed FCC informative references, because not used.

- o Updated the affiliation of one author.

- o Reformulation of some phrases for better readability, and correction of typographical errors.

From draft-ietf-ipwave-ipv6-over-80211ocb-03 to draft-ietf-ipwave-ipv6-over-80211ocb-04

- o Removed a few informative references pointing to Dx draft IEEE 1609 documents.

- o Removed outdated informative references to ETSI documents.

- o Added citations to IEEE 1609.2, .3 and .4-2016.

- o Minor textual issues.

From draft-ietf-ipwave-ipv6-over-80211ocb-02 to draft-ietf-ipwave-ipv6-over-80211ocb-03

- o Keep the previous text on multiple addresses, so remove talk about MIP6, NEMOv6 and MCoA.

- o Clarified that a ’Beacon’ is an IEEE 802.11 frame Beacon.

- o Clarified the figure showing Infrastructure mode and OCB mode side by side.

- o Added a reference to the IP Security Architecture RFC.

- o Detailed the IPv6-per-channel prohibition paragraph which reflects the discussion at the last IETF IPWAVE WG meeting.

- o Added section "Address Mapping -- Unicast".

- o Added the ".11 Trailer" to pictures of 802.11 frames.

- o Added text about SNAP carrying the Ethertype.

- o New RSU definition allowing for it be both a Router and not necessarily a Router some times.

- o Minor textual issues.

From draft-ietf-ipwave-ipv6-over-80211ocb-01 to draft-ietf-ipwave-ipv6-over-80211ocb-02

- o Replaced almost all occurences of 802.11p with 802.11-OCB, leaving only when explanation of evolution was necessary.

- o Shortened by removing parameter details from a paragraph in the Introduction.

- o Moved a reference from Normative to Informative.

- o Added text in intro clarifying there is no handover spec at IEEE, and that 1609.2 does provide security services.

- o Named the contents the fields of the EthernetII header (including the Ethertype bitstring).

- o Improved relationship between two paragraphs describing the increase of the Sequence Number in 802.11 header upon IP fragmentation.

- o Added brief clarification of "tracking".

From draft-ietf-ipwave-ipv6-over-80211ocb-00 to draft-ietf-ipwave-ipv6-over-80211ocb-01

- o Introduced message exchange diagram illustrating differences between 802.11 and 802.11 in OCB mode.

- o Introduced an appendix listing for information the set of 802.11 messages that may be transmitted in OCB mode.

- o Removed appendix sections "Privacy Requirements", "Authentication Requirements" and "Security Certificate Generation".

- o Removed appendix section "Non IP Communications".

- o Introductory phrase in the Security Considerations section.

- o Improved the definition of "OCB".

- o Introduced theoretical stacked layers about IPv6 and IEEE layers including EPD.

- o Removed the appendix describing the details of prohibiting IPv6 on certain channels relevant to 802.11-OCB.

- o Added a brief reference in the privacy text about a precise clause in IEEE 1609.3 and .4.

- o Clarified the definition of a Road Side Unit.

- o Removed the discussion about security of WSA (because is non-IP).

- o Removed mentioning of the GeoNetworking discussion.

- o Moved references to scientific articles to a separate 'overview' draft, and referred to it.

Appendix B. 802.11p

The term "802.11p" is an earlier definition. The behaviour of "802.11p" networks is rolled in the document IEEE Std 802.11-2016. In that document the term 802.11p disappears. Instead, each 802.11p feature is conditioned by the Management Information Base (MIB) attribute "OCBActivated". Whenever OCBActivated is set to true the IEEE Std 802.11 OCB state is activated. For example, an 802.11 STAtion operating outside the context of a basic service set has the OCBActivated flag set. Such a station, when it has the flag set, uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

Appendix C. Aspects introduced by the OCB mode to 802.11

In the IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. At link layer, it is necessary to set the same channel number (or frequency) on two stations that need to communicate with each other. The manner in which stations set their channel number is not specified in this document. Stations STA1 and STA2 can exchange IP packets if they are set on the same channel. At IP layer, they then discover each other by using the IPv6 Neighbor Discovery protocol.

Briefly, the IEEE 802.11-OCB mode has the following properties:

- o The use by each node of a 'wildcard' BSSID (i.e., each bit of the BSSID is set to 1)
- o No IEEE 802.11 Beacon frames are transmitted
- o No authentication is required in order to be able to communicate
- o No association is needed in order to be able to communicate
- o No encryption is provided in order to be able to communicate
- o Flag dot11OCBActivated is set to true

All the nodes in the radio communication range (IP-OBU and IP-RSU) receive all the messages transmitted (IP-OBU and IP-RSU) within the radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

The message exchange diagram in Figure 3 illustrates a comparison between traditional 802.11 and 802.11 in OCB mode. The 'Data' messages can be IP packets such as HTTP or others. Other 802.11 management and control frames (non IP) may be transmitted, as specified in the 802.11 standard. For information, the names of these messages as currently specified by the 802.11 standard are listed in Appendix G.

```
   STA                    AP              STA1                    STA2
   |                       |               |                       |
   |<------ Beacon -------|               |<------ Data -------->|
   |                       |               |                       |
   |---- Probe Req. ----->|               |<------ Data -------->|
   |<--- Probe Res. ------|               |                       |
   |                       |               |<------ Data -------->|
   |---- Auth Req. ------>|               |                       |
   |<--- Auth Res. -------|               |<------ Data -------->|
   |                       |               |                       |
   |---- Asso Req. ------>|               |<------ Data -------->|
   |<--- Asso Res. -------|               |                       |
   |                       |               |<------ Data -------->|
   |<------ Data -------->|               |                       |
   |<------ Data -------->|               |<------ Data -------->|

      (i) 802.11 Infrastructure mode         (ii) 802.11-OCB mode
```

Figure 3: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

The interface 802.11-OCB was specified in IEEE Std 802.11p (TM) -2010 [IEEE-802.11p-2010] as an amendment to IEEE Std 802.11 (TM) -2007, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, this amendment has been integrated in IEEE 802.11(TM) -2012 and -2016 [IEEE-802.11-2016].

In document 802.11-2016, anything qualified specifically as "OCBActivated", or "outside the context of a basic service" set to be true, then it is actually referring to OCB aspects introduced to 802.11.

In order to delineate the aspects introduced by 802.11-OCB to 802.11, we refer to the earlier [IEEE-802.11p-2010]. The amendment is concerned with vehicular communications, where the wireless link is similar to that of Wireless LAN (using a PHY layer specified by 802.11a/b/g/n), but which needs to cope with the high mobility factor inherent in scenarios of communications between moving vehicles, and between vehicles and fixed infrastructure deployed along roads. While ’p’ is a letter identifying the Ammendment, just like ’a, b, g’ and ’n’ are, ’p’ is concerned more with MAC modifications, and a little with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a 'p' MAC with an 'a' PHY by operating outside the context of a BSS with OFDM at 5.4GHz and 5.9GHz.

The 802.11-OCB links are specified to be compatible as much as possible with the behaviour of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11-OCB MAC layer offers practically the same interface to IP as the 802.11a/b/g/n and 802.3. A packet sent by an IP-OBU may be received by one or multiple IP-RSUs. The link-layer resolution is performed by using the IPv6 Neighbor Discovery protocol.

To support this similarity statement (IPv6 is layered on top of LLC on top of 802.11-OCB, in the same way that IPv6 is layered on top of LLC on top of 802.11a/b/g/n (for WLAN) or layered on top of LLC on top of 802.3 (for Ethernet)) it is useful to analyze the differences between 802.11-OCB and 802.11 specifications. During this analysis, we note that whereas 802.11-OCB lists relatively complex and numerous changes to the MAC layer (and very little to the PHY layer), there are only a few characteristics which may be important for an implementation transmitting IPv6 packets on 802.11-OCB links.

The most important 802.11-OCB point which influences the IPv6 functioning is the OCB characteristic; an additional, less direct influence, is the maximum bandwidth afforded by the PHY modulation/demodulation methods and channel access specified by 802.11-OCB. The maximum bandwidth theoretically possible in 802.11-OCB is 54 Mbit/s (when using, for example, the following parameters: 20 MHz channel; modulation 64-QAM; coding rate R is 3/4); in practice of IP-over-802.11-OCB a commonly observed figure is 12Mbit/s; this bandwidth allows the operation of a wide range of protocols relying on IPv6.

o Operation Outside the Context of a BSS (OCB): the (earlier 802.11p) 802.11-OCB links are operated without a Basic Service Set (BSS). This means that the frames IEEE 802.11 Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always 0xffffffffffff (48 '1' bits, represented as MAC address ff:ff:ff:ff:ff:ff, or otherwise the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by administrator (e.g. 'My-Home-AccessPoint'). The OCB operation - namely the lack of beacon-based scanning and lack of authentication - should be taken into account when the Mobile IPv6 protocol [RFC6275] and the protocols for IP layer security [RFC4301] are used. The way these protocols adapt to OCB is not described in this document.

- Timing Advertisement: is a new message defined in 802.11-OCB, which does not exist in 802.11a/b/g/n. This message is used by stations to inform other stations about the value of time. It is similar to the time as delivered by a GNSS system (Galileo, GPS, ...) or by a cellular system. This message is optional for implementation.

- Frequency range: this is a characteristic of the PHY layer, with almost no impact on the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, ECC/CEPT based on ENs from ETSI, FCC, etc.); as part of the regulation process, specific applications are associated with specific frequency ranges. In the case of 802.11-OCB, the regulator associates a set of frequency ranges, or slots within a band, to the use of applications of vehicular communications, in a band known as "5.9GHz". The 5.9GHz band is different from the 2.4GHz and 5GHz bands used by Wireless LAN. However, as with Wireless LAN, the operation of 802.11-OCB in "5.9GHz" bands is exempt from owning a license in EU (in US the 5.9GHz is a licensed band of spectrum; for the fixed infrastructure an explicit FCC authorization is required; for an on-board device a 'licensed-by-rule' concept applies: rule certification conformity is required.) Technical conditions are different than those of the bands "2.4GHz" or "5GHz". The allowed power levels, and implicitly the maximum allowed distance between vehicles, is of 33dBm for 802.11-OCB (in Europe), compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to a maximum distance of approximately 1km, compared to approximately 50m. Additionally, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in US) and on the use of frequencies for Intelligent Transportation Systems (in EU), compared to Wireless LAN (802.11a/b/g/n).

- 'Half-rate' encoding: as the frequency range, this parameter is related to PHY, and thus has not much impact on the interface between the IP layer and the MAC layer.

- In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in Section 5. A relevant function is described in IEEE 1609.3-2016 [IEEE-1609.3], clause 5.5.1 and IEEE 1609.4-2016 [IEEE-1609.4], clause 6.7.

Other aspects particular to 802.11-OCB, which are also particular to 802.11 (e.g. the 'hidden node' operation), may have an influence on the use of transmission of IPv6 packets on 802.11-OCB networks. The OCB subnet structure is described in Section 4.6.

Appendix D. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver

The 802.11p amendment modifies both the 802.11 stack's physical and MAC layers but all the induced modifications can be quite easily obtained by modifying an existing 802.11a ad-hoc stack.

Conditions for a 802.11a hardware to be 802.11-OCB compliant:

- The PHY entity shall be an orthogonal frequency division multiplexing (OFDM) system. It must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11-OCB layer, in France: 5875MHz to 5925MHz.

- The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.

- The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).

- The chip should be able to transmit up to 44.8 dBm when used by the US government in the United States, and up to 33 dBm in Europe; other regional conditions apply.

Changes needed on the network stack in OCB mode:

- Physical layer:

  * The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.

  * The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).

  * The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules, if used by the kernel to enforce local specific restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

MAC layer:

* All management frames (beacons, join, leave, and others) emission and reception must be disabled except for frames of subtype Action and Timing Advertisement (defined below).

* No encryption key or method must be used.

* Packet emission and reception must be performed as in ad-hoc mode, using the wildcard BSSID (ff:ff:ff:ff:ff:ff).

* The functions related to joining a BSS (Association Request/ Response) and for authentication (Authentication Request/Reply, Challenge) are not called.

* The beacon interval is always set to 0 (zero).

* Timing Advertisement frames, defined in the amendment, should be supported. The upper layer should be able to trigger such frames emission and to retrieve information contained in received Timing Advertisements.

Appendix E. EtherType Protocol Discrimination (EPD)

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated in Figure 4. The IP layer operates on top of the EtherType Protocol Discrimination (EPD); this Discrimination layer is described in IEEE Std 802.3-2012; the interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 IPv6                    |
+-+-+-+-+-+-{           }+-+-+-+-+-+-+-+-+
            {   LLC_SAP  }                  802.11-OCB
+-+-+-+-+-+-{           }+-+-+-+-+-+-+-+-+  Boundary
|            EPD         |       |       |
|                        | MLME  |       |
+-+-+-{  MAC_SAP   }+-+-+-|  MLME_SAP    |
|      MAC Sublayer      |       |       |  802.11-OCB
|     and ch. coord.     |       | SME   |  Services
+-+-+-{   PHY_SAP  }+-+-+-+-+-+-+-|      |
|                        | PLME  |       |
|            PHY Layer   |   PLME_SAP    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4: EtherType Protocol Discrimination

Appendix F. Design Considerations

The networks defined by 802.11-OCB are in many ways similar to other networks of the 802.11 family. In theory, the encapsulation of IPv6 over 802.11-OCB could be very similar to the operation of IPv6 over other networks of the 802.11 family. However, the high mobility, strong link asymmetry and very short connection makes the 802.11-OCB link significantly different from other 802.11 networks. Also, the automotive applications have specific requirements for reliability, security and privacy, which further add to the particularity of the 802.11-OCB link.

F.1. Vehicle ID

In automotive networks it is required that each node is represented uniquely at a certain point in time. Accordingly, a vehicle must be identified by at least one unique identifier. The current specification at ETSI and at IEEE 1609 identifies a vehicle by its MAC address, which is obtained from the 802.11-OCB Network Interface Card (NIC).

In case multiple 802.11-OCB NICs are present in one car, implicitely multiple vehicle IDs will be generated. Additionally, some software generates a random MAC address each time the computer boots; this constitutes an additional difficulty.

A mechanim to uniquely identify a vehicle irrespectively to the multiplicity of NICs, or frequent MAC address generation, is necessary.

F.2. Reliability Requirements

The dynamically changing topology, short connectivity, mobile transmitter and receivers, different antenna heights, and many-to-many communication types, make IEEE 802.11-OCB links significantly different from other IEEE 802.11 links. Any IPv6 mechanism operating on IEEE 802.11-OCB link must support strong link asymmetry, spatio-temporal link quality, fast address resolution and transmission.

IEEE 802.11-OCB strongly differs from other 802.11 systems to operate outside of the context of a Basic Service Set. This means in practice that IEEE 802.11-OCB does not rely on a Base Station for all Basic Service Set management. In particular, IEEE 802.11-OCB shall not use beacons. Any IPv6 mechanism requiring L2 services from IEEE 802.11 beacons must support an alternative service.

Channel scanning being disabled, IPv6 over IEEE 802.11-OCB must implement a mechanism for transmitter and receiver to converge to a common channel.

Authentication not being possible, IPv6 over IEEE 802.11-OCB must implement an distributed mechanism to authenticate transmitters and receivers without the support of a DHCP server.

Time synchronization not being available, IPv6 over IEEE 802.11-OCB must implement a higher layer mechanism for time synchronization between transmitters and receivers without the support of a NTP server.

The IEEE 802.11-OCB link being asymmetric, IPv6 over IEEE 802.11-OCB must disable management mechanisms requesting acknowledgements or replies.

The IEEE 802.11-OCB link having a short duration time, IPv6 over IEEE 802.11-OCB should implement fast IPv6 mobility management mechanisms.

F.3. Multiple interfaces

There are considerations for 2 or more IEEE 802.11-OCB interface cards per vehicle. For each vehicle taking part in road traffic, one IEEE 802.11-OCB interface card could be fully allocated for Non IP safety-critical communication. Any other IEEE 802.11-OCB may be used for other type of traffic.

The mode of operation of these other wireless interfaces is not clearly defined yet. One possibility is to consider each card as an independent network interface, with a specific MAC Address and a set of IPv6 addresses. Another possibility is to consider the set of these wireless interfaces as a single network interface (not including the IEEE 802.11-OCB interface used by Non IP safety critical communications). This will require specific logic to ensure, for example, that packets meant for a vehicle in front are actually sent by the radio in the front, or that multiple copies of the same packet received by multiple interfaces are treated as a single packet. Treating each wireless interface as a separate network interface pushes such issues to the application layer.

Certain privacy requirements imply that if these multiple interfaces are represented by many network interface, a single renumbering event shall cause renumbering of all these interfaces. If one MAC changed and another stayed constant, external observers would be able to correlate old and new values, and the privacy benefits of randomization would be lost.

The privacy requirements of Non IP safety-critical communications imply that if a change of pseudonyme occurs, renumbering of all other interfaces shall also occur.

F.4. MAC Address Generation

In 802.11-OCB networks, the MAC addresses may change during well defined renumbering events. A 'randomized' MAC address has the following characteristics:

- Bit "Local/Global" set to "locally admninistered".
- Bit "Unicast/Multicast" set to "Unicast".
- The 46 remaining bits are set to a random value, using a random number generator that meets the requirements of [RFC4086].

To meet the randomization requirements for the 46 remaining bits, a hash function may be used. For example, the SHA256 hash function may be used with input a 256 bit local secret, the "nominal" MAC Address of the interface, and a representation of the date and time of the renumbering event.

Appendix G. IEEE 802.11 Messages Transmitted in OCB mode

For information, at the time of writing, this is the list of IEEE 802.11 messages that may be transmitted in OCB mode, i.e. when dot11OCBActivated is true in a STA:

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;

o The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;

o The STA may send data frames of subtype Data, Null, QoS Data, and QoS Null.

Appendix H. Implementation Status

This section describes an example of an IPv6 Packet captured over a IEEE 802.11-OCB link.

By way of example we show that there is no modification in the headers when transmitted over 802.11-OCB networks - they are transmitted like any other 802.11 and Ethernet packets.

We describe an experiment of capturing an IPv6 packet on an 802.11-OCB link. In topology depicted in Figure 5, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11-OCB interface. The packet is captured on the Host, using a network protocol analyzer (e.g. Wireshark); the capture is performed in two different modes: direct mode and 'monitor' mode. The topology used during the capture is depicted below.

The packet is captured on the Host. The Host is an IP-OBU containing an 802.11 interface in format PCI express (an ITRI product). The kernel runs the ath5k software driver with modifications for OCB mode. The capture tool is Wireshark. The file format for save and analyze is 'pcap'. The packet is generated by the Router. The Router is an IP-RSU (ITRI product).

```
      +--------+                                +-------+
      |        |        802.11-OCB Link         |       |
   ---| Router |--------------------------------| Host  |
      |        |                                |       |
      +--------+                                +-------+
```

Figure 5: Topology for capturing IP packets on 802.11-OCB

During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

H.1. Capture in Monitor Mode

The IPv6 RA packet captured in monitor mode is illustrated below. The radio tap header provides more flexibility for reporting the characteristics of frames. The Radiotap Header is prepended by this particular stack and operating system on the Host machine to the RA packet received from the network (the Radiotap Header is not present on the air). The implementation-dependent Radiotap Header is useful for piggybacking PHY information from the chip's registers as data in a packet understandable by userland applications using Socket interfaces (the PHY interface can be, for example: power levels, data rate, ratio of signal to noise).

The packet present on the air is formed by IEEE 802.11 Data Header, Logical Link Control Header, IPv6 Base Header and ICMPv6 Header.

```
Radiotap Header v0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Header Revision|  Header Pad   |    Header length               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Present flags                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data Rate     |             Pad                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

IEEE 802.11 Data Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type/Subtype and Frame Ctrl  |          Duration              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Receiver Address...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... Receiver Address            |      Transmitter Address...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... Transmitter Address                                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             BSS Id...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... BSS Id                     |  Frag Number and Seq Number   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Logical-Link Control Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
      |      DSAP   |I|     SSAP    |C| Control field | Org. code...
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       ... Organizational Code        |             Type              |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

      IPv6 Base Header
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |Version| Traffic Class |           Flow Label                  |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |         Payload Length        |  Next Header  |   Hop Limit   |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                                                               |
      +                                                               +
      |                                                               |
      +                         Source Address                        +
      |                                                               |
      +                                                               +
      |                                                               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                                                               |
      +                                                               +
      |                                                               |
      +                      Destination Address                      +
      |                                                               |
      +                                                               +
      |                                                               |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

      Router Advertisement
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |     Type      |     Code      |          Checksum             |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      | Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         Reachable Time                        |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                          Retrans Timer                        |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |   Options ...
      +-+-+-+-+-+-+-+-+-+-+-+-+-
```

The value of the Data Rate field in the Radiotap header is set to 6 Mb/s. This indicates the rate at which this RA was received.

The value of the Transmitter address in the IEEE 802.11 Data Header is set to a 48bit value. The value of the destination address is 33:33:00:00:00:1 (all-nodes multicast address). The value of the BSS

Id field is ff:ff:ff:ff:ff:ff, which is recognized by the network protocol analyzer as being "broadcast". The Fragment number and sequence number fields are together set to 0x90C6.

The value of the Organization Code field in the Logical-Link Control Header is set to 0x0, recognized as "Encapsulated Ethernet". The value of the Type field is 0x86DD (hexadecimal 86DD, or otherwise #86DD), recognized as "IPv6".

A Router Advertisement is periodically sent by the router to multicast group address ff02::1. It is an icmp packet type 134. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags, as described in [RFC4861].

The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1. Recent versions of network protocol analyzers (e.g. Wireshark) provide additional informations for an IP address, if a geolocalization database is present. In this example, the geolocalization database is absent, and the "GeoIP" information is set to unknown for both source and destination addresses (although the IPv6 source and destination addresses are set to useful values). This "GeoIP" can be a useful information to look up the city, country, AS number, and other information for an IP address.

The Ethernet Type field in the logical-link control header is set to 0x86dd which indicates that the frame transports an IPv6 packet. In the IEEE 802.11 data, the destination address is 33:33:00:00:00:01 which is the corresponding multicast MAC address. The BSS id is a broadcast address of ff:ff:ff:ff:ff:ff. Due to the short link duration between vehicles and the roadside infrastructure, there is no need in IEEE 802.11-OCB to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11-OCB enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.

H.2. Capture in Normal Mode

The same IPv6 Router Advertisement packet described above (monitor mode) is captured on the Host, in the Normal mode, and depicted below.

```
Ethernet II Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Destination...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
...Destination                  |           Source...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
...Source                                                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Type                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

IPv6 Base Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Router Advertisement
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Reachable Time                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Retrans Timer                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...
+-+-+-+-+-+-+-+-+-+-+-+-
```

One notices that the Radiotap Header, the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On the other hand, a new header named Ethernet II Header is present.

The Destination and Source addresses in the Ethernet II header contain the same values as the fields Receiver Address and Transmitter Address present in the IEEE 802.11 Data Header in the "monitor" mode capture.

The value of the Type field in the Ethernet II header is 0x86DD (recognized as "IPv6"); this value is the same value as the value of the field Type in the Logical-Link Control Header in the "monitor" mode capture.

The knowledgeable experimenter will no doubt notice the similarity of this Ethernet II Header with a capture in normal mode on a pure Ethernet cable interface.

An Adaptation layer is inserted on top of a pure IEEE 802.11 MAC layer, in order to adapt packets, before delivering the payload data to the applications. It adapts 802.11 LLC/MAC headers to Ethernet II headers. In further detail, this adaptation consists in the elimination of the Radiotap, 802.11 and LLC headers, and in the insertion of the Ethernet II header. In this way, IPv6 runs straight over LLC over the 802.11-OCB MAC layer; this is further confirmed by the use of the unique Type 0x86DD.

Appendix I. Extra Terminology

The following terms are defined outside the IETF. They are used to define the main terms in the main terminology section Section 2.

DSRC (Dedicated Short Range Communication): a term defined outside the IETF. The US Federal Communications Commission (FCC) Dedicated Short Range Communication (DSRC) is defined in the Code of Federal Regulations (CFR) 47, Parts 90 and 95. This Code is referred in the definitions below. At the time of the writing of this Internet Draft, the last update of this Code was dated October 1st, 2010.

DSRCS (Dedicated Short-Range Communications Services): a term defined outside the IETF. The use of radio techniques to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments. DSRCS systems may also transmit status and instructional messages related to the units involve. [Ref. 47 CFR 90.7 - Definitions]

OBU (On-Board Unit): a term defined outside the IETF. An On-Board Unit is a DSRCS transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of the respective chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of the respective chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands. - [CFR 90.7 - Definitions].

RSU (Road-Side Unit): a term defined outside of IETF. A Roadside Unit is a DSRC transceiver that is mounted along a road or pedestrian passageway. An RSU may also be mounted on a vehicle or is hand carried, but it may only operate when the vehicle or hand- carried unit is stationary. Furthermore, an RSU operating under the respectgive part is restricted to the location where it is licensed to operate. However, portable or hand-held RSUs are permitted to operate where they do not interfere with a site-licensed operation. A RSU broadcasts data to OBUs or exchanges data with OBUs in its communications zone. An RSU also provides channel assignments and operating instructions to OBUs in its communications zone, when required. - [CFR 90.7 - Definitions].

Authors' Addresses

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

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

Nabil Benamar
Moulay Ismail University
Morocco

Phone: +212670832236
Email: n.benamar@est.umi.ac.ma

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

Phone: +33493008134
Email: Jerome.Haerri@eurecom.fr

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan 31066
Republic of Korea

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr

IPWAVE Working Group   N. Benamar
Internet-Draft   Moulay Ismail University of Meknes
Intended status: Standards Track   J. Haerri
Expires: February 10, 2020   Eurecom
                                                                  J. Lee
                                                    Sangmyung University
                                                                T. Ernst
                                                                  YoGoKo
                                                          August 9, 2019

Basic Support for IPv6 over IEEE Std 802.11 Networks Operating Outside the Context of a Basic Service Set

draft-ietf-ipwave-ipv6-over-80211ocb-52

Abstract

This document provides methods and settings, for using IPv6 to communicate among nodes within range of one another over a single IEEE 802.11-OCB link. Support for these methods and settings require minimal changes to existing stacks. This document also describes limitations associated with using these methods. Optimizations and usage of IPv6 over more complex scenarios is not covered in this specification and is subject of future work.

Table of Contents

1. Introduction

This document provides a baseline for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link [IEEE-802.11-2016] (a.k.a., "802.11p" see Appendix A, Appendix B and Appendix C) with minimal changes to existing stacks. Moreover, the document identifies limitations of such usage. Concretely, the document describes the layering of IPv6 networking on top of the IEEE Std 802.11 MAC layer or an IEEE Std 802.3 MAC layer with a frame translation underneath. The resulting stack is derived from IPv6 over Ethernet [RFC2464], but operates over 802.11-OCB to provide at least P2P (Point to Point) connectivity using IPv6 ND and link-local addresses.

The IPv6 network layer operates on 802.11-OCB in the same manner as operating on Ethernet with the following exceptions:

- Exceptions due to different operation of IPv6 network layer on 802.11 than on Ethernet. The operation of IP on Ethernet is described in [RFC1042] and [RFC2464].

- Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure and movement detection. Security and privacy recommendations are discussed in Section 5 and Section 4.4. The subnet structure is described in Section 4.6. The movement detection on OCB links is not described in this document. Likewise, ND Extensions and IPWAVE optimizations for vehicular communications are not in scope. The expectation is that further specifications will be edited to cover more complex vehicular networking scenarios.

The reader may refer to [I-D.ietf-ipwave-vehicular-networking] for an overview of problems related to running IPv6 over 802.11-OCB. It is out of scope of this document to reiterate those.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The document makes uses of the following terms: IP-OBU (Internet Protocol On-Board Unit): an IP-OBU denotes a computer situated in a vehicle such as a car, bicycle, or similar. It has at least one IP interface that runs in mode OCB of 802.11, and that has an "OBU" transceiver. See the definition of the term "OBU" in section Appendix H.

IP-RSU (IP Road-Side Unit): an IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. An IP-RSU communicates with the IP-OBU in the vehicle over 802.11 wireless link operating in OCB mode. An IP-RSU is similar to an Access Network Router (ANR) defined in [RFC3753], and a Wireless Termination Point (WTP) defined in [RFC5415].

OCB (outside the context of a basic service set - BSS): is a mode of operation in which a STA is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality.

802.11-OCB: refers to the mode specified in IEEE Std 802.11-2016 when the MIB attribute dot11OCBActivited is 'true'.

3. Communication Scenarios where IEEE 802.11-OCB Links are Used

The IEEE 802.11-OCB networks are used for vehicular communications, as 'Wireless Access in Vehicular Environments'. In particular, we refer the reader to [I-D.ietf-ipwave-vehicular-networking], that lists some scenarios and requirements for IP in Intelligent Transportation Systems (ITS).

The link model is the following: STA --- 802.11-OCB --- STA. In vehicular networks, STAs can be IP-RSUs and/or IP-OBUs. All links are assumed to be P2P and multiple links can be on one radio interface. While 802.11-OCB is clearly specified, and a legacy IPv6 stack can operate on such links, the use of the operating environment (vehicular networks) brings in new perspectives.

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

The default MTU for IP packets on 802.11-OCB is inherited from [RFC2464] and is, as such, 1500 octets. As noted in [RFC8200], every link on the Internet must have a minimum MTU of 1280 octets, as well as follow the other recommendations, especially with regard to fragmentation.

4.2. Frame Format

IP packets MUST be transmitted over 802.11-OCB media as QoS Data frames whose format is specified in IEEE 802.11 spec [IEEE-802.11-2016].

The IPv6 packet transmitted on 802.11-OCB are immediately preceded by a Logical Link Control (LLC) header and an 802.11 header. In the LLC header, and in accordance with the EtherType Protocol Discrimination (EPD, see Appendix D), the value of the Type field MUST be set to 0x86DD (IPv6). The mapping to the 802.11 data service SHOULD use a 'priority' value of 1 (QoS with a 'Background' user priority), reserving higher priority values for safety-critical and time-sensitive traffic, including the ones listed in [ETSI-sec-archi].

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers MAY implement IPv6-over-Ethernet as per [RFC2464] and then a frame translation from 802.3 to 802.11 in order to minimize the code changes.

4.3. Link-Local Addresses

There are several types of IPv6 addresses [RFC4291], [RFC4193], that may be assigned to an 802.11-OCB interface. Among these types of addresses only the IPv6 link-local addresses can be formed using an EUI-64 identifier, in particular during transition time, (the time spent before an interface starts using a different address than the LL one).

If the IPv6 link-local address is formed using an EUI-64 identifier, then the mechanism of forming that address is the same mechanism as used to form an IPv6 link-local address on Ethernet links. Moreover, whether or not the interface identifier is derived from the EUI-64 identifier, its length is 64 bits as is the case for Ethernet [RFC2464].

4.4. Stateless Autoconfiguration

The steps a host takes in deciding how to autoconfigure its interfaces in IPv6 are described in [RFC4862]. This section describes the formation of Interface Identifiers for IPv6 addresses of type 'Global' or 'Unique Local'. Interface Identifiers for IPv6 address of type 'Link-Local' are discussed in Section 4.3.

The RECOMMENDED method for forming stable Interface Identifiers (IIDs) is described in [RFC8064]. The method of forming IIDs described in Section 4 of [RFC2464] MAY be used during transition time, in particular for IPv6 link-local addresses. Regardless of how to form the IID, its length is 64 bits, similarely to IPv6 over Ethernet [RFC2464].

The bits in the IID have no specific meaning and the identifier should be treated as an opaque value. The bits 'Universal' and 'Group' in the identifier of an 802.11-OCB interface are significant, as this is an IEEE link-layer address. The details of this significance are described in [RFC7136].

Semantically opaque IIDs, instead of meaningful IIDs derived from a valid and meaningful MAC address ([RFC2464], Section 4), help avoid certain privacy risks (see the risks mentioned in Section 5.1.1). If semantically opaque IIDs are needed, they may be generated using the method for generating semantically opaque IIDs with IPv6 Stateless Address Autoconfiguration given in [RFC7217]. Typically, an opaque IID is formed starting from identifiers different than the MAC addresses, and from cryptographically strong material. Thus, privacy sensitive information is absent from Interface IDs, because it is impossible to calculate back the initial value from which the Interface ID was first generated.

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose IIDs don't change too often. It is RECOMMENDED to use the mechanisms described in RFC 7217 to permit the use of Stable IIDs that do not change within one subnet prefix. A possible source for the Net-Iface Parameter is a virtual interface name, or logical interface name, that is decided by a local administrator.

4.5. Address Mapping

Unicast and multicast address mapping MUST follow the procedures specified for Ethernet interfaces specified in Sections 6 and 7 of [RFC2464].

4.5.1. Address Mapping -- Unicast

This document is scoped for Address Resolution (AR) and Duplicate Address Detection (DAD) per [RFC4862].

4.5.2. Address Mapping -- Multicast

The multicast address mapping is performed according to the method specified in section 7 of [RFC2464]. The meaning of the value "3333" mentioned there is defined in section 2.3.1 of [RFC7042].

Transmitting IPv6 packets to multicast destinations over 802.11 links proved to have some performance issues [I-D.ietf-mboned-ieee802-mcast-problems]. These issues may be exacerbated in OCB mode. A future improvement to this specification should consider solutions for these problems.

4.6. Subnet Structure

When vehicles are in close range, a subnet may be formed over 802.11-OCB interfaces (not by their in-vehicle interfaces). A Prefix List conceptual data structure ([RFC4861] Section 5.1) is maintained for each 802.11-OCB interface.

IPv6 Neighbor Discovery protocol (ND) requires reflexive properties (bidirectional connectivity) which is generally, though not always, the case for P2P OCB links. IPv6 ND also requires transitive properties for DAD and AR, so an IPv6 subnet can be mapped on an OCB network only if all nodes in the network share a single physical broadcast domain. The extension to IPv6 ND operating on a subnet that covers multiple OCB links and not fully overlapping (NBMA) is not in scope. Finally, IPv6 ND requires a permanent connectivity of all nodes in the subnet to defend their addresses, in other words very stable network conditions.

The structure of this subnet is ephemeral, in that it is strongly influenced by the mobility of vehicles: the hidden terminal effects appear; the 802.11 networks in OCB mode may be considered as 'ad-hoc' networks with an addressing model as described in [RFC5889]. On another hand, the structure of the internal subnets in each vehicle is relatively stable.

As recommended in [RFC5889], when the timing requirements are very strict (e.g., fast-drive-through IP-RSU coverage), no on-link subnet prefix should be configured on an 802.11-OCB interface. In such cases, the exclusive use of IPv6 link-local addresses is RECOMMENDED.

Additionally, even if the timing requirements are not very strict (e.g., the moving subnet formed by two following vehicles is stable, a fixed IP-RSU is absent), the subnet is disconnected from the Internet (i.e., a default route is absent), and the addressing peers are equally qualified (that is, it is impossible to determine that some vehicle owns and distributes addresses to others) the use of link-local addresses is RECOMMENDED.

The baseline ND protocol [RFC4861] MUST be supported over 802.11-OCB links. Transmitting ND packets may prove to have some performance issues as mentioned in Section 4.5.2, and Appendix I. These issues may be exacerbated in OCB mode. Solutions for these problems should consider the OCB mode of operation. Future solutions to OCB should consider solutions for avoiding broadcast. The best of current knowledge indicates the kinds of issues that may arise with ND in OCB mode; they are described in Appendix I.

Protocols like Mobile IPv6 [RFC6275] , [RFC3963] and DNAv6 [RFC6059], which depend on a timely movement detection, might need additional tuning work to handle the lack of link-layer notifications during handover. This is for further study.

5. Security Considerations

Any security mechanism at the IP layer or above that may be carried out for the general case of IPv6 may also be carried out for IPv6 operating over 802.11-OCB.

The OCB operation does not use existing 802.11 link-layer security mechanisms. There is no encryption applied below the network layer running on 802.11-OCB. At the application layer, the IEEE 1609.2 document [IEEE-1609.2] provides security services for certain applications to use; application-layer mechanisms are out of scope of this document. On another hand, a security mechanism provided at networking layer, such as IPsec [RFC4301], may provide data security protection to a wider range of applications.

802.11-OCB does not provide any cryptographic protection, because it operates outside the context of a BSS (no Association Request/ Response, no Challenge messages). Therefore, an attacker can sniff or inject traffic while within range of a vehicle or IP-RSU (by setting an interface card's frequency to the proper range). Also, an attacker may not heed to legal limits for radio power and can use a very sensitive directional antenna; if attackers wishe to attack a given exchange they do not necessarily need to be in close physical proximity. Hence, such a link is less protected than commonly used links (wired link or aforementioned 802.11 links with link-layer security).

Therefore, any node can join a subnet, directly communicate with any nodes on the subset to include potentially impersonating another node. This design allows for a number of threats outlined in Section 3 of [RFC6959]. While not widely deployed, SeND [RFC3971], [RFC3972] is a solution that can address Spoof-Based Attack Vectors.

5.1. Privacy Considerations

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11-OCB interface may involve privacy, MAC address spoofing and IP hijacking risks. A vehicle embarking an IP-

OBU whose egress interface is 802.11-OCB may expose itself to eavesdropping and subsequent correlation of data. This may reveal data considered private by the vehicle owner; there is a risk of being tracked. In outdoors public environments, where vehicles typically circulate, the privacy risks are more important than in indoors settings. It is highly likely that attacker sniffers are deployed along routes which listen for IEEE frames, including IP packets, of vehicles passing by. For this reason, in the 802.11-OCB deployments, there is a strong necessity to use protection tools such as dynamically changing MAC addresses Section 5.2, semantically opaque Interface Identifiers and stable Interface Identifiers Section 4.4. An example of change policy is to change the MAC address of the OCB interface each time the system boots up. This may help mitigate privacy risks to a certain level. Furthermore, for privacy concerns, ([RFC8065]) recommends using an address generation scheme rather than addresses generated from a fixed link-layer address. However, there are some specificities related to vehicles. Since roaming is an important characteristic of moving vehicles, the use of the same Link-Local Address over time can indicate the presence of the same vehicle in different places and thus leads to location tracking. Hence, a vehicle should get hints about a change of environment (e.g. , engine running, GPS, etc..) and renew the IID in its LLAs.

5.1.1. Privacy Risks of Meaningful info in Interface IDs

The privacy risks of using MAC addresses displayed in Interface Identifiers are important. The IPv6 packets can be captured easily in the Internet and on-link in public roads. For this reason, an attacker may realize many attacks on privacy. One such attack on 802.11-OCB is to capture, store and correlate Company ID information present in MAC addresses of many cars (e.g. listen for Router Advertisements, or other IPv6 application data packets, and record the value of the source address in these packets). Further correlation of this information with other data captured by other means, or other visual information (car color, others) may constitute privacy risks.

5.2. MAC Address and Interface ID Generation

In 802.11-OCB networks, the MAC addresses may change during well defined renumbering events. In the moment the MAC address is changed on an 802.11-OCB interface all the Interface Identifiers of IPv6 addresses assigned to that interface MUST change.

Implementations should use a policy dictating when the MAC address is changed on the 802.11-OCB interface. For more information on the motivation of this policy please refer to the privacy discussion in Appendix B.

A 'randomized' MAC address has the following characteristics:

- Bit "Local/Global" set to "locally administered".

- Bit "Unicast/Multicast" set to "Unicast".

- The 46 remaining bits are set to a random value, using a random number generator that meets the requirements of [RFC4086].

To meet the randomization requirements for the 46 remaining bits, a hash function may be used. For example, the [SHA256] hash function may be used with input a 256 bit local secret, the 'nominal' MAC Address of the interface, and a representation of the date and time of the renumbering event.

A randomized Interface ID has the same characteristics of a randomized MAC address, except the length in bits.

5.3. Pseudonymization impact on confidentiality and trust

Vehicles 'and drivers' privacy relies on pseudonymization mechanisms such as the ones described in Section 5.2. This pseudonymization means that upper-layer protocols and applications SHOULD NOT rely on layer-2 or layer-3 addresses to assume that the other participant can be trusted.

6. IANA Considerations

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

Romain Kuntz contributed extensively about IPv6 handovers between links running outside the context of a BSS (802.11-OCB links).

Tim Leinmueller contributed the idea of the use of IPv6 over 802.11-OCB for distribution of certificates.

Marios Makassikis, Jose Santa Lozano, Albin Severinson and Alexey Voronov provided significant feedback on the experience of using IP messages over 802.11-OCB in initial trials.

Michelle Wetterwald contributed extensively the MTU discussion, offered the ETSI ITS perspective, and reviewed other parts of the document.

8. Acknowledgements

The authors would like to thank Alexandre Petrescu for initiating this work and for being the lead author until the version 43 of this draft.

The authors would like to thank Pascal Thubert for reviewing, proofreading and suggesting modifications of this document.

The authors would like to thank Mohamed Boucadair for proofreading and suggesting modifications of this document.

The authors would like to thank Eric Vyncke for reviewing suggesting modifications of this document.

The authors would like to thank Witold Klaudel, Ryuji Wakikawa, Emmanuel Baccelli, John Kenney, John Moring, Francois Simon, Dan Romascanu, Konstantin Khait, Ralph Droms, Richard 'Dick' Roy, Ray Hunter, Tom Kurihara, Michal Sojka, Jan de Jongh, Suresh Krishnan, Dino Farinacci, Vincent Park, Jaehoon Paul Jeong, Gloria Gwynne, Hans-Joachim Fischer, Russ Housley, Rex Buddenberg, Erik Nordmark, Bob Moskowitz, Andrew Dryden, Georg Mayer, Dorothy Stanley, Sandra Cespedes, Mariano Falcitelli, Sri Gundavelli, Abdussalam Baryun, Margaret Cullen, Erik Kline, Carlos Jesus Bernardos Cano, Ronald in 't Velt, Katrin Sjoberg, Roland Bless, Tijink Jasja, Kevin Smith, Brian Carpenter, Julian Reschke, Mikael Abrahamsson, Dirk von Hugo, Lorenzo Colitti, Pascal Thubert, Ole Troan, Jinmei Tatuya, Joel Halpern, Eric Gray and William Whyte. Their valuable comments clarified particular issues and generally helped to improve the document.

Pierre Pfister, Rostislav Lisovy, and others, wrote 802.11-OCB drivers for linux and described how.

For the multicast discussion, the authors would like to thank Owen DeLong, Joe Touch, Jen Linkova, Erik Kline, Brian Haberman and participants to discussions in network working groups.

The authors would like to thank participants to the Birds-of-a-Feather "Intelligent Transportation Systems" meetings held at IETF in 2016.

Human Rights Protocol Considerations review by Amelia Andersdotter.

9. References

9.1. Normative References

[IEEE-802.11-2016]
"IEEE Standard 802.11-2016 - IEEE Standard for Information Technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Status - Active Standard. Description retrieved freely; the document itself is also freely available, but with some difficulty (requires registration); description and document retrieved on April 8th, 2019, starting from URL https://standards.ieee.org/findstds/standard/802.11-2016.html".

[RFC1042] Postel, J. and J. Reynolds, "Standard for the transmission of IP datagrams over IEEE 802 networks", STD 43, RFC 1042, DOI 10.17487/RFC1042, February 1988, <https://www.rfc-editor.org/info/rfc1042>.

[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>.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <https://www.rfc-editor.org/info/rfc2464>.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, DOI 10.17487/RFC4086, June 2005, <https://www.rfc-editor.org/info/rfc4086>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[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>.

[RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley, Ed., "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, DOI 10.17487/RFC5415, March 2009, <https://www.rfc-editor.org/info/rfc5415>.

[RFC6059] Krishnan, S. and G. Daley, "Simple Procedures for Detecting Network Attachment in IPv6", RFC 6059, DOI 10.17487/RFC6059, November 2010, <https://www.rfc-editor.org/info/rfc6059>.

[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>.

[RFC7042] Eastlake 3rd, D. and J. Abley, "IANA Considerations and IETF Protocol and Documentation Usage for IEEE 802 Parameters", BCP 141, RFC 7042, DOI 10.17487/RFC7042, October 2013, <https://www.rfc-editor.org/info/rfc7042>.

[RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136, February 2014, <https://www.rfc-editor.org/info/rfc7136>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

9.2. Informative References

[ETSI-sec-archi] "ETSI TS 102 940 V1.2.1 (2016-11), ETSI Technical Specification, Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management, November 2016. Downloaded on September 9th, 2017, freely available from ETSI website at URL http://www.etsi.org/deliver/etsi_ts/102900_102999/102940/01.02.01_60/ts_102940v010201p.pdf".

[I-D.ietf-ipwave-vehicular-networking] Jeong, J., "IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", draft-ietf-ipwave-vehicular-networking-11 (work in progress), July 2019.

[I-D.ietf-mboned-ieee802-mcast-problems] Perkins, C., McBride, M., Stanley, D., Kumari, W., and J. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-ietf-mboned-ieee802-mcast-problems-07 (work in progress), July 2019.

[IEEE-1609.2] "IEEE SA - 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Security Services for Applications and Management Messages. Example URL http://ieeexplore.ieee.org/document/7426684/ accessed on August 17th, 2017.".

[IEEE-1609.3] "IEEE SA - 1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Networking Services. Example URL http://ieeexplore.ieee.org/document/7458115/ accessed on August 17th, 2017.".

[IEEE-1609.4]
"IEEE SA - 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) -- Multi-Channel Operation. Example URL http://ieeexplore.ieee.org/document/7435228/ accessed on August 17th, 2017.".

[IEEE-802.11p-2010]
"IEEE Std 802.11p (TM)-2010, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments; document freely available at URL http://standards.ieee.org/getieee802/ download/802.11p-2010.pdf retrieved on September 20th, 2013.".

[RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004, <https://www.rfc-editor.org/info/rfc3753>.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, DOI 10.17487/RFC3963, January 2005, <https://www.rfc-editor.org/info/rfc3963>.

[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>.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <https://www.rfc-editor.org/info/rfc3972>.

[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>.

[RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address Validation Improvement (SAVI) Threat Scope", RFC 6959, DOI 10.17487/RFC6959, May 2013, <https://www.rfc-editor.org/info/rfc6959>.

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <https://www.rfc-editor.org/info/rfc7721>.

[RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <https://www.rfc-editor.org/info/rfc8065>.

[SHA256] "Secure Hash Standard (SHS), National Institute of Standards and Technology. https://csrc.nist.gov/CSRC/media/Publications/fips/180/2/archive/2002-08-01/documents/fips180-2.pdf".

Appendix A. 802.11p

The term "802.11p" is an earlier definition. The behaviour of "802.11p" networks is rolled in the document IEEE Std 802.11-2016. In that document the term 802.11p disappears. Instead, each 802.11p feature is conditioned by the IEEE Management Information Base (MIB) attribute "OCBActivated" [IEEE-802.11-2016]. Whenever OCBActivated is set to true the IEEE Std 802.11-OCB state is activated. For example, an 802.11 STAtion operating outside the context of a basic service set has the OCBActivated flag set. Such a station, when it has the flag set, uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

Appendix B. Aspects introduced by the OCB mode to 802.11

In the IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. In OCB mode, the manner in which channels are selected and used is simplified compared to when in BSS mode. Contrary to BSS mode, at link layer, it is necessary to set statically the same channel number (or frequency) on two stations that need to communicate with each other (in BSS mode this channel set operation is performed automatically during 'scanning'). The manner in which stations set their channel number in OCB mode is not specified in this document. Stations STA1 and STA2 can exchange IP packets only if they are set on the same channel. At IP layer, they then discover each other by using the IPv6 Neighbor Discovery protocol. The allocation of a particular channel for a particular use is defined statically in standards authored by ETSI (in Europe), FCC in America, and similar organisations in South Korea, Japan and other parts of the world.

Briefly, the IEEE 802.11-OCB mode has the following properties:

o The use by each node of a 'wildcard' BSSID (i.e., each bit of the BSSID is set to 1)

o No IEEE 802.11 Beacon frames are transmitted

o No authentication is required in order to be able to communicate

o No association is needed in order to be able to communicate

o No encryption is provided in order to be able to communicate

o Flag dot11OCBActivated is set to true

All the nodes in the radio communication range (IP-OBU and IP-RSU) receive all the messages transmitted (IP-OBU and IP-RSU) within the radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

The message exchange diagram in Figure 1 illustrates a comparison between traditional 802.11 and 802.11 in OCB mode. The 'Data' messages can be IP packets such as HTTP or others. Other 802.11 management and control frames (non IP) may be transmitted, as specified in the 802.11 standard. For information, the names of these messages as currently specified by the 802.11 standard are listed in Appendix F.

```
      STA                    AP               STA1                   STA2
      |                      |                |                      |
      |<------ Beacon -------|                |<------ Data -------->|
      |                      |                |                      |
      |---- Probe Req. ----->|                |<------ Data -------->|
      |<--- Probe Res. ------|                |                      |
      |                      |                |<------ Data -------->|
      |---- Auth Req. ------>|                |                      |
      |<--- Auth Res. -------|                |<------ Data -------->|
      |                      |                |                      |
      |---- Asso Req. ------>|                |<------ Data -------->|
      |<--- Asso Res. -------|                |                      |
      |                      |                |<------ Data -------->|
      |<------ Data -------->|                |                      |
      |<------ Data -------->|                |<------ Data -------->|

         (i) 802.11 Infrastructure mode         (ii) 802.11-OCB mode
```

Figure 1: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

The interface 802.11-OCB was specified in IEEE Std 802.11p (TM) -2010 [IEEE-802.11p-2010] as an amendment to IEEE Std 802.11 (TM) -2007, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, this amendment has been integrated in IEEE 802.11(TM) -2012 and -2016 [IEEE-802.11-2016].

In document 802.11-2016, anything qualified specifically as "OCBActivated", or "outside the context of a basic service" set to be true, then it is actually referring to OCB aspects introduced to 802.11.

In order to delineate the aspects introduced by 802.11-OCB to 802.11, we refer to the earlier [IEEE-802.11p-2010]. The amendment is concerned with vehicular communications, where the wireless link is similar to that of Wireless LAN (using a PHY layer specified by 802.11a/b/g/n), but which needs to cope with the high mobility factor inherent in scenarios of communications between moving vehicles, and between vehicles and fixed infrastructure deployed along roads. While 'p' is a letter identifying the Amendment, just like 'a, b, g' and 'n' are, 'p' is concerned more with MAC modifications, and a little with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a 'p' MAC with an 'a' PHY by operating outside the context of a BSS with OFDM at 5.4GHz and 5.9GHz.

The 802.11-OCB links are specified to be compatible as much as possible with the behaviour of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11-OCB MAC layer offers practically the same interface to IP as the 802.11a/b/g/n and 802.3. A packet sent by an IP-OBU may be received by one or multiple IP-RSUs. The link-layer resolution is performed by using the IPv6 Neighbor Discovery protocol.

To support this similarity statement (IPv6 is layered on top of LLC on top of 802.11-OCB, in the same way that IPv6 is layered on top of LLC on top of 802.11a/b/g/n (for WLAN) or layered on top of LLC on top of 802.3 (for Ethernet)) it is useful to analyze the differences between 802.11-OCB and 802.11 specifications. During this analysis, we note that whereas 802.11-OCB lists relatively complex and numerous changes to the MAC layer (and very little to the PHY layer), there are only a few characteristics which may be important for an implementation transmitting IPv6 packets on 802.11-OCB links.

The most important 802.11-OCB point which influences the IPv6 functioning is the OCB characteristic; an additional, less direct influence, is the maximum bandwidth afforded by the PHY modulation/ demodulation methods and channel access specified by 802.11-OCB. The maximum bandwidth theoretically possible in 802.11-OCB is 54 Mbit/s (when using, for example, the following parameters: 20 MHz channel; modulation 64-QAM; coding rate R is 3/4); in practice of IP-over-802.11-OCB a commonly observed figure is 12Mbit/s; this bandwidth allows the operation of a wide range of protocols relying on IPv6.

o Operation Outside the Context of a BSS (OCB): the (earlier 802.11p) 802.11-OCB links are operated without a Basic Service Set (BSS). This means that the frames IEEE 802.11 Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always 0xffffffffffff (48 '1' bits, represented as MAC address ff:ff:ff:ff:ff:ff, or otherwise the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by administrator (e.g. 'My-Home-AccessPoint'). The OCB operation - namely the lack of beacon-based scanning and lack of authentication - should be taken into account when the Mobile IPv6 protocol [RFC6275] and the protocols for IP layer security [RFC4301] are used. The way these protocols adapt to OCB is not described in this document.

o Timing Advertisement: is a new message defined in 802.11-OCB, which does not exist in 802.11a/b/g/n. This message is used by stations to inform other stations about the value of time. It is similar to the time as delivered by a GNSS system (Galileo, GPS, ...) or by a cellular system. This message is optional for implementation.

o Frequency range: this is a characteristic of the PHY layer, with almost no impact on the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, ECC/CEPT based on ENs from ETSI, FCC, etc.); as part of the regulation process, specific applications are associated with specific frequency ranges. In the case of 802.11-OCB, the regulator associates a set of frequency ranges, or slots within a band, to the use of applications of vehicular communications, in a band known as "5.9GHz". The 5.9GHz band is different from the 2.4GHz and 5GHz bands used by Wireless LAN. However, as with Wireless LAN, the operation of 802.11-OCB in "5.9GHz" bands is exempt from owning a license in EU (in US the 5.9GHz is a licensed band of spectrum; for the fixed infrastructure an explicit FCC authorization is required; for an on-board device a 'licensed-by-rule' concept applies: rule certification conformity is required.) Technical conditions are different than those of the bands "2.4GHz" or "5GHz". The allowed power levels, and implicitly the maximum allowed distance between vehicles, is of 33dBm for 802.11-OCB (in Europe), compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to a maximum distance of approximately 1km, compared to approximately 50m.

Additionally, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in US) and on the use of frequencies for Intelligent Transportation Systems (in EU), compared to Wireless LAN (802.11a/b/g/n).

- 'Half-rate' encoding: as the frequency range, this parameter is related to PHY, and thus has not much impact on the interface between the IP layer and the MAC layer.

- In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in Section 5. A relevant function is described in documents IEEE 1609.3-2016 [IEEE-1609.3] and IEEE 1609.4-2016 [IEEE-1609.4].

Appendix C. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver

The 802.11p amendment modifies both the 802.11 stack's physical and MAC layers but all the induced modifications can be quite easily obtained by modifying an existing 802.11a ad-hoc stack.

Conditions for a 802.11a hardware to be 802.11-OCB compliant:

- The PHY entity shall be an orthogonal frequency division multiplexing (OFDM) system. It must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11-OCB layer, in France: 5875MHz to 5925MHz.

- The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.

- The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).

- The chip should be able to transmit up to 44.8 dBm when used by the US government in the United States, and up to 33 dBm in Europe; other regional conditions apply.

Changes needed on the network stack in OCB mode:

o Physical layer:

* The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.

* The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).

* The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules, if used by the kernel to enforce local specific restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

MAC layer:

* All management frames (beacons, join, leave, and others) emission and reception must be disabled except for frames of subtype Action and Timing Advertisement (defined below).

* No encryption key or method must be used.

* Packet emission and reception must be performed as in ad-hoc mode, using the wildcard BSSID (ff:ff:ff:ff:ff:ff).

* The functions related to joining a BSS (Association Request/ Response) and for authentication (Authentication Request/Reply, Challenge) are not called.

* The beacon interval is always set to 0 (zero).

* Timing Advertisement frames, defined in the amendment, should be supported. The upper layer should be able to trigger such frames emission and to retrieve information contained in received Timing Advertisements.

Appendix D. Protocol Layering

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated in Figure 2. The IP layer operates on top of the EtherType Protocol Discrimination (EPD); this Discrimination layer is described in IEEE Std 802.3-2012; the interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 IPv6                    |
+-+-+-+-+-+-{            }+-+-+-+-+-+-+-+-+
            {   LLC_SAP  }                 802.11-OCB
+-+-+-+-+-+-{            }+-+-+-+-+-+-+-+-+  Boundary
|            EPD          |       |       |
|                         | MLME  |       |
+-+-+-{  MAC_SAP   }+-+-+-|  MLME_SAP     |
|      MAC Sublayer       |       |       |  802.11-OCB
|     and ch. coord.      |       |  SME  |  Services
+-+-+-{   PHY_SAP  }+-+-+-+-+-+-+-|       |
|                         | PLME  |       |
|            PHY Layer    |   PLME_SAP    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: EtherType Protocol Discrimination

Appendix E. Design Considerations

The networks defined by 802.11-OCB are in many ways similar to other networks of the 802.11 family. In theory, the transportation of IPv6 over 802.11-OCB could be very similar to the operation of IPv6 over other networks of the 802.11 family. However, the high mobility, strong link asymmetry and very short connection makes the 802.11-OCB link significantly different from other 802.11 networks. Also, the automotive applications have specific requirements for reliability, security and privacy, which further add to the particularity of the 802.11-OCB link.

Appendix F. IEEE 802.11 Messages Transmitted in OCB mode

For information, at the time of writing, this is the list of IEEE 802.11 messages that may be transmitted in OCB mode, i.e. when dot11OCBActivated is true in a STA:

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;

- The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;

- The STA MUST send data frames of subtype QoS Data.

Appendix G. Examples of Packet Formats

This section describes an example of an IPv6 Packet captured over a IEEE 802.11-OCB link.

By way of example we show that there is no modification in the headers when transmitted over 802.11-OCB networks - they are transmitted like any other 802.11 and Ethernet packets.

We describe an experiment of capturing an IPv6 packet on an 802.11-OCB link. In topology depicted in Figure 3, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11-OCB interface. The packet is captured on the Host, using a network protocol analyzer (e.g. Wireshark); the capture is performed in two different modes: direct mode and 'monitor' mode. The topology used during the capture is depicted below.

The packet is captured on the Host. The Host is an IP-OBU containing an 802.11 interface in format PCI express (an ITRI product). The kernel runs the ath5k software driver with modifications for OCB mode. The capture tool is Wireshark. The file format for save and analyze is 'pcap'. The packet is generated by the Router. The Router is an IP-RSU (ITRI product).

```
       +--------+                                +-------+
       |        |          802.11-OCB Link       |       |
    ---| Router |--------------------------------| Host  |
       |        |                                |       |
       +--------+                                +-------+
```

Figure 3: Topology for capturing IP packets on 802.11-OCB

During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

G.1. Capture in Monitor Mode

The IPv6 RA packet captured in monitor mode is illustrated below. The radio tap header provides more flexibility for reporting the characteristics of frames. The Radiotap Header is prepended by this particular stack and operating system on the Host machine to the RA packet received from the network (the Radiotap Header is not present on the air). The implementation-dependent Radiotap Header is useful for piggybacking PHY information from the chip's registers as data in a packet understandable by userland applications using Socket interfaces (the PHY interface can be, for example: power levels, data rate, ratio of signal to noise).

The packet present on the air is formed by IEEE 802.11 Data Header, Logical Link Control Header, IPv6 Base Header and ICMPv6 Header.

```
Radiotap Header v0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Header Revision| Header Pad    |    Header length              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Present flags                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Data Rate     |             Pad                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

IEEE 802.11 Data Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Type/Subtype and Frame Ctrl  |          Duration             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Receiver Address...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
... Receiver Address            |      Transmitter Address...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... Transmitter Address                                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            BSS Id...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... BSS Id                     | Frag Number and Seq Number    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Logical-Link Control Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      DSAP   |I|     SSAP    |C| Control field | Org. code...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 ... Organizational Code        |             Type              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
IPv6 Base Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Router Advertisement
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Reachable Time                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Retrans Timer                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...
+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The value of the Data Rate field in the Radiotap header is set to 6 Mb/s. This indicates the rate at which this RA was received.

The value of the Transmitter address in the IEEE 802.11 Data Header is set to a 48bit value. The value of the destination address is 33:33:00:00:00:1 (all-nodes multicast address). The value of the BSS Id field is ff:ff:ff:ff:ff:ff, which is recognized by the network protocol analyzer as being "broadcast". The Fragment number and sequence number fields are together set to 0x90C6.

The value of the Organization Code field in the Logical-Link Control Header is set to 0x0, recognized as "Encapsulated Ethernet". The value of the Type field is 0x86DD (hexadecimal 86DD, or otherwise #86DD), recognized as "IPv6".

A Router Advertisement is periodically sent by the router to multicast group address ff02::1. It is an icmp packet type 134. The IPv6 Neighbor Discovery's Router Advertisement message contains an 8-bit field reserved for single-bit flags, as described in [RFC4861].

The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1.

The Ethernet Type field in the logical-link control header is set to 0x86dd which indicates that the frame transports an IPv6 packet. In the IEEE 802.11 data, the destination address is 33:33:00:00:00:01 which is the corresponding multicast MAC address. The BSS id is a broadcast address of ff:ff:ff:ff:ff:ff. Due to the short link duration between vehicles and the roadside infrastructure, there is no need in IEEE 802.11-OCB to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11-OCB enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.

G.2. Capture in Normal Mode

The same IPv6 Router Advertisement packet described above (monitor mode) is captured on the Host, in the Normal mode, and depicted below.

```
Ethernet II Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Destination...                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
...Destination                 |           Source...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
...Source                                                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Type                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

IPv6 Base Header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version| Traffic Class |           Flow Label                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

Router Advertisement
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Reachable Time                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Retrans Timer                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...
+-+-+-+-+-+-+-+-+-+-+-+-
```

One notices that the Radiotap Header, the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On the other hand, a new header named Ethernet II Header is present.

The Destination and Source addresses in the Ethernet II header contain the same values as the fields Receiver Address and Transmitter Address present in the IEEE 802.11 Data Header in the "monitor" mode capture.

The value of the Type field in the Ethernet II header is 0x86DD (recognized as "IPv6"); this value is the same value as the value of the field Type in the Logical-Link Control Header in the "monitor" mode capture.

The knowledgeable experimenter will no doubt notice the similarity of this Ethernet II Header with a capture in normal mode on a pure Ethernet cable interface.

A frame translation is inserted on top of a pure IEEE 802.11 MAC layer, in order to adapt packets, before delivering the payload data to the applications. It adapts 802.11 LLC/MAC headers to Ethernet II headers. In further detail, this adaptation consists in the elimination of the Radiotap, 802.11 and LLC headers, and in the insertion of the Ethernet II header. In this way, IPv6 runs straight over LLC over the 802.11-OCB MAC layer; this is further confirmed by the use of the unique Type 0x86DD.

Appendix H. Extra Terminology

The following terms are defined outside the IETF. They are used to define the main terms in the main terminology Section 2.

DSRC (Dedicated Short Range Communication): a term defined outside the IETF. The US Federal Communications Commission (FCC) Dedicated Short Range Communication (DSRC) is defined in the Code of Federal Regulations (CFR) 47, Parts 90 and 95. This Code is referred in the definitions below. At the time of the writing of this Internet Draft, the last update of this Code was dated October 1st, 2010.

DSRCS (Dedicated Short-Range Communications Services): a term defined outside the IETF. The use of radio techniques to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments. DSRCS systems may also transmit status and instructional messages related to the units involve. [Ref. 47 CFR 90.7 - Definitions]

OBU (On-Board Unit): a term defined outside the IETF. An On-Board Unit is a DSRCS transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of the respective chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of the respective chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands. - [CFR 90.7 - Definitions].

RSU (Road-Side Unit): a term defined outside of IETF. A Roadside Unit is a DSRC transceiver that is mounted along a road or pedestrian passageway. An RSU may also be mounted on a vehicle or is hand carried, but it may only operate when the vehicle or hand- carried unit is stationary. Furthermore, an RSU operating under the respectgive part is restricted to the location where it is licensed to operate. However, portable or hand-held RSUs are permitted to operate where they do not interfere with a site-licensed operation. A RSU broadcasts data to OBUs or exchanges data with OBUs in its communications zone. An RSU also provides channel assignments and operating instructions to OBUs in its communications zone, when required. - [CFR 90.7 - Definitions].

Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861][RFC4862] was designed for point-to-point and transit links such as Ethernet, with the expectation of a cheap and reliable support for multicast from the lower layer. Section 3.2 of RFC 4861 indicates that the operation on Shared Media and on non-broadcast multi-access (NBMA) networks require additional support, e.g., for Address Resolution (AR) and duplicate address detection (DAD), which depend on multicast. An infrastructureless radio network such as OCB shares properties with both Shared Media and NBMA networks, and then adds its own complexity, e.g., from movement and interference that allow only transient and non-transitive reachability between any set of peers.

The uniqueness of an address within a scoped domain is a key pillar of IPv6 and the base for unicast IP communication. RFC 4861 details the DAD method to avoid that an address is duplicated. For a link local address, the scope is the link, whereas for a Globally Reachable address the scope is much larger. The underlying assumption for DAD to operate correctly is that the node that owns an

IPv6 address can reach any other node within the scope at the time it claims its address, which is done by sending a NS multicast message, and can hear any future claim for that address by another party within the scope for the duration of the address ownership.

In the case of OCB, there is a potentially a need to define a scope that is compatible with DAD, and that cannot be the set of nodes that a transmitter can reach at a particular time, because that set varies all the time and does not meet the DAD requirements for a link local address that could possibly be used anytime, anywhere. The generic expectation of a reliable multicast is not ensured, and the operation of DAD and AR (Address Resolution) as specified by RFC 4861 cannot be guaranteed. Moreover, multicast transmissions that rely on broadcast are not only unreliable but are also often detrimental to unicast traffic (see [draft-ietf-mboned-ieee802-mcast-problems]).

Early experience indicates that it should be possible to exchange IPv6 packets over OCB while relying on IPv6 ND alone for DAD and AR (Address Resolution) in good conditions. In the absence of a correct DAD operation, a node that relies only on IPv6 ND for AR and DAD over OCB should ensure that the addresses that it uses are unique by means others than DAD. It must be noted that deriving an IPv6 address from a globally unique MAC address has this property but may yield privacy issues.

RFC 8505 provides a more recent approach to IPv6 ND and in particular DAD. RFC 8505 is designed to fit wireless and otherwise constrained networks whereby multicast and/or continuous access to the medium may not be guaranteed. RFC 8505 Section 5.6 "Link-Local Addresses and Registration" indicates that the scope of uniqueness for a link local address is restricted to a pair of nodes that use it to communicate, and provides a method to assert the uniqueness and resolve the link-Layer address using a unicast exchange.

RFC 8505 also enables a router (acting as a 6LR) to own a prefix and act as a registrar (acting as a 6LBR) for addresses within the associated subnet. A peer host (acting as a 6LN) registers an address derived from that prefix and can use it for the lifetime of the registration. The prefix is advertised as not onlink, which means that the 6LN uses the 6LR to relay its packets within the subnet, and participation to the subnet is constrained to the time of reachability to the 6LR. Note that RSU that provides internet connectivity MAY announce a default router preference [RFC4191], whereas a car that does not provide that connectivity MUST NOT do so. This operation presents similarities with that of an access point, but at Layer-3. This is why RFC 8505 well-suited for wireless in general.

Support of RFC 8505 may be implemented on OCB. OCB nodes that support RFC 8505 SHOULD support the 6LN operation in order to act as a host, and may support the 6LR and 6LBR operations in order to act as a router and in particular own a prefix that can be used by RFC 8505-compliant hosts for address autoconfiguration and registration.

Authors' Addresses

Nabil Benamar
Moulay Ismail University of Meknes
Morocco

Phone: +212670832236
Email: n.benamar@est.umi.ac.ma

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

Phone: +33493008134
Email: Jerome.Haerri@eurecom.fr

Jong-Hyouk Lee
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan 31066
Republic of Korea

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr

Network Working Group   J. Jeong, Ed.
Internet-Draft   Sungkyunkwan University
Intended status: Informational   March 5, 2018
Expires: September 6, 2018

IP-based Vehicular Networking: Use Cases, Survey and Problem Statement
draft-ietf-ipwave-vehicular-networking-02

Abstract

This document discusses use cases, survey, and problem statement on IP-based vehicular networks, which are considered a key component of Intelligent Transportation Systems (ITS). The main topics of vehicular networking are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) networking. First, this document surveys use cases using V2V and V2I networking. Second, this document deals with some critical aspects in vehicular networking, such as vehicular network architectures, standardization activities, IP address autoconfiguration, routing, mobility management, DNS naming service, service discovery, and security and privacy. For each aspect, this document discusses problem statement to analyze the gap between the state-of-the-art techniques and requirements in IP-based vehicular networking. Finally, this document articulates discussions including the summary and analysis of vehicular networking aspects and raises deployment issues.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Vehicular networks have been focused on the driving safety, driving efficiency, and entertainment in road networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC], service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850 - 5.925 GHz band (5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) networking.

For driving safety services based on the DSRC, IEEE has standardized Wireless Access in Vehicular Environments (WAVE) standards, such as IEEE 802.11p [IEEE-802.11p], IEEE 1609.2 [WAVE-1609.2], IEEE 1609.3 [WAVE-1609.3], and IEEE 1609.4 [WAVE-1609.4]. Note that 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. Along with these WAVE standards, IPv6 and Mobile IP protocols (e.g., MIPv4 and MIPv6) can be extended to vehicular networks [RFC2460][RFC6275].

This document discusses use cases, survey, and problem statements related to IP-based vehicular networking for Intelligent Transportation Systems (ITS). This document first surveys the use cases for using V2V and V2I networking in the ITS. Second, this document deals with some critical aspects in vehicular networking, such as vehicular network architectures, standardization activities, IP address autoconfiguration, routing, mobility management, DNS naming service, service discovery, and security and privacy. For each aspect, this document shows problem statement to analyze the gap between the state-of-the-art techniques and requirements in IP-based vehicular networking. Finally, this document addresses discussions including the summary and analysis of vehicular networking aspects, raising deployment issues in road environments.

Based on the use cases, survey, and problem statement of this document, we can specify the requirements for vehicular networks for the intended purposes, such as the driving safety, driving efficiency, and entertainment. As a consequence, this will make it possible to design a network architecture and protocols for vehicular networking.

2. Terminology

This document uses the following definitions:

- o Road-Side Unit (RSU): A node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, etc.) for wireless communication with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is deployed either at an intersection or in a road segment.

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

- Vehicle Detection Loop (or Loop Detector): An inductive device used for detecting vehicles passing or arriving at a certain point, for instance approaching a traffic light or in motorway traffic. The relatively crude nature of the loop's structure means that only metal masses above a certain size are capable of triggering the detection.

- 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. Example functions of TCC include the management of evacuation routes, the monitoring of real-time mass 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. TCC can communicate with road infrastructure nodes (e.g., RSUs, traffic signals, and loop detectors) to share measurement data and management information by an application-layer protocol.

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

- DMM: Acronym for "Distributed Mobility Management" [DMM].

3. Use Cases

This section provides use cases of V2V and V2I networking.

3.1. V2I Use Cases

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

A navigation service, such as the Self-Adaptive Interactive Navigation Tool (called SAINT) [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. The enhanced SAINT (called SAINT+) [SAINTplus] can give the fast moving paths for emergency vehicles (e.g., ambulance and fire engine) toward accident spots while providing other vehicles with efficient detour paths.

The emergency communication between accident vehicles (or emergency vehicles) and TCC can be performed via either RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, such as emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to FirstNet's network core. The current RAN is mainly constructed by 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Annual-Report-2017], but DSRC-based vehicular networks can be used for V2I in near future [DSRC].

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I networking can reduce the collision of a pedestrian and a vehicle, which have a smartphone, in a road network. Vehicles and pedestrians can communicate with each other via an RSU that delivers scheduling information for wireless communication to save the smartphones' battery.

3.2. V2V Use Cases

The use cases of V2V networking include context-aware navigation for driving safety, cooperative adaptive cruise control in an urban roadway, and platooning in a highway. These three techniques will be important elements for self-driving vehicles.

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely by letting the drivers recognize dangerous obstacles and situations. That is, CASD navigator displays obstables or neighboring vehicles relevant to possible collisions in real-time through V2V networking. CASD provides vehicles with a class-based automatic safety action plan, which considers three situations, such as the Line-of-Sight unsafe, Non-Line-of-Sight unsafe and safe situations. This action plan can be performed among vehicles through V2V networking.

Cooperative Adaptive Cruise Control (CACC) [CA-Cuise-Control] helps vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles in an urban roadway or a highway. CACC can help adjacent vehicles to efficiently adjust their speed in a cascade way through V2V networking.

Platooning [Truck-Platooning] allows a series of vehicles (e.g., trucks) to move together with a very short inter-distance. Trucks can use V2V communication in addition to forward sensors in order to maintain constant clearance between two consecutive vehicles at very short gaps (from 3 meters to 10 meters). This platooning can maximize the throughput of vehicular traffic in a highway and reduce the gas consumption because the leading vehicle can help the following vehicles to experience less air resistance.

4. Vehicular Network Architectures

This section surveys vehicular network architectures based on IP along with various radio technologies, and then discusses problem statement for a vehicular network architecture for IP-based vehicular networking.

4.1. Existing Architectures

4.1.1. VIP-WAVE: IP in 802.11p Vehicular Networks

Cespedes et al. proposed a vehicular IP in WAVE called VIP-WAVE for I2V and V2I networking [VIP-WAVE]. IEEE 1609.3 specified a WAVE stack of protocols and includes IPv6 as a network layer protocol in data plane [WAVE-1609.3]. The standard WAVE [WAVE-1609.0] [WAVE-1609.3] does not support Duplicate Address Detection (DAD) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862] by having its own efficient IP address configuration mechanism based on a WAVE Service Advertisement (WSA) management frame [WAVE-1609.3]. It does not support both seamless communications for Internet services and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU), either. To overcome these limitations of the standard WAVE for IP-based networking, VIP-WAVE enhances the standard WAVE by the following three schemes: (i) an efficient mechanism for the IPv6 address assignment and DAD, (ii) on-demand IP mobility based on Proxy Mobile IPv6 (PMIPv6), and (iii) one-hop and two-hop communications for I2V and V2I networking.

In WAVE, IPv6 Neighbor Discovery (ND) protocol is not recommended due to the overhead of ND against the timely and prompt communications in vehicular networking. By WAVE service advertisement (WAS) management frame, an RSU can provide vehicles with IP configuration information (e.g., IPv6 prefix, prefix length, gateway, router lifetime, and DNS server) without using ND. However, WAVE devices may support readdressing to provide pseudonymity, so a MAC address of a vehicle may be changed or randomly generated. This update of the MAC address may lead to the collision of an IPv6 address based on a MAC address, so VIP-WAVE includes a light-weight, on-demand ND to perform DAD.

For IP-based Internet services, VIP-WAVE adopts PMIPv6 for network-based mobility management in vehicular networks. In VIP-WAVE, RSU plays a role of mobile anchor gateway (MAG) of PMIPv6, which performs the detection of a vehicle as a mobile node in a PMIPv6 domain and registers it into the PMIPv6 domain. For PMIPv6 operations, VIP-WAVE requires a central node called local mobility anchor (LMA), which assigns IPv6 prefixes to vehicles as mobile nodes and forwards data packets to the vehicles moving in the coverage of RSUs under its control through tunnels between MAGs and itself.

For two-hop communications between a vehicle and an RSU, VIP-WAVE allows an intermediate vehicle between the vehicle and the RSU to play a role of a packet relay for the vehicle. When it becomes out of the communication range of an RSU, a vehicle searches for another vehicle as a packet relay by sending a relay service announcement. When it receives this relay service announcement and is within the communication range of an RSU, another vehicle registers itself into the RSU as a relay and notifies the relay-requester vehicle of a relay maintenance announcement.

Thus, VIP-WAVE is a good candidate for I2V and V2I networking, supporting an enhanced ND, handover, and two-hop communications through a relay.

4.1.2. IPv6 Operation for WAVE

Baccelli et al. provided an analysis of the operation of IPv6 as it has been described by the IEEE WAVE standards 1609 [IPv6-WAVE]. Although the main focus of WAVE has been the timely delivery of safety related information, the deployment of IP-based entertainment applications is also considered. Thus, in order to support entertainment traffic, WAVE supports IPv6 and transport protocols such as TCP and UDP.

In the analysis provided in [IPv6-WAVE], it is identified that the IEEE 1609.3 standard’s recommendations for IPv6 operation over WAVE are rather minimal. Protocols on which the operation of IPv6 relies for IP address configuration and IP-to-link-layer address translation (e.g., IPv6 ND protocol) are not recommended in the standard. Additionally, IPv6 implementations work under certain assumptions for the link model that do not necessarily hold in WAVE. For instance, some IPv6 implementations assume symmetry in the connectivity among neighboring interfaces. However, interference and different levels of transmission power may cause unidirectional links to appear in a WAVE link model. Also, in an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix are on the same IP link. Hence, there is a relationship between link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. Such a relationship does not hold in a WAVE link model due to node mobility and highly dynamic topology.

Baccelli et al. concluded that the use of the standard IPv6 protocol stack, as the IEEE 1609 family of specifications stipulate, is not sufficient. Instead, the addressing assignment should follow considerations for ad-hoc link models, defined in [RFC5889], which are similar to the characteristics of the WAVE link model. In terms of the supporting protocols for IPv6, such as ND, DHCP, or stateless auto-configuration, which rely largely on multicast, do not operate as expected in the case where the WAVE link model does not have the same behavior expected for multicast IPv6 traffic due to nodes' mobility and link variability. Additional challenges such as the support of pseudonimity through MAC address change along with the suitability of traditional TCP applications are discussed by the authors since those challenges require the design of appropriate solutions.

4.1.3. Multicast Framework for Vehicular Networks

Jemaa et al. presented a framework that enables deploying multicast services for vehicular networks in Infrastructure-based scenarios [VNET-Framework]. This framework deals with two phases: (i) Initialization or bootstrapping phase that includes a geographic multicast auto-configuration process and a group membership building method and (ii) Multicast traffic dissemination phase that includes a network selecting mechanism on the transmission side and a receiver-based multicast delivery in the reception side. To this end, the authors define a distributed mechanism that allows the vehicles to configure a common multicast address: Geographic Multicast Address Auto-configuration (GMAA), which allows a vehicle to configure its own address without signaling. A vehicle may also be able to change the multicast address to which it is subscribed when it changes its location.

This framework suggests a network selecting approach that allows IP and non-IP multicast data delivery on the sender side. Then, to meet the challenges of multicast address auto-configuration, the authors propose a distributed geographic multicast auto-addressing mechanism for multicast groups of vehicles, and a simple multicast data delivery scheme in hybrid networks from a server to the group of moving vehicles. However, the GMAA study lacks simulations related to performance assessment.

4.1.4. Joint IP Networking and Radio Architecture

Petrescu et al. defined the joint IP networking and radio architecture for V2V and V2I communication in [Joint-IP-Networking]. The paper proposes to consider an IP topology in a similar way as a radio link topology, in the sense that an IP subnet would correspond to the range of 1-hop vehicular communication. The paper defines three types of vehicles: Leaf Vehicle (LV), Range Extending Vehicle (REV), and Internet Vehicle (IV). The first class corresponds to the largest set of communicating vehicles (or network nodes within a vehicle), while the role of the second class is to build an IP relay between two IP-subnet and two sub-IP networks. Finally, the last class corresponds to vehicles being connected to Internet. Based on these three classes, the paper defines six types of IP topologies corresponding to V2V communication between two LVs in direct range, or two LVs over a range extending vehicle, or V2I communication again either directly via an IV, via another vehicles being IV, or via an REV connecting to an IV.

Consider a simplified example of a vehicular train, where LV would be in-wagon communicating nodes, REV would be inter-wagon relays, and IV would be one node (e.g., train head) connected to Internet. Petrescu et al. defined the required mechanisms to build subnetworks, and evaluated the protocol time that is required to build such networks. Although no simulation-based evaluation is conducted, the initial analysis shows a long initial connection overhead, which should be alleviated once the multi-wagon remains stable. However, this approach does not describe what would happen in the case of a dynamic multi-hop vehicular network, where such overhead would end up being too high for V2V/V2I IP-based vehicular applications.

One other aspect described in their paper is to join the IP-layer relaying with radio-link channels. Their paper proposes separating different subnetworks in different WiFi/ITS-G5 channels, which could be advertised by the REV. Accordingly, the overall interference could be controlled within each subnetwork. This approach is similar to multi-channel topology management proposals in multi-hop sensor networks, yet adapted to an IP topology.

Their paper concludes that the generally complex multi-hop IP vehicular topology could be represented by only six different topologies, which could be further analyzed and optimized. A prefix dissemination protocol is proposed for one of the topologies.

4.1.5. Mobile Internet Access in FleetNet

Bechler et al. described the FleetNet project approach to integrate Internet Access in future vehicular networks [FleetNet]. The FleetNet paper is probably one of the first papers to address this aspect, and in many ways, introduces concepts that will be later used in MIPv6 or other subsequent IP mobility management schemes. The paper describes a V2I architecture consisting of Vehicles, Internet Gateways (IGW), Proxy, and Corresponding Nodes (CN). Considering that vehicular networks are required to use IPv6 addresses and also the new wireless access technology ITS-G5 (new at that time), one of the challenges is to bridge the two different networks (i.e., VANET and IPv4/IPv6 Internet). Accordingly, the paper introduces a Fleetnet Gateway (FGW), which allows vehicles in IPv6 to access the IPv4 Internet and to bridge two types of networks and radio access technologies. Another challenge is to keep the active addressing and flows while vehicles move between FGWs. Accordingly, the paper introduces a proxy node, a hybrid MIP Home Agent, which can re-route flows to the new FGW as well as acting as a local IPv4-IPv6 NAT.

The authors from the paper mostly observed two issues that VANET brings into the traditional IP mobility. First, VANET vehicles must mostly be addressed from the Internet directly, and do not specifically have a Home Network. Accordingly, VANET vehicles require a globally (predefined) unique IPv6 address, while an IPv6 co-located care-of address (CCoA) is a newly allocated IPv6 address every time a vehicle would enter a new IGW radio range. Second, VANET links are known to be unreliable and short, and the extensive use of IP tunneling on-the-air was judged not efficient. Accordingly, the first major architecture innovation proposed in this paper is to re-introduce a foreign agent (FA) in MIP located at the IGW, so that the IP-tunneling would be kept in the back-end (between a Proxy and an IGW) and not on the air. Second, the proxy has been extended to build an IP tunnel and be connected to the right FA/IWG for an IP flow using a global IPv6 address.

This is a pioneer paper, which contributed to changing MIP and led to the new IPv6 architecture currently known as Proxy-MIP and the subsequent DMM-PMIP. Three key messages can be yet kept in mind. First, unlike the Internet, vehicles can be more prominently directly addressed than the Internet traffic, and do not have a Home Network in the traditional MIP sense. Second, IP tunneling should be avoided as much as possible over the air. Third, the protocol-based mobility (induced by the physical mobility) must be kept hidden to both the vehicle and the correspondent node (CN).

4.1.6. A Layered Architecture for Vehicular DTNs

Soares et al. addressed the case of delay tolerant vehicular network [Vehicular-DTN]. For delay tolerant or disruption tolerant networks, rather than building a complex VANET-IP multi-hop route, vehicles may also be used to carry packets closer to the destination or directly to the destination. The authors built the well-accepted DTN Bundle architecture and protocol to propose a VANET extension. They introduced three types of VANET nodes: (i) terminal nodes (requiring data), (ii) mobile nodes (carrying data along their routes), and (iii) relay nodes (storing data at cross-roads of mobile nodes as data hotspot).

The major innovation in this paper is to propose a DTN VANET architecture separating a Control plane and a Data plane. The authors claimed it to be designed to allow full freedom to select the most appropriate technology, as well as allow to use out-of-band communication for small Control plane packets and use DTN in-band for the Data plane. The paper then further describes the different layers from the Control and the Data planes. One interesting aspect is the positioning of the Bundle layer between L2 and L3, rather than above TCP/IP as for the DTN Bundle architecture. The authors claimed this to be required first to keep bundle aggregation/disaggregation transparent to IP, as well as to allow bundle transmission over multiple access technologies (described as MAC/PHY layers in the paper).

Although DTN architectures have evolved since the paper was written, the Vehicular-DTN paper takes a different approach to IP mobility management. An important aspect is to separate the Control plane from the Data plane to allow a large flexibility in a Control plane to coordinate a heterogeneous radio access technology (RAT) Data plane.

4.2. V2I and V2V Internetworking Problem Statement

This section provides a problem statement of a vehicular network architecture of IPv6-based V2I and V2V networking. The main focus in this document 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 focus is 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 an architecture 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.

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

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

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

In vehicular networks, unidirectional links exist and must be considered. The control plane must be separated from data plane. ID/Pseudonym change requires a lightweight DAD. IP tunneling should be avoided. The mobility information of a mobile device (e.g., vehicle), such as trajectory, position, speed, and direction, can be used by the mobile device and infrastructure nodes (e.g., TCC and RSU) for the accommodation of proactive protocols because it is usually equipped with a GPS receiver. Vehicles can use the TCC as its Home Network, so the TCC maintains the mobility information of vehicles for location management. A vehicular network architecture may be composed of three types of vehicles in Figure 1: Leaf Vehicle, Range Extending Vehicle, and Internet Vehicle[Joint-IP-Networking].

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

4.2.1. V2I-based Internetworking

As shown in Figure 2, the vehicle’s moving network and the RSU’s fixed network are self-contained 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. 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.

```
                     (*)<.........>(*)
                      |              | 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

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle's moving network and the RSU's fixed network. DNS should be supported to enable name resolution for hosts or servers residing either in the vehicle's moving network or the RSU's fixed 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 (called mobile router) and RSU1's Router3 (called fixed router) 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.

```
                           (*)<..........>(*)
                            |              | 2001:DB8:1:1::/64
   .------------------------------.  .---------------------------------.
   |                        |     |  |     |                           |
   | .-------. .------. .-------. |  | .-------. .------. .-------.    |
   | | Host1 | |RDNSS1| |Router1| |  | |Router3| |RDNSS2| | Host3 |    |
   | ._______. .______. ._______. |  | ._______. .______. ._______.    |
   |     ^        ^         ^     |  |     ^         ^        ^        |
   |     |        |         |     |  |     |         |        |        |
   |     v        v         v     |  |     v         v        v        |
   | ---------------------------- |  | ------------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |     ^ 2001:DB8:30:1::/64        |
   |                    |         |  |     |                           |
   |                    v         |  |     v                           |
   | .-------.      .-------.     |  | .-------.      .-------.        |
   | | Host2 |      |Router2|     |  | |Router4|      | Host4 |        |
   | ._______.      ._______.     |  | ._______.      ._______.        |
   |     ^              ^         |  |     ^              ^            |
   |     |              |         |  |     |              |            |
   |     v              v         |  |     v              v            |
   | ---------------------------- |  | ------------------------------- |
   |  2001:DB8:10:2::/64          |  |       2001:DB8:30:2::/64        |
   .______________________________.  ._________________________________.
      Vehicle1 (Moving Network1)        Vehicle2 (Moving Network2)

      <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 3: Internetworking between Two Vehicle Networks

4.2.2. 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 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 (called mobile router) and Vehicle2’s Router3 (called mobile router) 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.

5. Standardization Activities

This section surveys standard activities for vehicular networks in standards developing organizations.

5.1. IEEE Guide for WAVE - Architecture

IEEE 1609 is a suite of standards for Wireless Access in Vehicular Environments (WAVE) developed in the IEEE Vehicular Technology Society (VTS). They define an architecture and a complementary standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications.

IEEE 1609.0 provides a description of the WAVE system architecture and operations (called WAVE reference model) [WAVE-1609.0]. The reference model of a typical WAVE device includes two data plane protocol stacks (sharing a common lower stack at the data link and physical layers): (i) the standard Internet Protocol Version 6 (IPv6) and (ii) the WAVE Short Message Protocol (WSMP) designed for optimized operation in a wireless vehicular environment. WAVE Short Messages (WSM) may be sent on any channel. IP traffic is only allowed on service channels (SCHs), so as to offload high-volume IP traffic from the control channel (CCH).

The Layer 2 protocol stack distinguishes between the two upper stacks by the Ethertype field. Ethertype is a 2-octet field in the Logical Link Control (LLC) header, used to identify the networking protocol to be employed above the LLC protocol. In particular, it specifies the use of two Ethertype values (i.e., two networking protocols), such as IPv6 and WSMP.

Regarding the upper layers, while WAVE communications use standard port numbers for IPv6-based protocols (e.g., TCP, UDP), they use a Provider Service Identifier (PSID) as an identifier in the context of WSMP.

5.2. IEEE Standard for WAVE - Networking Services

IEEE 1609.3 defines services operating at the network and transport layers, in support of wireless connectivity among vehicle-based devices, and between fixed roadside devices and vehicle-based devices using the 5.9 GHz Dedicated Short-Range Communications/Wireless Access in Vehicular Environments (DSRC/WAVE) mode [WAVE-1609.3].

WAVE Networking Services represent layer 3 (networking) and layer 4 (transport) of the OSI communications stack. The purpose is then to provide addressing and routing services within a WAVE system, enabling multiple stacks of upper layers above WAVE Networking Services and multiple lower layers beneath WAVE Networking Services. Upper layer support includes in-vehicle applications offering safety and convenience to users.

The WAVE standards support IPv6. IPv6 was selected over IPv4 because IPv6 is expected to be a viable protocol into the foreseeable future. Although not described in the WAVE standards, IPv4 has been tunnelled over IPv6 in some WAVE trials.

The document provides requirements for IPv6 configuration, in particular for the address setting. It specifies the details of the different service primitives, among which is the WAVE Routing Advertisement (WRA), part of the WAVE Service Advertisement (WSA). When present, the WRA provides information about infrastructure internetwork connectivity, allowing receiving devices to be configured to participate in the advertised IPv6 network. For example, an RSU can broadcast in the WRA portion of its WSA all the information necessary for an OBU to access an application-service available over IPv6 through the RSU as a router. This feature removes the need for IPv6 Router Advertisement messages, which are based on ICMPv6.

5.3. ETSI Intelligent Transport Systems: GeoNetwork-IPv6

ETSI published a standard specifying the transmission of IPv6 packets over the ETSI GeoNetworking (GN) protocol [ETSI-GeoNetworking] [ETSI-GeoNetwork-IP]. IPv6 packet transmission over GN is defined in ETSI EN 302 636-6-1 [ETSI-GeoNetwork-IP] using a protocol adaptation sub-layer called "GeoNetworking to IPv6 Adaptation Sub-Layer (GN6ASL)". It enables an ITS station (ITS-S) running the GN protocol and an IPv6-compliant protocol layer to: (i) exchange IPv6 packets with other ITS-S; (ii) acquire globally routable IPv6 unicast addresses and communicate with any IPv6 host located in the Internet by having the direct connectivity to the Internet or via other relay ITS stations; (iii) perform operations as a Mobile Router for network mobility [RFC3963].

The document introduces three types of virtual link, the first one providing symmetric reachability by means of stable geographically scoped boundaries and two others that can be used when the dynamic definition of the broadcast domain is required. The combination of these three types of virtual link in the same station allows running the IPv6 ND protocol including SLAAC [RFC4862] as well as distributing other IPv6 link-local multicast traffic and, at the same time, reaching nodes that are outside specific geographic boundaries. The IPv6 virtual link types are provided by the GN6ASL to IPv6 in the form of virtual network interfaces.

The document also describes how to support bridging on top of the GN6ASL, how IPv6 packets are encapsulated in GN packets and delivered, as well as the support of IPv6 multicast and anycast traffic, and neighbor discovery. For latency reasons, the standard strongly recommends to use SLAAC for the address configuration.

Finally, the document includes the required operations to support the change of pseudonym, e.g., changing IPv6 addresses when the GN address is changed, in order to prevent attackers from tracking the ITS-S.

5.4. ISO Intelligent Transport Systems: IPv6 over CALM

ISO published a standard specifying the IPv6 network protocols and services for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6]. These services are necessary to support the global reachability of ITS-S, the continuous Internet connectivity for ITS-S, and the handover functionality required to maintain such connectivity. This functionality also allows legacy devices to effectively use an ITS-S as an access router to connect to the Internet. Essentially, this specification describes how IPv6 is configured to support ITS-S and provides the associated management functionality.

The requirements apply to all types of nodes implementing IPv6: personal, vehicle, roadside, or central node. The standard defines IPv6 functional modules that are necessary in an IPv6 ITS-S, covering IPv6 forwarding, interface between IPv6 and lower layers (e.g., LAN interface), mobility management, and IPv6 security. It defines the mechanisms to be used to configure the IPv6 address for static nodes as well as for mobile nodes, while maintaining reachability from the Internet.

6. IP Address Autoconfiguration

This section surveys IP address autoconfiguration schemes for vehicular networks, and then discusses problem statement for IP addressing and address autoconfiguration for vehicular networking.

6.1. Existing Protocols for Address Autoconfiguration

6.1.1. Automatic IP Address Configuration in VANETs

Fazio et al. proposed a vehicular address configuration called VAC for automatic IP address configuration in Vehicular Ad Hoc Networks (VANET) [Address-Autoconf]. VAC uses a distributed dynamic host configuration protocol (DHCP). This scheme uses a leader playing a role of a DHCP server within a cluster having connected vehicles within a VANET. In a connected VANET, vehicles are connected with each other within communication range. In this VANET, VAC dynamically elects a leader-vehicle to quickly provide vehicles with unique IP addresses. The leader-vehicle maintains updated information on configured addresses in its connected VANET. It aims at the reduction of the frequency of IP address reconfiguration due to mobility.

VAC defines "SCOPE" to be a delimited geographic area within which IP addresses are guaranteed to be unique. When a vehicle is allocated an IP address from a leader-vehicle with a scope, it is guaranteed to have a unique IP address while moving within the scope of the leader-vehicle. If it moves out of the scope of the leader vehicle, it needs to ask for another IP address from another leader-vehicle so that its IP address can be unique within the scope of the new leader-vehicle. This approach may allow for less frequent change of an IP address than the address allocation from a fixed Internet gateway.

Thus, VAC can support a feasible address autoconfiguration for V2V scenarios, but the overhead to guarantee the uniqueness of IP addresses is not ignorable under high-speed mobility.

6.1.2. Using Lane/Position Information

Kato et al. proposed an IPv6 address assignment scheme using lane and position information [Address-Assignment]. In this addressing scheme, each lane of a road segment has a unique IPv6 prefix. When it moves in a lane in a road segment, a vehicle autoconfigures its IPv6 address with its MAC address and the prefix assigned to the lane. A group of vehicles constructs a connected VANET within the same subnet such that their IPv6 addresses have the same prefix. Whenever it moves to another lane, a vehicle updates its IPv6 address with the prefix corresponding to the new lane and also joins the group corresponding to the lane.

However, this address autoconfiguration scheme may have too much overhead when vehicles change their lanes frequently on the highway.

6.1.3. GeoSAC: Scalable Address Autoconfiguration

Baldessari et al. proposed an IPv6 scalable address autoconfiguration scheme called GeoSAC for vehicular networks [GeoSAC]. GeoSAC uses geographic networking concepts such that it combines the standard IPv6 Neighbor Discovery (ND) and geographic routing functionality. It matches geographically-scoped network partitions to individual IPv6 multicast-capable links. In the standard IPv6, all nodes within the same link must communicate with each other, but due to the characteristics of wireless links, this concept of a link is not clear in vehicular networks. GeoSAC defines a link as a geographic area having a network partition. This geographic area can have a connected VANET. Thus, vehicles within the same VANET in a specific geographic area are regarded as staying in the same link, that is, an IPv6 multicast link.

The GeoSAC paper identifies eight key requirements of IPv6 address autoconfiguration for vehicular networks: (i) the configuration of globally valid addresses, (ii) a low complexity for address autoconfiguration, (iii) a minimum signaling overhead of address autoconfiguration, (iv) the support of network mobility through movement detection, (v) an efficient gateway selection from multiple RSUs, (vi) a fully distributed address autoconfiguration for network security, (vii) the authentication and integrity of signaling messages, and (viii) the privacy protection of vehicles' users.

To support the proposed link concept, GeoSAC performs ad hoc routing for geographic networking in a sub-IP layer called Car-to-Car (C2C) NET. Vehicles within the same link can receive an IPv6 router advertisement (RA) message transmitted by an RSU as a router, so they can autoconfigure their IPv6 address based on the IPv6 prefix contained in the RA and perform Duplicate Address Detection (DAD) to verify the uniqueness of the autoconfigured IP address by the help of the geographic routing within the link.

For location-based applications, to translate between a geographic area and an IPv6 prefix belonging to an RSU, this paper takes advantage of an extended DNS service, using GPS-based addressing and routing along with geographic IPv6 prefix format [GeoSAC].

Thus, GeoSAC can support the IPv6 link concept through geographic routing within a specific geographic area.

6.1.4. Cross-layer Identities Management in ITS Stations

ITS and vehicular networks are built on the concept of an ITS station (ITS-S) (e.g., vehicle and RSU), which is a common reference model inspired from the Open Systems Interconnection (OSI) standard [Identity-Management]. In vehicular networks using multiple access network technologies through a cross-layer architecture, a vehicle with an OBU may have multiple identities corresponding to the access network interfaces. Wetterwald et al. conducted a comprehensive study of the cross-layer identity management in vehicular networks using multiple access network technologies, which constitutes a fundamental element of the ITS architecture [Identity-Management].

Besides considerations related to the case where ETSI GeoNetworking [ETSI-GeoNetworking] is used, this paper analyzes the major requirements and constraints weighing on the identities of ITS stations, e.g., privacy and compatibility with safety applications and communications. The concerns related to security and privacy of the users need to be addressed for vehicular networking, considering all the protocol layers. In other words, for security and privacy constraints to be met, the IPv6 address of a vehicle should be derived from a pseudonym-based MAC address and renewed simultaneously with that changing MAC address. By dynamically changing its IPv6 address, an ITS-S can avoid being tracked by a hacker. However, sometimes this address update cannot be applied; in some situations, continuous knowledge about the surrounding vehicles is required.

Also, the ITS-S Identity Management paper defines a cross-layer framework that fulfills the requirements on the identities of ITS stations and analyzes systematically, layer by layer, how an ITS station can be identified uniquely and safely, whether it is a moving station (e.g., car or bus using temporary trusted pseudonyms) or a static station (e.g., RSU and central station). This paper has been applied to the specific case of the ETSI GeoNetworking as the network layer, but an identical reasoning should be applied to IPv6 over 802.11 in Outside the Context of a Basic Service Set (OCB) mode now.

6.2. Problem Statement for IP Address Autoconfiguration

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 has been used sometimes 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.

6.2.1. Neighbor Discovery

Neighbor Discovery (ND) [RFC4861] is a core part of the IPv6 protocol suite. This section discusses the need for modifying ND for use with 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.

6.2.2. IP Address Autoconfiguration

This section discusses IP address autoconfiguration for vehicular networking. For IP address autoconfiguration, high-speed vehicles should also be considered. For V2I networking, 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 traverses 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].

For IP address autoconfiguration in V2V, vehicles can autoconfigure their address using prefixes for ULAs for vehicular networks [RFC4193].

High-speed mobility should be considered for a light-overhead address autoconfiguration. A cluster leader can have an IPv6 prefix [Address-Autoconf]. Each lane in a road segment can have an IPv6 prefix [Address-Assignment]. A geographic region under the communication range of an RSU can have an IPv6 prefix [GeoSAC].

IPv6 ND should be extended to support the concept of a link for an IPv6 prefix in terms of multicast. Ad Hoc routing is required for the multicast in a connected VANET with the same IPv6 prefix [GeoSAC]. A rapid DAD should be supported to prevent or reduce IPv6 address conflicts.

In the ETSI GeoNetworking, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities and the corresponding IPv6 addresses [Identity-Management]. For the continuity of an end-to-end transport session, the cross-layer identity management has to be performed carefully.

7. Routing

This section surveys routing in vehicular networks, and then discusses problem statement for routing in vehicular networks.

7.1. Existing Routing Protocols

7.1.1. Experimental Evaluation for IPv6 over GeoNet

Tsukada et al. presented a work that aims at combining IPv6 networking and a Car-to-Car Network routing protocol (called C2CNet) proposed by the Car2Car Communication Consortium (C2C-CC), which is an architecture using a geographic routing protocol

[VANET-Geo-Routing]. In the C2C-CC architecture, the C2CNet layer is located between IPv6 and link layers. Thus, an IPv6 packet is delivered with an outer C2CNet header, which introduces the challenge of how to support the communication types defined in C2CNet in IPv6 layer.

The main goal of GeoNet is to enhance the C2C specifications and create a prototype software implementation interfacing with IPv6. C2CNet is specified in C2C-CC as a geographic routing protocol.

In order to assess the performance of C2CNet, the authors measured the network performance with UDP and ICMPv6 traffic using iperf and ping6. The test results show that IPv6 over C2CNet does not have too much delay (less than 4ms with a single hop) and is feasible for vehicle communication. In the outdoor testbed, they developed AnaVANET to enable hop-by-hop performance measurement and position trace of the vehicles.

The combination of IPv6 multicast and GeoBroadcast was implemented; however, the authors did not evaluate the performance with such a scenario. One of the reasons is that a sufficiently high number of receivers are necessary to properly evaluate multicast but experimental evaluation is limited in the number of vehicles (4 in this study).

7.1.2. Location-Aided Gateway Advertisement and Discovery

Abrougui et al. presented a gateway discovery scheme for VANET, called Location-Aided Gateway Advertisement and Discovery (LAGAD) mechanism[LAGAD]. LAGAD enables vehicles to route packets toward the closest gateway quickly by discovering nearby gateways. The major problem that LAGAD tackles is to determine the radius of advertisement zone of a gateway, which depends on the location and velocity of a vehicle.

A gateway sends advertisement (GAdv) messages perodically to neighboring vehicles. When receiving a request message from a vehicle, the gateway replies to the source vehicle by a gateway reply (GRep) message. The GRep message contains the location information of the gateway and the subnet prefix of the gateway by which the source vehicle can send data packet via the gateway. The gateway sends GAdv messages through all vehicles within an advertisement zone built based on the velocity of the source vehicle.

The source vehicle starts gateway discovery process by sending routing request packets. The routing request packet is encapsulated into a Gateway Reactive Discovery (GRD) packet or a GReq message to send to the surrounding vehicles. The GRD contains both discovery and routing information as well as the location and the velocity of the source vehicle. Meanwhile, the intermediate vehicles in an advertisement zone of the gateway forward packets sent from the source vehicle. The gateway continuously updates the advertisement zone whenever receiving a new data packet from the source vehicle.

7.2. Routing Problem Statement

IP address autoconfiguration should be modified to support the efficient networking. Due to network fragmentation, vehicles sometimes cannot communicate with each other temporarily. IPv6 ND should consider the temporary network fragmentation. IPv6 link concept can be supported by Geographic routing to connect vehicles with the same IPv6 prefix.

The gateway advertisement and discovery process for routing in VANET can probably work when the density of vehicle in a road network is not sparse. A sparse vehicular network challenges the gateway discovery since network fragmentation interrupts the discovery process.

8. Mobility Management

This section surveys mobility management schemes in vehicular networks to support handover, and then discusses problem statement for mobility management in vehicular networks.

8.1. Existing Protocols

8.1.1. Vehicular Ad Hoc Networks with Network Fragmentation

Chen et al. tackled the issue of network fragmentation in VANET environments [IP-Passing-Protocol]. The paper proposes a protocol that can postpone the time to release IP addresses to the DHCP server and select a faster way to get the vehicle’s new IP address, when the vehicle density is low or the speeds of vehicles are varied. In such circumstances, the vehicle may not be able to communicate with the intended vehicle either directly or through multi-hop relays as a consequence of network fragmentation.

The paper claims that although the existing IP passing and mobility solutions may reduce handoff delay, but they cannot work properly on VANET especially with network fragmentation. This is due to the fact that messages cannot be transmitted to the intended vehicles. When network fragmentation occurs, it may incur longer handoff latency and higher packet loss rate. The main goal of this study is to improve existing works by proposing an IP passing protocol for VANET with network fragmentation.

The paper makes the assumption that on the highway, when a vehicle moves to a new subnet, the vehicle will receive broadcast packet from the target Base Station (BS), and then perform the handoff procedure. The handoff procedure includes two parts, such as the layer-2 handoff (new frequency channel) and the layer-3 handover (a new IP address). The handoff procedure contains movement detection, DAD procedure, and registration. In the case of IPv6, the DAD procedure is time consuming and may cause the link to be disconnected.

This paper proposes another handoff mechanism. The handoff procedure contains the following phases. The first is the information collecting phase, where each mobile node (vehicle) will broadcast its own and its neighboring vehicles' locations, moving speeds, and directions periodically. The remaining phases are, the fast IP acquiring phase, the cooperation of vehicle phase, the make before break phase, and the route redirection phase.

Simulations results show that for the proposed protocol, network fragmentation ratio incurs less impact. Vehicle speed and density has great impact on the performance of the IP passing protocol because vehicle speed and vehicle density will affect network fragmentation ratio. A longer IP lifetime can provide a vehicle with more chances to acquire its IP address through IP passing. Simulation results show that the proposed scheme can reduce IP acquisition time and packet loss rate, so extend IP lifetime with extra message overhead.

8.1.2. Hybrid Centralized-Distributed Mobility Management

Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support highly mobile vehicles [H-DMM]. Legacy mobility management systems are not suitable for high-speed scenarios because a registration delay is imposed proportional to the distance between a vehicle and its anchor network. H-DMM is designed to satisfy requirements such as service disruption time, end-to-end delay, packet delivery cost, and tunneling cost.

H-DMM proposes a central node called central mobility anchor (CMA), which plays the role of a local mobility anchor (LMA) in PMIPv6. When it enters a mobile access router (MAR) as an access router, a vehicle obtains a prefix from the MAR (called MAR-prefix) according to the legacy DMM protocol. In addition, it obtains another prefix from the CMA (called LMA-prefix) for a PMIPv6 domain. Whenever it performs a handover between the subnets for two adjacent MARs, a vehicle keeps the LMA-prefix while obtaining a new prefix from the new MAR. For a new data exchange with a new CN, the vehicle can select the MAR-prefix or the LMA-prefix for its own source IPv6 address. If the number of active prefixes is greater than a threshold, the vehicle uses the LMA-prefix-based IPv6 address as its source address. In addition, it can continue receiving data packets with the destination IPv6 addresses based on the previous prefixes through the legacy DMM protocol.

Thus, H-DMM can support an efficient tunneling for a high-speed vehicle that moves fast across the subnets of two adjacent MARs. However, when H-DMM asks a vehicle to perform DAD for the uniqueness test of its configured IPv6 address in the subnet of the next MAR, the activation of the configured IPv6 address for networking will be delayed. This indicates that a proactive DAD by a network component (i.e., MAR and LMA) can shorten the address configuration delay of the current DAD triggered by a vehicle.

8.1.3. Hybrid Architecture for Network Mobility Management

Nguyen et al. proposed H-NEMO, a hybrid centralized-distributed mobility management scheme to handle IP mobility of moving vehicles [H-NEMO]. The standard Network Mobility (NEMO) basic support, which is a centralized scheme for network mobility, provides IP mobility for a group of users in a moving vehicle, but also inherits the drawbacks from Mobile IPv6, such as suboptimal routing and signaling overhead in nested scenarios as well as reliability and scalability issues. On the contrary, distributed schemes such as the recently proposed Distributed Mobility Management (DMM) locates the mobility anchor at the network edge and enables mobility support only to traffic flows that require such support. However, in high speed moving vehicles, DMM may suffer from high signaling cost and high handover latency.

The proposed H-NEMO architecture is not designed for a specific wireless technology. Instead, it defines a general architecture and signaling protocol so that a mobile node can obtain mobility from fixed locations or mobile platforms, and also allows the use of DMM or Proxy Mobile IPv6 (PMIPv6), depending on flow characteristics and mobility patterns of the node. For IP addressing allocation, a mobile router (MR) or the mobile node (MN) connected to an MR in a NEMO obtain two sets of prefixes: one from the central mobility anchor and one from the mobile access router (MAR). In this way, the MR/MN may choose a more stable prefix for long-lived flows to be routed via the central mobility anchor and the MAR-prefix for short-lived flows to be routed following the DMM concept. The multi-hop scenario is considered under the concept of a nested-NEMO.

Nguyen et al. did not provide simulation-based evaluations, but they provided an analytical evaluation that considered signaling and packet delivery costs, and showed that H-NEMO outperforms the previous proposals, which are either centralized or distributed ones with NEMO support. For some measures, such as the signaling cost, H-NEMO may be more costly than centralized schemes when the velocity of the node is increasing, but behaves better in terms of packet delivery cost and handover delay.

8.1.4. NEMO-Enabled Localized Mobility Support

In [NEMO-LMS], the authors proposed an architecture to enable IP mobility for moving networks using a network-based mobility scheme based on PMIPv6. In PMIPv6, only mobile terminals are provided with IP mobility. In contrast to from host-based mobility, PMIPv6 shifts the signaling to the network side, so that the mobile access gateway (MAG) is in charge of detecting connection/disconnection of the mobile node, upon which the signaling to the Local Mobility Anchor (LMA) is triggered to guarantee a stable IP addressing assignment when the mobile node performs handover to a new MAG.

Soto et al. proposed NEMO support in PMIPv6 (N-PMIP). In this scheme, the functionality of the MAG is extended to the mobile router (MR), also called a mobile MAG (mMAG). The functionality of the mobile terminal remains unchanged, but it can receive an IPv6 prefix belonging to the PMIPv6 domain through the new functionality of the mMAG. Therefore, in N-PMIP, the mobile terminal connects to the MR as if it is connecting to a fixed MAG, and the MR connects to the fixed MAG using PMIPv6 signaling. When the mobile terminal roams to a new MAG or a new MR, the network forwards the packets through the LMA. Hence, N-PMIP defines an extended functionality in the LMA that enables a recursive lookup. First, it locates the binding entry corresponding to the mMAG. Next, it locates the entry corresponding to the fixed MAG, after which the LMA can encapsulate packets to the mMAG to which the mobile terminal is currently connected.

The performance of N-PMIP was evaluated through simulations and compared to a NEMO+MIPv6+PMIPv6 scheme, with better results obtained in N-PMIP. The work did not consider the case of multi-hop connectivity in the vehicular scenario. In addition, since the MR should be a trusted entity in the PMIP domain, it requires specific security associations that were not addressed in [NEMO-LMS].

8.1.5. Network Mobility for Vehicular Ad Hoc Networks

Chen et al. proposed a network mobility protocol to reduce handoff delay and maintain Internet connectivity to moving vehicles in a highway [NEMO-VANET]. In this work, vehicles can acquire IP addresses from other vehicles through V2V communications. At the time the vehicle goes out of the coverage of the base station, another vehicle may assist the roaming car to acquire a new IP address. Also, cars on the same or opposite lane are authorized to assist the vehicle to perform a pre-handoff.

The authors assumed that the wireless connectivity is provided by WiFi and WiMAX access networks. Also, they considered scenarios in which a single vehicle, i.e., a bus, may need two mobile routers in order to have an effective pre-handoff procedure. Evaluations are performed through simulations and the comparison schemes are the standard NEMO Basic Support protocol and the fast NEMO Basic Support protocol. Authors did not mention applicability of the scheme in other scenarios such as in urban transport schemes.

8.1.6. Performance Analysis of P-NEMO for ITS

Lee et al. proposed P-NEMO, which is a PMIPv6-based IP mobility management scheme to maintain the Internet connectivity at the vehicle as a mobile network, and provides a make-before-break mechanism when vehicles switch to a new access network [PMIP-NEMO-Analysis]. Since the standard PMIPv6 only supports mobility for a single node, the solution in [PMIP-NEMO-Analysis] adapts the protocol to reduce the signaling when a local network is to be served by an in-vehicle mobile router. To achieve this, P-NEMO extends the binding update lists at both MAG and LMA, so that the mobile router (MR) can receive a home network prefix (HNP) and a mobile network prefix (MNP). The latter prefix enables mobility for the moving network, instead of a single node as in the standard PMIPv6.

An additional feature is proposed by Lee et al. named fast P-NEMO (FP-NEMO). It adopts the fast handover approach standardized for PMIPv6 in [RFC5949] with both predictive and reactive modes. The difference of the proposed feature with the standard version is that by using the extensions provided by P-NEMO, the predictive transferring of the context from the old MAG to the new MAG also includes information for the moving network, i.e., the MNP. In that way, mobility support can be achieved not only for the mobile router, but also for mobile nodes traveling with the vehicle.

The performance of P-NEMO and F-NEMO is evaluated through an analytical model that is compared only to the standard NEMO-BS. No comparison was provided to other schemes that enable network mobility in PMIPv6 domains, such as the one presented in [NEMO-LMS].

8.1.7. Integration of VANets and Fixed IP Networks

Peng et al. proposed a novel mobility management scheme for integration of VANET and fixed IP networks [VNET-MM]. The proposed scheme deals with mobility of vehicles based on a street layout instead of a general two dimensional ad hoc network. This scheme makes use of the information provided by vehicular networks to reduce mobility management overhead. It allows multiple base stations that are close to a destination vehicle to discover the connection to the vehicle simultaneously, which leads to an improvement of the connectivity and data delivery ratio without redundant messages. The performance was assessed by using a road traffic simulator called SUMO (Simulation of Urban Mobility).

8.1.8. SDN-based Mobility Management for 5G Networks

Nguyen et al. extended their previous works on a vehicular adapted DMM considering a Software-Defined Networking (SDN) architecture [SDN-DMM]. On one hand, in their previous work, Nguyen et al. proposed DMM-PMIP and DMM-MIP architectures for VANET. The major innovation behind DMM is to distribute the Mobility Functions (MFs) through the network instead of concentrating them in one bottleneck MF, or in a hierarchically organized backbone of MFs. Highly mobile vehicular networks impose frequent IP route optimizations that lead to suboptimal routes (detours) between CN and vehicles. The suboptimality critically increases when there are nested or hierarchical MF nodes. Therefore, flattening the IP mobility architecture significantly reduces detours, as it is the role of the last MF to get the closest next MF (in most cases nearby). Yet, with an MF being distributed throughout the network, a Control plane becomes necessary in order to provide a solution for CN to address vehicles. The various solutions developed by Nguyen at al. not only showed the large benefit of a DMM approach for IPv6 mobility management, but also emphasized the critical role of an efficient Control plane.

One the other hand, SDN has recently gained attention from the Internet Networking community due to its capacity to provide a significantly higher scalability of highly dynamic flows, which is required by future 5G dynamic networks In particular, SDN also suggests a strict separation between a Control plane (SDN-Controller) and a Data plane (OpenFlow Switches) based on the OpenFlow standard. Such an architecture has two advantages that are critical for IP mobility management in VANET. First, unlike traditional routing mechanisms, OpenFlow focuses on flows rather than optimized routes. Accordingly, they can optimize routing based on flows (grouping multiple flows in one route, or allowing one flow to have different routes), and can detect broken flows much earlier than the traditional networking solutions. Second, SDN controllers may dynamically reprogram (reconfigure) OpenFlow Switches (OFS) to always keep an optimal route between CN and a vehicular node.

Nguyen et. al observed the mutual benefits IPv6 DMM could obtain from an SDN architecture, and then proposed an SDN-based DMM for VANET. In their proposed architecture, a PMIP-DMM is used, where MF is OFS for the Data plane, and one or more SDN controllers handle the Control plane. The evaluation and prototype in the paper prove that the proposed architecture can provide a higher scalability than the standard DMM.

The SDN-DMM paper makes several observations leading to a strong suggestion that IP mobility management should be based on an SDN architecture. First, SDN will be integrated into future Internet and 5G in the near future. Second, after separating the Identity and Routing addressing, IP mobility management further requires to separate the Control from the Data plane if it needs to remain scalable for VANET. Finally, Flow-based routing (in particular OpenFlow standard) will be required in future heterogeneous vehicular networks (e.g., multi-RAT and multi-protocol) and the SDN coupled with DMM provides a double benefit of dynamic flow detection/ reconfiguration and short(-er) route optimizations.

8.1.9. IP Mobility for VANETs: Challenges and Solutions

Cespedes et al. provided a survey of the challenges for NEMO Basic Support for VANET [Vehicular-IP-MM]. NEMO allows the management of a group of nodes (a mobile network) rather than a single node. However, although a vehicle and even a platoon of vehicles could be seen as a group of nodes, NEMO has not been designed considering the particularities of VANET. For example, NEMO builds a tunnel between an MR (on board of a vehicle) and its HA, which in a VANET context is suboptimal, for instance due to over-the-air tunneling cost. Also, a detour may be taken by the MR’s HA, even if the CN is nearby. Furthermore, route optimization is needed when the MR moves to a new AR.

Cespedes et al. first summarize the requirements of IP mobility management, such as reduced power at end-device, reduced handover event, reduced complexity, or reduced bandwidth consumption. VANET adds the following requirements, such as minimum signaling for route optimization (RO), per-flow separability, security and binding privacy protection, multi-homing, and switching HA. As observed, these provide several challenges to IP mobility and NEMO BS for VANET.

Cespedes et al. then describe various optimization schemes available for NEMO BS. Considering a single hop connection to CN, one major optimization direction is to avoid the HA detour and reach the CN directly. In that direction, a few optimizations are proposed, such as creating an IP tunnel between the MR and the CR directly, creating an IP tunnel between the MR and a CR (rather than the HA), a delegation mechanism allowing visiting nodes to use MIPv6 directly rather than NEMO or finally intra-NEMO optimization for a direct path within NEMO bypassing HAs.

Specific to VANET, multi-hop connection is possible to the fixed network. In that case, NEMO BS must be enhanced to avoid requiring that the path to immediate neighbors must pass by the respective HAs instead of directly. More specifically, two approaches are proposed to rely on VANET sub-IP multi-hop routing to hide a NEMO complex topology (e.g., Nested NEMO) and provide a direct route between two VANET nodes. Generally, one major challenge is security and privacy when opening a multi-hop route between a VANET and a CN. Heterogeneous multi-hop in a VANET (e.g., relying on various access technologies) corresponds to another challenge for NEMO BS as well.

Cespedes et al. conclude their paper with an overview of critical research challenges, such as Anchor Point location, the optimized usage of geographic information at the subIP as well as at the IP level to improve NEMO BS, security and privacy, and the addressing allocation schema for NEMO.

In summary, this paper illustrates that NEMO BS for VANET should avoid the HA detour as well as opening IP tunnels over the air. Also, NEMO BS could use geographic information for subIP routing when a direct link between vehicles is required to reach an AR, but also anticipate handovers and optimize ROs. From an addressing perspective, dynamic MNP assignments should be preferred, but should be secured in particular during binding update (BU).

8.2. Problem Statement for 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.

Mobility Management (MM) solution design varies, depending on scenarios: highway vs. urban roadway. Hybrid schemes (NEMO + PMIP, PMIP + DMM, etc.) usually show better performance than pure schemes. Most schemes assume that IP address configuration is already set up. Most schemes have been tested only at either simulation or analytical level. SDN can be considered as a player in the MM solution.

9. DNS Naming Service

This section surveys and analyzes DNS naming service to translate a device's DNS name into the corresponding IP address, and then discusses problem statement for DNS naming service in vehicular networks.

9.1. Existing Protocols

9.1.1. Multicast DNS

Multicast DNS (mDNS)[RFC6762] allows devices in one-hop communication range to resolve each other's DNS name into the corresponding IP address in multicast. Each device has a DNS resolver and a DNS server. The DNS resolver generates a DNS query for the device's application and the DNS server responds to a DNS query corresponding to its device's DNS name.

9.1.2. DNS Name Autoconfiguration for IoT Devices

DNS Name Autoconfiguration (DNSNA) [ID-DNSNA] proposes a DNS naming service for Internet-of-Things (IoT) devices in a large-scale network.

The DNS naming service of DNSNA consists of four steps, such as DNS name generation, DNS name duplication detection, DNS name registration, and DNS name list retrieval.

First, in DNS name generation, DNSNA allows each IoT device to generate its own DNS name with a DNS suffix (acquired from ND or DHCP) and its device information (e.g., vendor, model, and serial number).

Second, in DNS name duplication detection, each device checks whether its generated DNS name is used by another IoT device in the same subnet.

Third, in DNS name registration, each device registers its DNS name and the corresponding IPv6 address into a designated DNS server via a router. The router periodically collects DNS information of IoT devices in its the subnets corresponding ot its network interfaces.

Last, in DNS name list retrieval, a user can retrieve the DNS name list of IoT devices available to the user through the designated DNS server. Once the user retrieves the list having a DNS name and the corresponding IP address(es), it can monitor and remote-control an IoT device.

9.2. Problem Statement

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.

mDNS is designed for a small ad hoc network with wireless/wired one-hop communication range. If it is used in a vehicle's mobile network having multiple subnets, mDNS cannot effectively work in such a multi-hop network. This is because the DNS query message of each DNS resolver should be multicasted into the whole mobile network, leading to a large volume of DNS traffic.

DNSNA is designed for a large-scale network with multiple subnets. If it is used in a vehicle's mobile network having multiple subnets, DNSNA can effectively work in such a multi-hop network. This is because the DNS query message of each DNS resolver should be unicasted to the designated DNS server.

DNSNA allows each host (e.g., in-vehicle device and a user's mobile device) within a vehicle's moving network to generate its unique DNS name 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. Service Discovery

This section surveys and analyzes service discovery to translate a required service into an IP address of a device to provide such a service, and then discusses problem statement for service discovery in vehicular networks.

10.1. Existing Protocols

10.1.1. mDNS-based Service Discovery

As a popular existing service discovery protocol, DNS-based Service Discovery (DNS-SD) [RFC6763] with mDNS [RFC6762] provides service discovery.

DNS-SD uses a DNS service (SRV) resource record (RR) [RFC2782] to support the service discovery of services provided by a device or server. An SRV RR contains a service instance name, consisting of an instance name (i.e., device), a service name, a transport layer protocol, a domain name, the corresponding port number, and the DNS name of the device eligible for the requested service. With this DNS-SD, a host can search for a service instance with the SRV RR to discover a list of devices corresponding to the searched service type.

10.1.2. ND-based Service Discovery

Vehicular ND [ID-Vehicular-ND] proposes an extension of IPv6 ND for the prefix and service discovery. 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.

10.2. Problem Statement

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. For these purposes, service discovery should be performed quickly.

mDNS-based DNS-SD [RFC6762][RFC6763] can be used for service discovery between vehicles or between a vehicle and an RSU by using a multicast protocol, the service discovery requires a nonnegligible service delay due to service discovery. This is because the service discovery message should traverse the mobile network or fixed network through multicasting. This 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. The Vehicular ND [ID-Vehicular-ND] can support this approach efficiently.

11. Security and Privacy

This section surveys security and privacy in vehicular networks, and then discusses problem statement for security and privacy in vehicular networks.

11.1. Existing Protocols

11.1.1. Securing Vehicular IPv6 Communications

Fernandez et al. proposed a secure vehicular IPv6 communication scheme using Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [Securing-VCOMM]. This scheme aims at the security support for IPv6 Network Mobility (NEMO) for in-vehicle devices inside a vehicle via a Mobile Router (MR). An MR has multiple wireless interfaces, such as 3G, IEEE 802.11p, WiFi, and WiMAX. The proposed architecture consists of Vehicle ITS Station (Vehicle ITS-S), Roadside ITS Station (Roadside ITS-S), and Central ITS Station (Central ITS-S). Vehicle ITS-S is a vehicle having a mobile Network along with an MR. Roadside ITS-S is an RSU as a gateway to connect vehicular networks to the Internet. Central ITS-S is a TCC as a Home Agent (HA) for the location management of vehicles having their MR.

The proposed secure vehicular IPv6 communication scheme sets up IPsec secure sessions for control and data traffic between the MR in a Vehicle ITS-S and the HA in a Central ITS-S. Roadside ITS-S plays a role of an Access Router (AR) for Vehicle ITS-S’s MR to provide the Internet connectivity for Vehicle ITS-S via wireless interfaces, such as IEEE 802.11p, WiFi, and WiMAX. In the case where Roadside ITS-S is not available to Vehicle ITS-S, Vehicle ITS-S communicates with Central ITS-S via cellular networks (e.g., 3G). The secure communication scheme enhances the NEMO protocol that interworks with IKEv2 and IPsec in network mobility in vehicular networks.

The authors implemented their scheme and evaluated its performance in a real testbed. This testbed supports two wireless networks, such as IEEE 802.11p and 3G. The in-vehicle devices (or hosts) in Vehicle ITS-S are connected to an MR of Vehicle ITS-S via IEEE 802.11g. The test results show that their scheme supports promising secure IPv6 communications with a low impact on communication performance.

11.1.2. Authentication and Access Control

Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks [VNET-AAA]. This secuirty scheme aims at the support of safe and reliable data services in vehicular networks. It authenticates vehicles as mobile clients to use the network access and various services that are provided by service providers. Also, it ensures a confidential data transfer between communicating parties (e.g., vehicle and infrastructure node) by using IEEE 802.11i (i.e., WPA2) for secure layer-2 links.

The authors proposed a vehicular network architecture consisting of three entities, such as Access network, Wireless mobile ad hoc networks (MANETs), and Access Points (APs). Access network is the fixed network infrastructure forming the back-end of the architecture. Wireless MANETs are constructed by moving vehicles forming the front-end of the architecture. APs is the IEEE 802.11 WLAN infrastructure forming the interface between the front-end and back-end of the architecture.

For AAA services, the proposed architecture uses a Kerberos authentication model that authenticates vehicles at the entry point with the AP and also authorizes them to the access of various services. Since vehicles are authenticated by a Kerberos Authentication Server (AS) only once, the proposed security scheme can minimize the load on the AS and reduce the delay imposed by layer 2 using IEEE 802.11i.

11.2. Problem Statement

Security and privacy are paramount in the V2I and V2V networking in vehicular networks. Only authorized vehicles should be allowed to use the V2I and V2V networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

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.

For secure V2I communication, the secure channel between a mobile router in a vehicle and a fixed router in an RSU should be established, as shown in Figure 2. Also, for secure V2V communication, the secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

The security for vehicular networks should provide vehicles with AAA services in an efficient way. It should consider not only horizontal handover, but also vertical handover since vehicles have multiple wireless interfaces.

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.

12. Discussions

12.1. Summary and Analysis

This document surveyed state-of-the-arts technologies for IP-based vehicular networks, such as IP address autoconfiguration, vehicular network architecture, vehicular network routing, and mobility management.

Through this survey, it is learned that IPv6-based vehicular networking can be well-aligned with IEEE WAVE standards for various vehicular network applications, such as driving safety, efficient driving, and entertainment. However, since the IEEE WAVE standards do not recommend to use the IPv6 ND protocol for the communication efficiency under high-speed mobility, it is necessary to adapt the ND for vehicular networks with such high-speed mobility.

The concept of a link in IPv6 does not match that of a link in VANET because of the physical separation of communication ranges of vehicles in a connected VANET. That is, in a linear topology of three vehicles (Vehicle-1, Vehicle-2, and Vehicle-3), Vehicle-1 and Vehicle-2 can communicate directly with each other. Vehicle-2 and Vehicle-3 can communicate directly with each other. However, Vehicle-1 and Vehicle-3 cannot communicate directly with each other due to the out-of-communication range. For the link in IPv6, all of three vehicles are on a link, so they can communicate directly with each other. On the other hand, in VANET, this on-link communication concept is not valid in VANET. Thus, the IPv6 ND should be extended to support this multi-link subnet of a connected VANET through either ND proxy or VANET routing.

For IP-based networking, IP address autoconfiguration is a prerequisite function. Since vehicles can communicate intermittently with TCC via RSUs through V2I communications, TCC can play a role of a DHCP server to allocate unique IPv6 addresses to the vehicles. This centralized address allocation can remove the delay of the DAD procedure for testing the uniqueness of IPv6 addresses.

For routing and mobility management, most of vehicles are equipped with a GPS navigator as a dedicated navigation system or a smartphone App. With this GPS navigator, vehicles can share their current position and trajectory (i.e., navigation path) with TCC. TCC can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory). With the prediction of the vehicle mobility, TCC supports RSUs to perform data packet routing and handover proactively.

12.2. Deployment Issues

Some automobile companies (e.g., BMW and Hyundai) started to use Ethernet for a vehicle's internal network instead of the traditional Contoller Area Network (CAN) for high-speed interconnectivity among electronic control units. With this trend, the IP-based vehicular networking in this document will be popular in near future.

Self-driving technologies are being developed by many automobile companies (e.g., Tesla, BMW, GM, Honda, Toyota, and Hyundai) and IT companies (e.g., Google and Apple). Since they require high-speed interaction among vehicles, infrastructure nodes (e.g., RSU), and cloud, IP-based networking will be mandatory.

Therefore, key component technologies for the IP-based vehicular networking need to be developed for future demands along with an efficient vehicular network architecture.

13. Security Considerations

Section 11 discusses security and privacy for IP-based vehicular networking.

The security for key components in vehicular networking, such as IP address autoconfiguration, routing, mobility management, DNS naming service, and service discovery, needs to be analyzed in depth.

14. Informative References

[Address-Assignment]
Kato, T., Kadowaki, K., Koita, T., and K. Sato, "Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network", IEEE Asia-Pacific Services Computing Conference, December 2008.

[Address-Autoconf]
Fazio, M., Palazzi, C., Das, S., and M. Gerla, "Automatic IP Address Configuration in VANETs", ACM International Workshop on Vehicular Inter-Networking, September 2016.

[CA-Cuise-Control]
California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", [Online] Available: http://www.path.berkeley.edu/research/automated-and-connected-vehicles/cooperative-adaptive-cruise-control, 2017.

[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.

[DMM] Chan, H., "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

[DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), October 2010.

[ETSI-GeoNetwork-IP]
ETSI Technical Committee Intelligent Transport Systems, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols", ETSI EN 302 636-6-1, October 2013.

[ETSI-GeoNetworking]
ETSI Technical Committee Intelligent Transport Systems, "Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications; Sub-part 1: Media-Independent Functionality", ETSI EN 302 636-4-1, May 2014.

[FirstNet]
U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", [Online]
Available: https://www.firstnet.gov/, 2012.

[FirstNet-Annual-Report-2017]
First Responder Network Authority, "FY 2017: ANNUAL REPORT TO CONGRESS, Advancing Public Safety Broadband Communications", FirstNet FY 2017, December 2017.

[FleetNet]
Bechler, M., Franz, W., and L. Wolf, "Mobile Internet Access in FleetNet", 13th Fachtagung Kommunikation in verteilten Systemen, February 2001.

[GeoSAC] Baldessari, R., Bernardos, C., and M. Calderon, "GeoSAC - Scalable Address Autoconfiguration for VANET Using Geographic Networking Concepts", IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, September 2008.

[H-DMM] Nguyen, T. and C. Bonnet, "A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users", IEEE International Conference on Communications, June 2015.

[H-NEMO] Nguyen, T. and C. Bonnet, "A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility", IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, June 2015.

[ID-DNSNA]
Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-02 (work in progress), March 2018.

[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-02 (work in progress), March 2018.

[Identity-Management]
Wetterwald, M., Hrizi, F., and P. Cataldi, "Cross-layer Identities Management in ITS Stations", The 10th International Conference on ITS Telecommunications, November 2010.

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

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

[IP-Passing-Protocol]
Chen, Y., Hsu, C., and W. Yi, "An IP Passing Protocol for Vehicular Ad Hoc Networks with Network Fragmentation", Elsevier Computers & Mathematics with Applications, January 2012.

[IPv6-WAVE]
Baccelli, E., Clausen, T., and R. Wakikawa, "IPv6 Operation for WAVE - Wireless Access in Vehicular Environments", IEEE Vehicular Networking Conference, December 2010.

[ISO-ITS-IPv6]
ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012.

[Joint-IP-Networking]
Petrescu, A., Boc, M., and C. Ibars, "Joint IP Networking and Radio Architecture for Vehicular Networks", 11th International Conference on ITS Telecommunications, August 2011.

[LAGAD] Abrougui, K., Boukerche, A., and R. Pazzi, "Location-Aided Gateway Advertisement and Discovery Protocol for VANets", IEEE Transactions on Vehicular Technology, Vol. 59, No. 8, October 2010.

[NEMO-LMS] Soto, I., Bernardos, C., Calderon, M., Banchs, A., and A. Azcorra, "NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios", IEEE Communications Magazine, May 2009.

[NEMO-VANET] Chen, Y., Hsu, C., and C. Cheng, "Network Mobility Protocol for Vehicular Ad Hoc Networks", Wiley International Journal of Communication Systems, November 2014.

[PMIP-NEMO-Analysis] Lee, J., Ernst, T., and N. Chilamkurti, "Performance Analysis of PMIPv6-Based Network Mobility for Intelligent Transportation Systems", IEEE Transactions on Vehicular Technology, January 2012.

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

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

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for Specifying the Location of Services (DNS SRV)", RFC 2782, February 2000.

[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.

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

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

[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.

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

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

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

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

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

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

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

[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.

[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.

[SAINTplus]
Shen, Y., Lee, J., Jeong, H., Jeong, J., Lee, E., and D. Du, "SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization", IEEE Transactions on Intelligent Transportation Systems, June 2017.

[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.

[SDN-DMM] Nguyen, T., Bonnet, C., and J. Harri, "SDN-based Distributed Mobility Management for 5G Networks", IEEE Wireless Communications and Networking Conference, April 2016.

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

[Truck-Platooning]
California Partners for Advanced Transportation Technology (PATH), "Automated Truck Platooning", [Online] Available: http://www.path.berkeley.edu/research/automated-and-connected-vehicles/truck-platooning, 2017.

[VANET-Geo-Routing]
Tsukada, M., Jemaa, I., Menouar, H., Zhang, W., Goleva, M., and T. Ernst, "Experimental Evaluation for IPv6 over VANET Geographic Routing", IEEE International Wireless Communications and Mobile Computing Conference, June 2010.

[Vehicular-DTN]
Soares, V., Farahmand, F., and J. Rodrigues, "A Layered Architecture for Vehicular Delay-Tolerant Networks", IEEE Symposium on Computers and Communications, July 2009.

[Vehicular-IP-MM]
Cespedes, S., Shen, X., and C. Lazo, "IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions", IEEE Communications Magazine, May 2011.

[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, March 2013.

[VNET-AAA]
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.

[VNET-Framework]
Jemaa, I., Shagdar, O., and T. Ernst, "A Framework for IP and non-IP Multicast Services for Vehicular Networks", Third International Conference on the Network of the Future, November 2012.

[VNET-MM] Peng, Y. and J. Chang, "A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks and Fixed IP Networks", Springer Mobile Networks and Applications, February 2010.

[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.

Appendix A. Acknowledgments

This work was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2017M3C4A7065980). This work was supported in part by the Global Research Laboratory Program (2013K1A1A2A02078326) through NRF and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science and ICT. This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

Appendix B. Contributors

This document is a group work of IPWAVE working group, greatly benefiting from inputs and texts by Rex Buddenberg (Naval Postgraduate School), Thierry Ernst (YoGoKo), Bokor Laszlo (Budapest University of Technology and Economics), Jose Santa Lozanoi (Universidad of Murcia), Richard Roy (MIT), and Francois Simon (Pilot). The authors sincerely appreciate their contributions.

The following are co-authors of this document:

Nabil Benamar
Department of Computer Sciences
High School of Technology of Meknes
Moulay Ismail University
Morocco

Phone: +212 6 70 83 22 36
EMail: benamar73@gmail.com

Sandra Cespedes
Department of Electrical Engineering
Universidad de Chile
Av. Tupper 2007, Of. 504
Santiago, 8370451
Chile

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

Jerome Haerri
Communication Systems Department
EURECOM

Sophia-Antipolis
France

Phone: +33 4 93 00 81 34
EMail: jerome.haerri@eurecom.fr

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

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

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

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

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

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

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

Yiwen Chris Shen

Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu
URI: http://iotlab.skku.edu/people-chris-shen.php

Michelle Wetterwald
FBConsulting
21, Route de Luxembourg
Wasserbillig, Luxembourg L-6633
Luxembourg

EMail: Michelle.Wetterwald@gmail.com

Appendix C. Changes from draft-ietf-ipwave-vehicular-networking-01

The following changes are made from draft-ietf-ipwave-vehicular-networking-01:

- In Section 1, the following sentence is added: The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC], service in the Intelligent Transportation Systems (ITS Radio Service in the 5.850 - 5.925 GHz band (5.9 GHz band).

- In Section 2, the definition of Road-Side Unit (RSU) is modified as a node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, etc.) for wireless communication with vehicles and is also connected to the Internet as a router or switch for packet forwarding.

- In Section 2, DMM is defined as the acronym for "Distributed Mobility Management" [DMM].

- In Section 3.1, the following sentence is clarified along with relevant references: The current RAN is mainly constructed by 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Annual-Report-2017], but DSRC-based vehicular networks can be used for V2I in near future [DSRC].

- o In Section 4.1.1, the following sentences are clarified along with relevant references: The standard WAVE [WAVE-1609.0][WAVE-1609.3] does not support Duplicate Address Detection (DAD) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862] by having its own efficient IP address configuration mechanism based on a WAVE Service Advertisement (WSA) management frame [WAVE-1609.3]. It does not support both seamless communications for Internet services and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU), either.

- o The contents are clarified with typo corrections and rephrasing.

Author's Address

Jaehoon Paul Jeong (editor)
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
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

IPWAVE Working Group
Internet-Draft
Intended status: Informational
Expires: January 30, 2021

J. Jeong, Ed.
Sungkyunkwan University
July 29, 2020

IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-19

Abstract

This document discusses the problem statement and use cases of IPv6-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document explains use cases using V2V, V2I, and V2X networking. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then lists up requirements for the extensions of those IPv6 protocols for IPv6-based vehicular networking.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Vehicular networking studies have mainly focused on improving safety and efficiency, and also enabling entertainment in vehicular networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC] in the Intelligent Transportation Systems (ITS) with the frequency band of 5.850 - 5.925 GHz (i.e., 5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. The European Union (EU) allocated radio spectrum for safety-related and non-safety-related applications of ITS with the frequency band of 5.875 - 5.905 GHz, as part of the Commission Decision 2008/671/EC [EU-2008-671-EC].

For direct inter-vehicular wireless connectivity, IEEE has amended standard 802.11 (commonly known as Wi-Fi) to enable safe driving services based on DSRC for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC of the DSRC, while IEEE 1609.2 [WAVE-1609.2] covers security aspects, IEEE 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE 1609.4 [WAVE-1609.4] specifies the multi-channel operation. IEEE 802.11p was first a separate amendment, but was later rolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) in 2012 [IEEE-802.11-OCB].

3GPP has standardized Cellular Vehicle-to-Everything (C-V2X) communications to support V2X in LTE mobile networks (called LTE V2X) and V2X in 5G mobile networks (called 5G V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. With C-V2X, vehicles can directly communicate with each other without relay nodes (e.g., eNodeB in LTE and gNodeB in 5G).

Along with these WAVE standards and C-V2X standards, regardless of a wireless access technology under the IP stack of a vehicle, vehicular networks can operate IP mobility with IPv6 [RFC8200] and Mobile IPv6 protocols (e.g., Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 (PMIPv6) [RFC5213], Distributed Mobility Management (DMM) [RFC7333], Locator/ID Separation Protocol (LISP) [RFC6830BIS], and Asymmetric Extended Route Optimization (AERO) [RFC6706BIS]). In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6] [ISO-ITS-IPv6-AMD1].

This document describes use cases and a problem statement about IPv6-based vehicular networking for ITS, which is named IPv6 Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in ITS. Next, for IPv6-based vehicular networks, it makes a gap analysis of current IPv6 protocols (e.g., IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy), and then lists up requirements for the extensions of those IPv6 protocols, which are tailored to IPv6-based vehicular networking. Thus, this document is intended to motivate development of key protocols for IPWAVE.

2. Terminology

This document uses the terminology described in [RFC8691]. In addition, the following terms are defined below:

- Class-Based Safety Plan: A vehicle can make a safety plan by classifying the surrounding vehicles into different groups for safety purposes according to the geometrical relationship among them. The vehicle groups can be classified as Line-of-Sight Unsafe, Non-Line-of-Sight Unsafe, and Safe groups [CASD].

- Context-Awareness: A vehicle can be aware of spatial-temporal mobility information (e.g., position, speed, direction, and acceleration/deceleration) of surrounding vehicles for both safety and non-safety uses through sensing or communication [CASD].

- DMM: "Distributed Mobility Management" [RFC7333][RFC7429].

- Edge Computing (EC): It is the local computing near an access network (i.e., edge network) for the sake of vehicles and pedestrians.

- Edge Computing Device (ECD): It is a computing device (or server) for edge computing for the sake of vehicles and pedestrians.

- Edge Network (EN): It is an access network that has an IP-RSU for wireless communication with other vehicles having an IP-OBU and wired communication with other network devices (e.g., routers, IP-RSUs, ECDs, servers, and MA). It may have a Global Positioning System (GPS) radio receiver for its position recognition and the localization service for the sake of vehicles.

- IP-OBU: "Internet Protocol On-Board Unit": An IP-OBU denotes a computer situated in a vehicle (e.g., car, bicycle, autobike, motor cycle, and a similar one) and a device (e.g., smartphone and IoT device). It has at least one IP interface that runs in IEEE 802.11-OCB and has an "OBU" transceiver. Also, it may have an IP interface that runs in Cellular V2X (C-V2X) [TS-23.285-3GPP] [TR-22.886-3GPP][TS-23.287-3GPP]. See the definition of the term "OBU" in [RFC8691].

- IP-RSU: "IP Roadside Unit": An IP-RSU is situated along the road. It has at least two distinct IP-enabled interfaces. The wireless PHY/MAC layer of at least one of its IP-enabled interfaces is configured to operate in 802.11-OCB mode. An IP-RSU communicates with the IP-OBU over an 802.11 wireless link operating in OCB mode. Also, it may have an IP interface that runs in C-V2X along with an "RSU" transceiver. An IP-RSU is similar to an Access Network Router (ANR), defined in [RFC3753], and a Wireless Termination Point (WTP), defined in [RFC5415]. See the definition of the term "RSU" in [RFC8691].

- LiDAR: "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.

- Mobility Anchor (MA): A node that maintains IPv6 addresses and mobility information of vehicles in a road network to support their IPv6 address autoconfiguration and mobility management with a binding table. An MA has End-to-End (E2E) connections (e.g., tunnels) with IP-RSUs under its control for the address autoconfiguration and mobility management of the vehicles. This MA is similar to a Local Mobility Anchor (LMA) in PMIPv6 [RFC5213] for network-based mobility management.

- OCB: "Outside the Context of a Basic Service Set - BSS". It is a mode of operation in which a Station (STA) is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality [IEEE-802.11-OCB].

- 802.11-OCB: It refers to the mode specified in IEEE Std 802.11-2016 [IEEE-802.11-OCB] when the MIB attribute dot11OCBActivited is 'true'.

- Platooning: Moving vehicles can be grouped together to reduce air-resistance for energy efficiency and reduce the number of drivers such that only the leading vehicle has a driver, and the other vehicles are autonomous vehicles without a driver and closely follow the leading vehicle [Truck-Platooning].

- Traffic Control Center (TCC): A system that manages road infrastructure nodes (e.g., IP-RSUs, MAs, traffic signals, and loop detectors), and also maintains 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 part of a vehicular cloud for vehicular networks.

- Vehicle: A Vehicle in this document is a node that has an IP-OBU for wireless communication with other vehicles and IP-RSUs. It has a GPS radio navigation receiver for efficient navigation. Any device having an IP-OBU and a GPS receiver (e.g., smartphone and table PC) can be regarded as a vehicle in this document.

- Vehicular Ad Hoc Network (VANET): A network that consists of vehicles interconnected by wireless communication. Two vehicles in a VANET can communicate with each other using other vehicles as relays even where they are out of one-hop wireless communication range.

- o Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network forwarding elements (e.g., switch and router).

- o V2D: "Vehicle to Device". It is the wireless communication between a vehicle and a device (e.g., smartphone and IoT device).

- o V2I2D: "Vehicle to Infrastructure to Device". It is the wireless communication between a vehicle and a device (e.g., smartphone and IoT device) via an infrastructure node (e.g., IP-RSU).

- o V2I2V: "Vehicle to Infrastructure to Vehicle". It is the wireless communication between a vehicle and another vehicle via an infrastructure node (e.g., IP-RSU).

- o V2I2X: "Vehicle to Infrastructure to Everything". It is the wireless communication between a vehicle and another entity (e.g., vehicle, smartphone, and IoT device) via an infrastructure node (e.g., IP-RSU).

- o V2X: "Vehicle to Everything". It is the wireless communication between a vehicle and any entity (e.g., vehicle, infrastructure node, smartphone, and IoT device), including V2V, V2I, and V2D.

- o VIP: "Vehicular Internet Protocol". It is an IPv6 extension for vehicular networks including V2V, V2I, and V2X.

- o VMM: "Vehicular Mobility Management". It is an IPv6-based mobility management for vehicular networks.

- o VND: "Vehicular Neighbor Discovery". It is an IPv6 ND extension for vehicular networks.

- o VSP: "Vehicular Security and Privacy". It is an IPv6-based security and privacy for vehicular networks.

- o WAVE: "Wireless Access in Vehicular Environments" [WAVE-1609.0].

3. Use Cases

This section explains use cases of V2V, V2I, and V2X networking. The use cases of the V2X networking exclude the ones of the V2V and V2I networking, but include Vehicle-to-Pedestrian (V2P) and Vehicle-to-Device (V2D).

IP is widely used among popular end-user devices (e.g., smartphone and tablet) in the Internet. Applications (e.g., navigator application) for those devices can be extended such that the V2V use cases in this section can work with IPv6 as a network layer protocol and IEEE 802.11-OCB as a link layer protocol. In addition, IPv6 security needs to be extended to support those V2V use cases in a safe, secure, privacy-preserving way.

The use cases presented in this section serve as the description and motivation for the need to extend IPv6 and its protocols to facilitate "Vehicular IPv6". Section 5 summarizes the overall problem statement and IPv6 requirements. Note that the adjective "Vehicular" in this document is used to represent extensions of existing protocols such as IPv6 Neighbor Discovery, IPv6 Mobility Management (e.g., PMIPv6 [RFC5213] and DMM [RFC7429]), and IPv6 Security and Privacy Mechanisms rather than new "vehicular-specific" functions. Refer to Section 5 for the problem statement of the requirements of vehicular IPv6.

3.1. V2V

The use cases of V2V networking discussed in this section include

- o Context-aware navigation for safe driving and collision avoidance;
- o Cooperative adaptive cruise control in a roadway;
- o Platooning in a highway;
- o Cooperative environment sensing;
- o Collision avoidance service of end systems of Urban Air Mobility (UAM) [UAM-ITS].

These five techniques will be important elements for autonomous vehicles, which may be either terrestrial vehicles or UAM end systems.

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely by alerting them to dangerous obstacles and situations. That is, a CASD navigator displays obstacles or neighboring vehicles relevant to possible collisions in real-time through V2V networking. CASD provides vehicles with a class-based automatic safety action plan, which considers three situations, namely, the Line-of-Sight unsafe, Non-Line-of-Sight unsafe, and safe situations. This action plan can be put into action among multiple vehicles using V2V networking.

Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps individual vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles in an urban roadway or a highway. Thus, CACC can help adjacent vehicles to efficiently adjust their speed in an interactive way through V2V networking in order to avoid a collision.

Platooning [Truck-Platooning] allows a series (or group) of vehicles (e.g., trucks) to follow each other very closely. Trucks can use V2V communication in addition to forward sensors in order to maintain constant clearance between two consecutive vehicles at very short gaps (from 3 meters to 10 meters). Platooning can maximize the throughput of vehicular traffic in a highway and reduce the gas consumption because the leading vehicle can help the following vehicles to experience less air resistance.

Cooperative-environment-sensing use cases suggest that vehicles can share environmental information (e.g., air pollution, hazards/ obstacles, slippery areas by snow or rain, road accidents, traffic congestion, and driving behaviors of neighboring vehicles) from various vehicle-mounted sensors, such as radars, LiDARs, and cameras, with other vehicles and pedestrians. [Automotive-Sensing] introduces millimeter-wave vehicular communication for massive automotive sensing. A lot of data can be generated by those sensors, and these data typically need to be routed to different destinations. In addition, from the perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver-operated vehicles. Through cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the other vehicles and environment. Vehicles can also share their intended maneuvering information (e.g., lane change, speed change, ramp in-and-out, cut-in, and abrupt braking) with neighboring vehicles. Thus, this information sharing can help the vehicles behave as more efficient traffic flows and minimize unnecessary acceleration and deceleration to achieve the best ride comfort.

A collision avoidance service of UAM end systems in air can be envisioned as a use case in air vehicular environments. This use case is similar to the context-aware navigator for terrestrial vehicles. Through V2V coordination, those UAM end systems (e.g., drones) can avoid a dangerous situation (e.g., collision) in three-dimensional space rather than two-dimensional space for terrestrial vehicles. Also, UAM end systems (e.g., flying car) with only a few meters off the ground can communicate with terrestrial vehicles with wireless communication technologies (e.g., DSRC, LTE, and C-V2X). Thus, V2V means any vehicle to any vehicle, whether the vehicles are ground-level or not.

To encourage more vehicles to participate in this cooperative environmental sensing, a reward system will be needed. Sensing activities of each vehicle need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) through other vehicles or infrastructure. In the case of a blockchain, each sensing message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain].

The existing IPv6 protocol must be augmented through the addition of an Overlay Multilink Network (OMNI) Interface [OMNI] and/or protocol changes in order to support wireless single-hop V2V communications as well as wireless multihop V2V communications. Thus, the IPv6 needs to support both single-hop and multihop communications in a wireless medium so that vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard in a highway.

To support applications of these V2V use cases, the functions of IPv6 such as VND and VSP are prerequisites for IPv6-based packet exchange and secure, safe communication between two vehicles.

3.2. V2I

The use cases of V2I networking discussed in this section include

- o Navigation service;
- o Energy-efficient speed recommendation service;
- o Accident notification service;
- o Electric vehicle (EV) charging service;
- o UAM navigation service with efficient battery charging.

A navigation service, for example, the Self-Adaptive Interactive Navigation Tool(SAINT) [SAINT], using V2I networking interacts with a TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles along appropriate navigation paths in real time. The enhanced version of SAINT [SAINTplus] can give fast moving paths to emergency vehicles (e.g., ambulance and fire engine) to let them reach an accident spot while redirecting other vehicles near the accident spot into efficient detour paths.

Either a TCC or an ECD can recommend an energy-efficient speed to a vehicle that depends on its traffic environment and traffic signal scheduling [SignalGuru]. For example, when a vehicle approaches an intersection area and a red traffic light for the vehicle becomes turned on, it needs to reduce its speed to save fuel consumption. In this case, either a TCC or an ECD, which has the up-to-date trajectory of the vehicle and the traffic light schedule, can notify the vehicle of an appropriate speed for fuel efficiency. [Fuel-Efficient] studies fuel-efficient route and speed plans for platooned trucks.

The emergency communication between accident vehicles (or emergency vehicles) and a TCC can be performed via either IP-RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, e.g., emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to the FirstNet's network core. The current RAN is mainly constructed using 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Report], but it is expected that DSRC-based vehicular networks [DSRC] will be available for V2I and V2V in the near future.

An EV charging service with V2I can facilitates the efficient battery charging of EVs. In the case where an EV charging station is connected to an IP-RSU, an EV can be guided toward the deck of the EV charging station through a battery charging server connected to the IP-RSU. In addition to this EV charging service, other value-added services (e.g., air firmware/software update and media streaming) can be provided to an EV while it is charging its battery at the EV charging station.

A UAM navigation service with efficient battery charging can make the battery charging schedule of UAM end systems (e.g., drone) for long-distance flying [CBDN]. For this battery charging schedule, a UAM end system can communicate with an infrastructure node (e.g., IP-RSU) toward a cloud server via V2I communications. This cloud server can coordinate the battery charging schedules of multiple UAM end systems for their efficient navigation path, considering flight time from their current position to a battery charging station, waiting time in a waiting queue at the station, and battery charging time at the station.

The existing IPv6 protocol must be augmented through the addition of an OMNI interface and/or protocol changes in order to support wireless multihop V2I communications in a highway where RSUs are sparsely deployed, so a vehicle can reach the wireless coverage of an

RSU through the multihop data forwarding of intermediate vehicles. Thus, IPv6 needs to be extended for multihop V2I communications.

To support applications of these V2I use cases, the functions of IPv6 such as VND, VMM, and VSP are prerequisites for IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and a server in the vehicular cloud.

3.3. V2X

The use case of V2X networking discussed in this section is for a pedestrian protection service.

A pedestrian protection service, such as Safety-Aware Navigation Application (SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with a network device for wireless communication (e.g., Wi-Fi) with an IP-RSU. Vehicles and pedestrians can also communicate with each other via an IP-RSU. An edge computing device behind the IP-RSU can collect the mobility information from vehicles and pedestrians, compute wireless communication scheduling for the sake of them. This scheduling can save the battery of each pedestrian's smartphone by allowing it to work in sleeping mode before the communication with vehicles, considering their mobility.

For Vehicle-to-Pedestrian (V2P), a vehicle can directly communicate with a pedestrian's smartphone by V2X without IP-RSU relaying. Light-weight mobile nodes such as bicycles may also communicate directly with a vehicle for collision avoidance using V2V.

The existing IPv6 protocol must be augmented through the addition of an OMNI interface and/or protocol changes in order to support wireless multihop V2X (or V2I2X) communications in an urban road network where RSUs are deployed at intersections, so a vehicle (or a pedestrian's smartphone) can reach the wireless coverage of an RSU through the multihop data forwarding of intermediate vehicles (or pedestrians' smartphones). Thus, IPv6 needs to be extended for multihop V2X (or V2I2X) communications.

To support applications of these V2X use cases, the functions of IPv6 such as VND, VMM, and VSP are prerequisites for IPv6-based packet exchange, transport-layer session continuity, and secure, safe communication between a vehicle and a pedestrian either directly or indirectly via an IP-RSU.

4. Vehicular Networks

This section describes an example vehicular network architecture supporting V2V, V2I, and V2X communications in vehicular networks. It describes an internal network within a vehicle or an edge network (called EN). It explains not only the internetworking between the internal networks of a vehicle and an EN via wireless links, but also the internetworking between the internal networks of two vehicles via wireless links.

```
                     Traffic Control Center in Vehicular Cloud
                    *******************************************
+-------------+    *                                           *
|Corresponding|   *             +-----------------+             *
|    Node     |<->*             | Mobility Anchor |             *
+-------------+   *             +-----------------+             *
                  *                      ^                      *
                  *                      |                      *
                   *                     v                     *
                    *******************************************
                    ^                   ^                     ^
                    |                   |                     |
                    |                   |                     |
                    v                   v                     v
              +---------+           +---------+           +---------+
              | IP-RSU1 |<--------->| IP-RSU2 |<--------->| IP-RSU3 |
              +---------+           +---------+           +---------+
                  ^                     ^                    ^
                  :                     :                    :
           +-----------------+ +-----------------+   +-----------------+
           |      : V2I      | |        : V2I    |   |       : V2I     |
           |      v          | |        v        |   |       v         |
+--------+ |   +--------+    | |   +--------+    |   |   +--------+    |
|Vehicle1|===> |Vehicle2|===>| |   |Vehicle3|===>|   |   |Vehicle4|===>|
+--------+<...>+--------+<........>+--------+    |   |   +--------+    |
           V2V     ^         V2V        ^        |   |        ^        |
           |       : V2V     | |        : V2V    |   |        : V2V    |
           |       v         | |        v        |   |        v        |
           |  +--------+     | |   +--------+    |   |    +--------+   |
           |  |Vehicle5|===> | |   |Vehicle6|===>|   |    |Vehicle7|==>|
           |  +--------+     | |   +--------+    |   |    +--------+   |
           +-----------------+ +-----------------+   +-----------------+
                 Subnet1              Subnet2              Subnet3
                (Prefix1)            (Prefix2)            (Prefix3)

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

Figure 1: An Example Vehicular Network Architecture for V2I and V2V

4.1. Vehicular Network Architecture

Figure 1 shows an example vehicular network architecture for V2I and V2V in a road network [OMNI]. The vehicular network architecture contains vehicles (including IP-OBU), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as components. Note that the components of the vehicular network architecture can be mapped to those of an IP-based aeronautical network architecture in [OMNI], as shown in Figure 2.

Vehicular Network	Aeronautical Network
IP-RSU	Access Router (AR)
Vehicle (IP-OBU)	Mobile Node (MN)
Moving Network	End User Network (EUN)
Mobility Anchor	Mobility Service Endpoint (MSE)
Vehicular Cloud	Internetwork (INET) Routing System

Figure 2: Mapping between Vehicular Network Components and Aeronautical Network Components

These components are not mandatory, and they can be deployed into vehicular networks in various ways. Some of them (e.g., Mobility Anchor, Traffic Control Center, and Vehicular Cloud) may not be needed for the vehicular networks according to target use cases in Section 3.

An existing network architecture (e.g., an IP-based aeronautical network architecture [OMNI][UAM-ITS], a network architecture of PMIPv6 [RFC5213], and a low-power and lossy network architecture [RFC6550]) can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. In a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). For example, the OMNI interface and/or RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] can be extended to support a multihop V2I since a vehicle can take advantage of other vehicles as relay nodes to reach the RSU. Also, RPL can be extended to support both multihop V2V and V2X in the similar way.

Wireless communications needs to be considered for end systems for Urban Air Mobility (UAM) such as flying cars and taxis [UAM-ITS].

These UAM end systems may have multiple wireless transmission media interfaces (e.g., cellular, communications satellite (SATCOM), short-range omni-directional interfaces), which are offered by different data link service providers. To support not only the mobility management of the UAM end systems, but also the multihop and multilink communications of the UAM interfaces, the UAM end systems can employ an Overlay Multilink Network (OMNI) interface [OMNI] as a virtual Non-Broadcast Multiple Access (NBMA) connection to a serving ground domain infrastructure. This infrastructure can be configured over the underlying data links. The OMNI interface and its link model provide a means of multilink, multihop and mobility coordination to the legacy IPv6 ND messaging [RFC4861] according to the NBMA principle. Thus, the OMNI link model can support efficient UAM internetworking services without additional mobility messaging, and without any modification to the IPv6 ND messaging services or link model.

As shown in this figure, IP-RSUs as routers and vehicles with IP-OBU have wireless media interfaces for VANET. Furthermore, the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking. Note that 2001:DB8::/32 is a documentation prefix [RFC3849] for example prefixes in this document, and also that any routable IPv6 address needs to be routable in a VANET and a vehicular network including IP-RSUs.

In Figure 1, three IP-RSUs (IP-RSU1, IP-RSU2, and IP-RSU3) are deployed in the road network and are connected with each other through the wired networks (e.g., Ethernet). A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of IP-RSUs and vehicles in the road network. A Mobility Anchor (MA) may be located in the TCC as a mobility management controller. Vehicle2, Vehicle3, and Vehicle4 are wirelessly connected to IP-RSU1, IP-RSU2, and IP-RSU3, respectively. The three wireless networks of IP-RSU1, IP-RSU2, and IP-RSU3 can belong to three different subnets (i.e., Subnet1, Subnet2, and Subnet3), respectively. Those three subnets use three different prefixes (i.e., Prefix1, Prefix2, and Prefix3).

Multiple vehicles under the coverage of an RSU share a prefix such that mobile nodes share a prefix of a Wi-Fi access point in a wireless LAN. This is a natural characteristic in infrastructure-based wireless networks. For example, in Figure 1, two vehicles (i.e., Vehicle2, and Vehicle5) can use Prefix 1 to configure their IPv6 global addresses for V2I communication. Alternatively, mobile nodes can employ an OMNI interface and use their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network without requiring the messaging of IPv6 Stateless Address Autoconfiguration

(SLAAC) [RFC4862], which uses an on-link prefix provided by the (visited) wireless LAN; this technique is known as "Bring-Your-Own-Addresses".

A single subnet prefix announced by an RSU can span multiple vehicles in VANET. For example, in Figure 1, for Prefix 1, three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle5) can construct a connected VANET. Also, for Prefix 2, two vehicles (i.e., Vehicle3 and Vehicle6) can construct another connected VANET, and for Prefix 3, two vehicles (i.e., Vehicle4 and Vehicle7) can construct another connected VANET. Alternatively, each vehicle could employ an OMNI interface with their own ULAs such that no topologically-oriented subnet prefixes need be announced by the RSU.

In wireless subnets in vehicular networks (e.g., Subnet1 and Subnet2 in Figure 1), vehicles can construct a connected VANET (with an arbitrary graph topology) and can communicate with each other via V2V communication. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the wireless communication range of each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., IP-RSU2 and IP-RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range of each other.

For IPv6 packets transported over IEEE 802.11-OCB, [RFC8691] specifies several details, including Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. An Ethernet Adaptation (EA) layer is in charge of transforming some parameters between the IEEE 802.11 MAC layer and the IPv6 network layer, which is located between the IEEE 802.11-OCB's logical link control layer and the IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IPv6-based vehicular networks.

An IPv6 mobility solution is needed for the guarantee of communication continuity in vehicular networks so that a vehicle's TCP session can be continued, or UDP packets can be delivered to a vehicle as a destination without loss while it moves from an IP-RSU's wireless coverage to another IP-RSU's wireless coverage. In Figure 1, assuming that Vehicle2 has a TCP session (or a UDP session) with a corresponding node in the vehicular cloud, Vehicle2 can move from IP-RSU1's wireless coverage to IP-RSU2's wireless coverage. In this case, a handover for Vehicle2 needs to be performed by either a host-based mobility management scheme (e.g., MIPv6 [RFC6275]) or a network-based mobility management scheme (e.g., PMIPv6 [RFC5213] and AERO [RFC6706BIS]).

In the host-based mobility scheme (e.g., MIPv6), an IP-RSU plays a role of a home agent. On the other hand, in the network-based mobility scheme (e.g., PMIPv6, an MA plays a role of a mobility management controller such as a Local Mobility Anchor (LMA) in PMIPv6, which also serves vehicles as a home agent, and an IP-RSU plays a role of an access router such as a Mobile Access Gateway (MAG) in PMIPv6 [RFC5213]. The host-based mobility scheme needs client functionality in IPv6 stack of a vehicle as a mobile node for mobility signaling message exchange between the vehicle and home agent. On the other hand, the network-based mobility scheme does not need such a client functionality for a vehicle because the network infrastructure node (e.g., MAG in PMIPv6) as a proxy mobility agent handles the mobility signaling message exchange with the home agent (e.g., LMA in PMIPv6) for the sake of the vehicle.

There are a scalability issue and a route optimization issue in the network-based mobility scheme (e.g., PMIPv6) when an MA covers a large vehicular network governing many IP-RSUs. In this case, a distributed mobility scheme (e.g., DMM [RFC7429]) can mitigate the scalability issue by distributing multiple MAs in the vehicular network such that they are positioned closer to vehicles for route optimization and bottleneck mitigation in a central MA in the network-based mobility scheme. All these mobility approaches (i.e., a host-based mobility scheme, network-based mobility scheme, and distributed mobility scheme) and a hybrid approach of a combination of them need to provide an efficient mobility service to vehicles moving fast and moving along with the relatively predictable trajectories along the roadways.

In vehicular networks, the control plane can be separated from the data plane for efficient mobility management and data forwarding by using the concept of Software-Defined Networking (SDN) [RFC7149][DMM-FPC]. Note that Forwarding Policy Configuration (FPC) in [DMM-FPC], which is a flexible mobility management system, can manage the separation of data-plane and control-plane in DMM. In SDN, the control plane and data plane are separated for the efficient management of forwarding elements (e.g., switches and routers) where an SDN controller configures the forwarding elements in a centralized way and they perform packet forwarding according to their forwarding tables that are configured by the SDN controller. An MA as an SDN controller needs to efficiently configure and monitor its IP-RSUs and vehicles for mobility management, location management, and security services.

The mobility information of a GPS receiver mounted in its vehicle (e.g., position, speed, and direction) can be used to accommodate mobility-aware proactive handover schemes, which can perform the handover of a vehicle according to its mobility and the wireless signal strength of a vehicle and an IP-RSU in a proactive way.

Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275] and PMIPv6 [RFC5213], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. IP tunneling over the wireless link should be avoided for performance efficiency. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle's internal network (i.e., moving network) and an EN's internal network (i.e., fixed network) via V2I communication. The internal network of a vehicle is nowadays constructed with Ethernet by many automotive vendors [In-Car-Network]. Note that an EN can accommodate multiple routers (or switches) and servers (e.g., ECDs, navigation server, and DNS server) in its internal network.

A vehicle's internal network often uses Ethernet to interconnect Electronic Control Units (ECUs) in the vehicle. The internal network can support Wi-Fi and Bluetooth to accommodate a driver's and passenger's mobile devices (e.g., smartphone or tablet). The network topology and subnetting depend on each vendor's network configuration for a vehicle and an EN. It is reasonable to consider the interaction between the internal network and an external network within another vehicle or an EN.

```
                                                    +-----------------+
                           (*)<........>(*)  +----->| Vehicular Cloud |
        (2001:DB8:1:1::/64) |            |   |      +-----------------+
   +------------------------------+  +---------------------------------+
   |                        v     |  |   v   v                         |
   | +-------+          +-------+ |  | +-------+          +-------+    |
   | | Host1 |          |IP-OBU1| |  | |IP-RSU1|          | Host3 |    |
   | +-------+          +-------+ |  | +-------+          +-------+    |
   |     ^                  ^     |  |     ^                  ^        |
   |     |                  |     |  |     |                  |        |
   |     v                  v     |  |     v                  v        |
   | ---------------------------- |  | ------------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |     ^ 2001:DB8:20:1::/64        |
   |                    |         |  |     |                           |
   |                    v         |  |     v                           |
   | +-------+      +-------+     |  | +-------+ +-------+   +-------+ |
   | | Host2 |      |Router1|     |  | |Router2| |Server1|...|ServerN| |
   | +-------+      +-------+     |  | +-------+ +-------+   +-------+ |
   |     ^              ^         |  |     ^         ^           ^     |
   |     |              |         |  |     |         |           |     |
   |     v              v         |  |     v         v           v     |
   | ---------------------------- |  | ------------------------------- |
   |      2001:DB8:10:2::/64      |  |       2001:DB8:20:2::/64        |
   +------------------------------+  +---------------------------------+
      Vehicle1 (Moving Network1)            EN1 (Fixed Network1)

      <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 3: Internetworking between Vehicle and Edge Network

As shown in Figure 3, as internal networks, a vehicle's moving network and an EN's fixed network are self-contained networks having multiple subnets and having an edge router (e.g., IP-OBU and IP-RSU) for the communication with another vehicle or another EN. The internetworking between two internal networks via V2I communication requires the exchange of the network parameters and the network prefixes of the internal networks. For the efficiency, the network prefixes of the internal networks (as a moving network) in a vehicle need to be delegated and configured automatically. Note that a moving network's network prefix can be called a Mobile Network Prefix (MNP) [OMNI].

Figure 3 also shows the internetworking between the vehicle's moving network and the EN's fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2), and two routers (IP-OBU1 and Router1). There exists another internal network (Fixed Network1) inside EN1. EN1 has one host (Host3), two routers (IP-RSU1 and Router2), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1's IP-OBU1 (as a mobile router) and EN1's IP-RSU1 (as a fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2I networking. Thus, a host (Host1) in Vehicle1 can communicate with a server (Server1) in EN1 for a vehicular service through Vehicle1's moving network, a wireless link between IP-OBU1 and IP-RSU1, and EN1's fixed network.

For the IPv6 communication between an IP-OBU and an IP-RSU or between two neighboring IP-OBUs, they need to know the network parameters, which include MAC layer and IPv6 layer information. The MAC layer information includes wireless link layer parameters, transmission power level, and the MAC address of an external network interface for the internetworking with another IP-OBU or IP-RSU. The IPv6 layer information includes the IPv6 address and network prefix of an external network interface for the internetworking with another IP-OBU or IP-RSU.

Through the mutual knowledge of the network parameters of internal networks, packets can be transmitted between the vehicle's moving network and the EN's fixed network. Thus, V2I requires an efficient protocol for the mutual knowledge of network parameters.

As shown in Figure 3, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be either global IPv6 addresses, or IPv6 ULAs as long as IPv6 packets can be routed within vehicular networks [OMNI]. When global IPv6 addresses are used, wireless interface configuration and control overhead for Duplicate Address Detection (DAD) [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways; when ULAs and the OMNI interface are used, no DAD nor MLD messaging is needed.

4.3. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles via V2V communication.

```
                           (*)<..........>(*)
        (2001:DB8:1:1::/64) |              |
   +------------------------------+  +------------------------------+
   |                        v     |  |     v                        |
   | +-------+          +-------+ |  | +-------+          +-------+ |
   | | Host1 |          |IP-OBU1| |  | |IP-OBU2|          | Host3 | |
   | +-------+          +-------+ |  | +-------+          +-------+ |
   |     ^                  ^     |  |     ^                  ^     |
   |     |                  |     |  |     |                  |     |
   |     v                  v     |  |     v                  v     |
   | ---------------------------- |  | ---------------------------- |
   | 2001:DB8:10:1::/64 ^         |  |         ^ 2001:DB8:30:1::/64 |
   |                    |         |  |         |                    |
   |                    v         |  |         v                    |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   | | Host2 |      |Router1|     |  |     |Router2|      | Host4 | |
   | +-------+      +-------+     |  |     +-------+      +-------+ |
   |     ^              ^         |  |         ^              ^     |
   |     |              |         |  |         |              |     |
   |     v              v         |  |         v              v     |
   | ---------------------------- |  | ---------------------------- |
   |      2001:DB8:10:2::/64      |  |       2001:DB8:30:2::/64     |
   +------------------------------+  +------------------------------+
      Vehicle1 (Moving Network1)        Vehicle2 (Moving Network2)

      <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 4: Internetworking between Two Vehicles

Figure 4 shows the internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2), and two routers (IP-OBU1 and Router1). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has two hosts (Host3 and Host4), and two routers (IP-OBU2 and Router2). Vehicle1's IP-OBU1 (as a mobile router) and Vehicle2's IP-OBU2 (as a mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. Alternatively, Vehicle1 and Vehicle2 employ an OMNI interface and use IPv6 ULAs for V2V networking. Thus, a host (Host1) in Vehicle1 can communicate with another host (Host3) in Vehicle2 for a vehicular service through Vehicle1's moving network, a wireless link between IP-OBU1 and IP-OBU2, and Vehicle2's moving network.

As a V2V use case in Section 3.1, Figure 5 shows the linear network topology of platooning vehicles for V2V communications where Vehicle3 is the leading vehicle with a driver, and Vehicle2 and Vehicle1 are the following vehicles without drivers.

```
        (*)<..................>(*)<..................>(*)
         |                      |                      |
   +-----------+          +-----------+          +-----------+
   |           |          |           |          |           |
   | +-------+ |          | +-------+ |          | +-------+ |
   | |IP-OBU1| |          | |IP-OBU2| |          | |IP-OBU3| |
   | +-------+ |          | +-------+ |          | +-------+ |
   |     ^     |          |     ^     |          |     ^     |
   |     |     |=====>    |     |     |=====>    |     |     |=====>
   |     v     |          |     v     |          |     v     |
   | +-------+ |          | +-------+ |          | +-------+ |
   | | Host1 | |          | | Host2 | |          | | Host3 | |
   | +-------+ |          | +-------+ |          | +-------+ |
   |           |          |           |          |           |
   +-----------+          +-----------+          +-----------+
      Vehicle1               Vehicle2               Vehicle3

    <----> Wired Link   <....> Wireless Link   ===> Moving Direction
    (*) Antenna
```

Figure 5: Multihop Internetworking between Two Vehicle Networks

As shown in Figure 5, multihop internetworking is feasible among the moving networks of three vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-OBU2 in Vehicle2, and IP-OBU3 in Vehicle3 in the linear network, as shown in the figure.

5. Problem Statement

In order to specify protocols using the architecture mentioned in Section 4.1, IPv6 core protocols have to be adapted to overcome certain challenging aspects of vehicular networking. Since the vehicles are likely to be moving at great speed, protocol exchanges need to be completed in a time relatively short compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles.

Note that if two vehicles are moving in the opposite directions in a roadway, the relative speed of this case is two times the relative speed of a vehicle passing through an RSU. The time constraint of a wireless link between two nodes needs to be considered because it may affect the lifetime of a session involving the link.

The lifetime of a session varies depending on the session’s type such as a web surfing, voice call over IP, and DNS query. Regardless of a session’s type, to guide all the IPv6 packets to their destination host, IP mobility should be supported for the session.

Thus, the time constraint of a wireless link has a major impact on IPv6 Neighbor Discovery (ND). Mobility Management (MM) is also vulnerable to disconnections that occur before the completion of identity verification and tunnel management. This is especially true given the unreliable nature of wireless communication. This section presents key topics such as neighbor discovery and mobility management.

5.1. Neighbor Discovery

IPv6 ND [RFC4861][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for link types including point-to-point, multicast-capable (e.g., Ethernet) and Non-Broadcast Multiple Access (NBMA). It assumes the efficient and reliable support of multicast and unicast from the link layer for various network operations such as MAC Address Resolution (AR), DAD, MLD and Neighbor Unreachability Detection (NUD).

Vehicles move quickly within the communication coverage of any particular vehicle or IP-RSU. Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and run IPv6 ND.

The requirements for IPv6 ND for vehicular networks are efficient DAD and NUD operations. An efficient DAD is required to reduce the overhead of the DAD packets during a vehicle's travel in a road network, which guaranteeing the uniqueness of a vehicle's global IPv6 address. An efficient NUD is required to reduce the overhead of the NUD packets during a vehicle's travel in a road network, which guaranteeing the accurate neighborhood information of a vehicle in terms of adjacent vehicles and RSUs.

The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks. The merging and partitioning of VANETs frequently occurs in vehicular networks. This merging and partitioning should be considered for the IPv6 ND such as IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. Due to the merging of VANETs, two IPv6 addresses may conflict with each other though they were unique before the merging. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. Also, SLAAC needs to prevent IPv6 address duplication due to the merging of VANETs. According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or an off-link host even though the source vehicle uses the same prefix as the destination vehicle.

To efficiently prevent IPv6 address duplication due to the VANET partitioning and merging from happening in vehicular networks, the vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD. In this case, two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and IP-RSUs, as shown in Figure 1. By using the vehicular-network-wide DAD, vehicles can assure that their IPv6 addresses are unique in the vehicular network whenever they are connected to the vehicular infrastructure or become disconnected from it in the form of VANET.

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval need to be adjusted for vehicle speed and vehicle density. For example, the NA interval needs to be dynamically adjusted according to a vehicle's speed so that the vehicle can maintain its neighboring vehicles in a stable way, considering the collision probability with the NA messages sent by other vehicles.

For IPv6-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular networks, the delay-bounded data delivery is critical. IPv6 ND needs to work to support those IPv6-based safety applications efficiently.

Thus, in IPv6-based vehicular networking, IPv6 ND should have minimum changes for the interoperability with the legacy IPv6 ND used in the Internet, including the DAD and NUD operations.

5.1.1. Link Model

A prefix model for a vehicular network needs to facilitate the communication between two vehicles with the same prefix regardless of the vehicular network topology as long as there exist bidirectional E2E paths between them in the vehicular network including VANETs and IP-RSUs. This prefix model allows vehicles with the same prefix to communicate with each other via a combination of multihop V2V and multihop V2I with VANETs and IP-RSUs. Note that the OMNI interface supports an NBMA link model where multihop V2V and V2I communications use each mobile node's ULAs without need for any DAD or MLD messaging.

IPv6 protocols work under certain assumptions that do not necessarily hold for vehicular wireless access link types other than OMNI/NBMA [VIP-WAVE][RFC5889]; the rest of this section discusses implications for those link types that do not apply when the OMNI/NBMA link model is used. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces [RFC6250]. However, radio interference and different levels of transmission power may cause asymmetric links to appear in vehicular wireless links. As a result, a new vehicular link model needs to consider the asymmetry of dynamically changing vehicular wireless links.

There is a relationship between a link and a prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IPv6 link. However, the vehicular link model needs to define the relationship between a link and a prefix, considering the dynamics of wireless links and the characteristics of VANET.

A VANET can have a single link between each vehicle pair within wireless communication range, as shown in Figure 5. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Suppose that a global-scope IPv6 prefix (or an IPv6 ULA prefix) is assigned to VANETs in vehicular networks. Even though two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, they may not communicate with each other not in one hop in the same VANET because of the multihop network connectivity between them. Thus, in this case, the concept of an on-link IPv6 prefix does not hold because two vehicles with the same on-link IPv6 prefix cannot communicate directly with each other. Also, when two vehicles are located in two different VANETs with the same IPv6 prefix, they cannot communicate with each other. When these two VANETs converge to one VANET, the two vehicles can communicate with each other in a multihop fashion, for example, when they are Vehicle1 and Vehicle3, as shown in Figure 5.

From the previous observation, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility. Therefore, the vehicular link model needs to use an on-link prefix and off-link prefix according to the network topology of vehicles such as a one-hop reachable network and a multihop reachable network (or partitioned networks). If the vehicles with the same prefix are reachable from each other in one hop, the prefix should be on-link. On the other hand, if some of the vehicles with the same prefix are not reachable from each other in one hop due to either the multihop topology in the VANET or multiple partitions, the prefix should be off-link.

The vehicular link model needs to support multihop routing in a connected VANET where the vehicles with the same global-scope IPv6 prefix (or the same IPv6 ULA prefix) are connected in one hop or multiple hops. It also needs to support the multihop routing in multiple connected VANETs through infrastructure nodes (e.g., IP-RSU) where they are connected to the infrastructure. For example, in Figure 1, suppose that Vehicle1, Vehicle2, and Vehicle3 are configured with their IPv6 addresses based on the same global-scope IPv6 prefix. Vehicle1 and Vehicle3 can also communicate with each other via either multihop V2V or multihop V2I2V. When Vehicle1 and Vehicle3 are connected in a VANET, it will be more efficient for them to communicate with each other directly via VANET rather than indirectly via IP-RSUs. On the other hand, when Vehicle1 and Vehicle3 are far away from direct communication range in separate VANETs and under two different IP-RSUs, they can communicate with each other through the relay of IP-RSUs via V2I2V. Thus, two separate VANETs can merge into one network via IP-RSU(s). Also, newly arriving vehicles can merge two separate VANETs into one VANET if they can play the role of a relay node for those VANETs.

Thus, in IPv6-based vehicular networking, the vehicular link model should have minimum changes for interoperability with standard IPv6 links in an efficient fashion to support IPv6 DAD, MLD and NUD operations. When the OMNI NBMA link model is used, there are no link model changes nor DAD/MLD messaging required.

5.1.2. MAC Address Pseudonym

For the protection of drivers' privacy, a pseudonym of a MAC address of a vehicle's network interface should be used, so that the MAC address can be changed periodically. However, although such a pseudonym of a MAC address can protect to some extent the privacy of a vehicle, it may not be able to resist attacks on vehicle identification by other fingerprint information, for example, the scrambler seed embedded in IEEE 802.11-OCB frames [Scrambler-Attack]. The pseudonym of a MAC address affects an IPv6 address based on the MAC address, and a transport-layer (e.g., TCP and SCTP) session with an IPv6 address pair. However, the pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

In the ETSI standards, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities (e.g., MAC address) and the corresponding IPv6 addresses [Identity-Management]. Whenever the network interface identifier changes, the IPv6 address based on the network interface identifier needs to be updated, and the uniqueness of the address needs to be checked through the DAD procedure. For vehicular networks with high mobility and density, this DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange application messages (e.g., collision avoidance and accident notification) with each other with a short interval (e.g., 0.5 second) [NHTSA-ACAS-Report].

5.1.3. Routing

For multihop V2V communications in either a VANET or VANETs via IP-RSUs, a vehicular Mobile Ad Hoc Networks (MANET) routing protocol may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead [ID-Multicast-Problems].

A routing protocol for a VANET may cause redundant wireless frames in the air to check the neighborhood of each vehicle and compute the routing information in a VANET with a dynamic network topology because the IPv6 ND is used to check the neighborhood of each vehicle. Thus, the vehicular routing needs to take advantage of the IPv6 ND to minimize its control overhead.

5.2. Mobility Management

The seamless connectivity and timely data exchange between two end points requires efficient mobility management including location management and handover. Most vehicles are equipped with a GPS receiver as part of a dedicated navigation system or a corresponding smartphone App. Note that the GPS receiver may not provide vehicles with accurate location information in adverse environments such as a building area or a tunnel. The location precision can be improved with assistance of the IP-RSUs or a cellular system with a GPS receiver for location information.

With a GPS navigator, efficient mobility management can be performed with the help of vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having IP-RSUs and an MA in TCC). This vehicular infrastructure can predict the future positions of the vehicles from their mobility information (i.e., the current position, speed, direction, and trajectory) for efficient mobility management (e.g., proactive handover). For a better proactive handover, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]), can be used to determine the moment of a handover between IP-RSUs along with mobility information.

By predicting a vehicle's mobility, the vehicular infrastructure needs to better support IP-RSUs to perform efficient SLAAC, data forwarding, horizontal handover (i.e., handover in wireless links using a homogeneous radio technology), and vertical handover (i.e., handover in wireless links using heterogeneous radio technologies) in advance along with the movement of the vehicle.

For example, as shown in Figure 1, when a vehicle (e.g., Vehicle2) is moving from the coverage of an IP-RSU (e.g., IP-RSU1) into the coverage of another IP-RSU (e.g., IP-RSU2) belonging to a different subnet, the IP-RSUs can proactively support the IPv6 mobility of the vehicle, while performing the SLAAC, data forwarding, and handover for the sake of the vehicle.

For a mobility management scheme in a shared link, where the wireless subnets of multiple IP-RSUs share the same prefix, an efficient vehicular-network-wide DAD is required. If DHCPv6 is used to assign a unique IPv6 address to each vehicle in this shared link, the DAD is not required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213] and OMNI [OMNI]), DAD is not required because the IPv6 address of a vehicle's external wireless interface is guaranteed to be unique. There is a tradeoff between the prefix usage efficiency and DAD overhead. Thus, the IPv6 address autoconfiguration for vehicular networks needs to consider this tradeoff to support efficient mobility management.

Therefore, for the proactive and seamless IPv6 mobility of vehicles, the vehicular infrastructure (including IP-RSUs and MA) needs to efficiently perform the mobility management of the vehicles with their mobility information and link-layer information. Also, in IPv6-based vehicular networking, IPv6 mobility management should have minimum changes for the interoperability with the legacy IPv6 mobility management schemes such as PMIPv6, DMM, LISP, and AERO.

6. Security Considerations

This section discusses security and privacy for IPv6-based vehicular networking. Security and privacy are key components of IPv6-based vehicular networking along with neighbor discovery and mobility management.

Security and privacy are paramount in V2I, V2V, and V2X networking. Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. Also, in-vehicle devices (e.g., ECU) and a driver/passenger's mobile devices (e.g., smartphone and tablet PC) in a vehicle need to communicate with other in-vehicle devices and another driver/passenger's mobile devices in another vehicle, or other servers behind an IP-RSU in a secure way. Even though a vehicle is perfectly authenticated and legitimate, it may be hacked for running malicious applications to track and collect its and other vehicles' information. In this case, an attack mitigation process may be required to reduce the aftermath of malicious behaviors.

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safe driving applications (e.g., context-aware navigation, cooperative adaptive cruise control, and platooning), as explained in Section 3.1, the cooperative action among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) for disturbing safe driving. For example, a Sybil attack, which tries to confuse a vehicle with multiple false identities, may disturb a vehicle from taking a safe maneuver.

Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles, so their communication activities need to be logged in either a central way through a logging server (e.g., TCC) in the vehicular cloud or a distributed way (e.g., blockchain [Bitcoin]) along with other vehicles or infrastructure. For the non-repudiation of the harmful activities of malicious nodes, a blockchain technology can be used [Bitcoin]. Each message from a vehicle can be treated as a transaction and the neighboring vehicles can play the role of peers in a consensus method of a blockchain [Bitcoin][Vehicular-BlockChain]. For a blockchain's efficient consensus in vehicular networks having fast moving vehicles, a new consensus algorithm needs to be developed or an existing consensus algorithm needs to be enhanced.

To identify malicious vehicles among vehicles, an authentication method is required. A Vehicle Identification Number (VIN) and a user certificate (e.g., X.509 certificate [RFC5280]) along with an in-vehicle device's identifier generation can be used to efficiently authenticate a vehicle or its driver (having a user certificate) through a road infrastructure node (e.g., IP-RSU) connected to an authentication server in the vehicular cloud. This authentication can be used to identify the vehicle that will communicate with an infrastructure node or another vehicle. In the case where a vehicle has an internal network (called Moving Network) and elements in the network (e.g., in-vehicle devices and a user's mobile devices), as shown in Figure 3, the elements in the network need to be authenticated individually for safe authentication. Also, Transport Layer Security (TLS) certificates [RFC8446][RFC5280] can be used for an element's authentication to allow secure E2E vehicular communications between an element in a vehicle and another element in a server in a vehicular cloud, or between an element in a vehicle and another element in another vehicle.

For secure V2I communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 3 [RFC4301][RFC4302][RFC4303][RFC4308][RFC7296]. Also, for secure V2V communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBU) in a vehicle and a mobile router (i.e., IP-OBU) in another vehicle needs to be established, as shown in Figure 4. For secure communication, an element in a vehicle (e.g., an in-vehicle device and a driver/passenger's mobile device) needs to establish a secure connection (e.g., TLS) with another element in another vehicle or another element in a vehicular cloud (e.g., a server). Even though IEEE 1609.2 [WAVE-1609.2] specifies security services for applications and management messages. This WAVE specification is optional, so if WAVE does not support the security of a WAVE frame, either the network layer or the transport layer needs to support security services for the WAVE frames.

For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC is required in a highway for the authentication by involving multiple intermediate vehicles as relay nodes toward an IP-RSU connected to an authentication server in the vehicular cloud. The V2I communications over 5G V2X (or LTE V2X) is required to allow a vehicle to communicate directly with a gNodeB (or eNodeB) connected to an authentication server in the vehicular cloud.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, especially for a long-living transport-layer session (e.g., voice call over IP and video streaming service), a MAC address pseudonym needs to be provided to each vehicle; that is, each vehicle periodically updates its MAC address and its IPv6 address needs to be updated accordingly by the MAC address change [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicles (or between a vehicle and an IP-RSU) for a long-living transport-layer session. However, if this pseudonym is performed without strong E2E confidentiality (using either IPsec or TLS), there will be no privacy benefit from changing MAC and IPv6 addresses, because an adversary can observe the change of the MAC and IPv6 addresses and track the vehicle with those addresses. Thus, the MAC address pseudonym and the IPv6 address update should be performed with strong E2E confidentiality.

For the IPv6 ND, the DAD is required to ensure the uniqueness of the IPv6 address of a vehicle's wireless interface. This DAD can be used as a flooding attack that uses the DAD-related ND packets disseminated over the VANET or vehicular networks. Thus, the vehicles and IP-RSUs need to filter out suspicious ND traffic in advance.

For mobility management, a malicious vehicle can construct multiple virtual bogus vehicles, and register them with IP-RSUs and MA. This registration makes the IP-RSUs and MA waste their resources. The IP-RSUs and MA need to determine whether a vehicle is genuine or bogus in mobility management. Also, the confidentiality of control packets and data packets among IP-RSUs and MA, the E2E paths (e.g., tunnels) need to be protected by secure communication channels. In addition, to prevent bogus IP-RSUs and MA from interfering with the IPv6 mobility of vehicles, mutual authentication among them needs to be performed by certificates (e.g., TLS certificate).

7. IANA Considerations

This document does not require any IANA actions.

8. Informative References

[Automotive-Sensing]
Choi, J., Va, V., Gonzalez-Prelcic, N., Daniels, R., R. Bhat, C., and R. W. Heath, "Millimeter-Wave Vehicular Communication to Support Massive Automotive Sensing", IEEE Communications Magazine, December 2016.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System", URL: https://bitcoin.org/bitcoin.pdf, May 2009.

[CA-Cruise-Control]
California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", Available: http://www.path.berkeley.edu/research/automated-and-connected-vehicles/cooperative-adaptive-cruise-control, 2017.

[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.

[CBDN] Kim, J., Kim, S., Jeong, J., Kim, H., Park, J., and T. Kim, "CBDN: Cloud-Based Drone Navigation for Efficient Battery Charging in Drone Networks", IEEE Transactions on Intelligent Transportation Systems, November 2019.

[DMM-FPC] Matsushima, S., Bertz, L., Liebsch, M., Gundavelli, S., Moses, D., and C. Perkins, "Protocol for Forwarding Policy Configuration (FPC) in DMM", draft-ietf-dmm-fpc-cpdp-13 (work in progress), March 2020.

[DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), October 2010.

[EU-2008-671-EC]
European Union, "Commission Decision of 5 August 2008 on the Harmonised Use of Radio Spectrum in the 5875 - 5905 MHz Frequency Band for Safety-related Applications of Intelligent Transport Systems (ITS)", EU 2008/671/EC, August 2008.

[FirstNet]
U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", Available: https://www.firstnet.gov/, 2012.

[FirstNet-Report]
First Responder Network Authority, "FY 2017: ANNUAL REPORT TO CONGRESS, Advancing Public Safety Broadband Communications", FirstNet FY 2017, December 2017.

[Fuel-Efficient]
van de Hoef, S., H. Johansson, K., and D. V. Dimarogonas, "Fuel-Efficient En Route Formation of Truck Platoons", IEEE Transactions on Intelligent Transportation Systems, January 2018.

[ID-Multicast-Problems]
Perkins, C., McBride, M., Stanley, D., Kumari, W., and JC. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", draft-ietf-mboned-ieee802-mcast-problems-11 (work in progress), December 2019.

[Identity-Management]
Wetterwald, M., Hrizi, F., and P. Cataldi, "Cross-layer Identities Management in ITS Stations", The 10th International Conference on ITS Telecommunications, November 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.

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

[In-Car-Network]
Lim, H., Volker, L., and D. Herrscher, "Challenges in a Future IP/Ethernet-based In-Car Network for Real-Time Applications", ACM/EDAC/IEEE Design Automation Conference (DAC), June 2011.

[ISO-ITS-IPv6]
ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012.

[ISO-ITS-IPv6-AMD1]
ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking - Amendment 1", ISO 21210:2012/AMD 1:2017, September 2017.

[NHTSA-ACAS-Report]
National Highway Traffic Safety Administration (NHTSA), "Final Report of Automotive Collision Avoidance Systems (ACAS) Program", DOT HS 809 080, August 2000.

[OMNI] Templin, F. and A. Whyman, "Transmission of IPv6 Packets over Overlay Multilink Network (OMNI) Interfaces", draft-templin-6man-omni-interface-27 (work in progress), July 2020.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, July 2004.

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

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

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, December 2005.

[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.

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

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

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

[RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250, May 2011.

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

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[RFC6706BIS]
Templin, F., "Asymmetric Extended Route Optimization (AERO)", draft-templin-intarea-6706bis-58 (work in progress), June 2020.

[RFC6830BIS]
Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, "The Locator/ID Separation Protocol (LISP)", draft-ietf-lisp-rfc6830bis-32 (work in progress), March 2020.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, March 2014.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 7296, October 2014.

[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.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 8200, July 2017.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018.

[RFC8691] Benamar, N., Haerri, 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, December 2019.

[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.

[SAINTplus]
Shen, Y., Lee, J., Jeong, H., Jeong, J., Lee, E., and D. Du, "SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization", IEEE Transactions on Intelligent Transportation Systems, June 2017.

[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.

[Scrambler-Attack]
Bloessl, B., Sommer, C., Dressier, F., and D. Eckhoff, "The Scrambler Attack: A Robust Physical Layer Attack on Location Privacy in Vehicular Networks", IEEE 2015 International Conference on Computing, Networking and Communications (ICNC), February 2015.

[SignalGuru]
Koukoumidis, E., Peh, L., and M. Martonosi, "SignalGuru: Leveraging Mobile Phones for Collaborative Traffic Signal Schedule Advisory", ACM MobiSys, June 2011.

[TR-22.886-3GPP]
3GPP, "Study on Enhancement of 3GPP Support for 5G V2X Services", 3GPP TR 22.886/Version 16.2.0, December 2018.

[Truck-Platooning]
California Partners for Advanced Transportation Technology (PATH), "Automated Truck Platooning", Available: http://www.path.berkeley.edu/research/automated-and-connected-vehicles/truck-platooning, 2017.

[TS-23.285-3GPP]
3GPP, "Architecture Enhancements for V2X Services", 3GPP TS 23.285/Version 16.2.0, December 2019.

[TS-23.287-3GPP]
3GPP, "Architecture Enhancements for 5G System (5GS) to Support Vehicle-to-Everything (V2X) Services", 3GPP TS 23.287/Version 16.2.0, March 2020.

[UAM-ITS] Templin, F., "Urban Air Mobility Implications for Intelligent Transportation Systems", draft-templin-ipwave-uam-its-03 (work in progress), July 2020.

[Vehicular-BlockChain]
Dorri, A., Steger, M., Kanhere, S., and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy", IEEE Communications Magazine, Vol. 55, No. 12, December 2017.

[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.

[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.

Appendix A. Acknowledgments

This work was supported 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 (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2017-0-01633) supervised by the IITP (Institute for Information & communications Technology Promotion).

This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

Appendix B. Contributors

This document is a group work of IPWAVE working group, greatly benefiting from inputs and texts by Rex Buddenberg (Naval Postgraduate School), Thierry Ernst (YoGoKo), Bokor Laszlo (Budapest University of Technology and Economics), Jose Santa Lozanoi (Universidad of Murcia), Richard Roy (MIT), Francois Simon (Pilot), Sri Gundavelli (Cisco), Erik Nordmark, Dirk von Hugo (Deutsche Telekom), Pascal Thubert (Cisco), Carlos Bernardos (UC3M), Russ Housley (Vigil Security), Suresh Krishnan (Kaloom), Nancy Cam-Winget (Cisco), Fred L. Templin (The Boeing Company), Jung-Soo Park (ETRI), Zeungil (Ben) Kim (Hyundai Motors), Kyoungjae Sun (Soongsil University), Zhiwei Yan (CNNIC), YongJoon Joe (LSware), and Peter E. Yee (Akayla). The authors sincerely appreciate their contributions.

The following are co-authors of this document:

Nabil Benamar
Department of Computer Sciences
High School of Technology of Meknes
Moulay Ismail University
Morocco

Phone: +212 6 70 83 22 36
EMail: benamar73@gmail.com

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

Santiago
Chile

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

Jerome Haerri
Communication Systems Department
EURECOM
Sophia-Antipolis
France

Phone: +33 4 93 00 81 34
EMail: jerome.haerri@eurecom.fr

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

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

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

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

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

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

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

Yiwen Chris Shen
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu
URI: http://iotlab.skku.edu/people-chris-shen.php

Michelle Wetterwald
FBConsulting
21, Route de Luxembourg
Wasserbillig, Luxembourg L-6633
Luxembourg

EMail: Michelle.Wetterwald@gmail.com

Author's Address

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
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Network Working Group J. Jeong
Internet-Draft Sungkyunkwan University
Intended status: Standards Track S. Lee
Expires: September 6, 2018 Ericsson-LG
J. Park
ETRI
March 5, 2018

DNS Name Autoconfiguration for Internet of Things Devices
draft-jeong-ipwave-iot-dns-autoconf-02

Abstract

This document specifies an autoconfiguration scheme for device discovery and service discovery. Through the device discovery, this document supports the global (or local) DNS naming of Internet of Things (IoT) devices, such as sensors, actuators, and in-vehicle units. By this scheme, the DNS name of an IoT device can be autoconfigured with the device's model information in wired and wireless target networks (e.g., vehicle, road network, home, office, shopping mall, and smart grid). Through the service discovery, IoT users (e.g., drivers, passengers, home residents, and customers) in the Internet (or local network) can easily identify each device for monitoring and remote-controlling it in a target network.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Many Internet of Things (IoT) devices (e.g., sensors, actuators, and in-vehicle units) have begun to have wireless communication capability (e.g., WiFi, Bluetooth, and ZigBee) for monitoring and remote-controlling in a local network or the Internet. According to the capacity, such IoT devices can be categorized into high-capacity devices and low-capacity devices. High-capacity devices have a high-power processor and a large storage, such as vehicles, road infrastructure devices (e.g., road-side unit, traffic light, and loop-detector), appliances (e.g., television, refrigerator, air conditioner, and washing machine), and smart devices (smartphone and tablet). They are placed in environments (e.g., vehicle, road network, home, office, shopping mall, and smart grid) for the direct use for human users, and they require the interaction with human users. Low-capacity devices have a low-power processor and a small storage, such as sensors (e.g., in-vehicle units, light sensor, meter, and fire detector) and actuators (e.g., vehicle engine, signal light, street light, and room temperature controller). They are installed for the easy management of environments (e.g., vehicle, road network, home, office, store, and factory), and they do not require the interaction with human users.

For the Internet connectivity of IoT devices, a variety of parameters (e.g., address prefixes, default routers, and DNS servers) can be automatically configured by Neighbor Discovery (ND) for IP Version 6, IPv6 Stateless Address Autoconfiguration, and IPv6 Router Advertisement (RA) Options for DNS Configuration [RFC4861][RFC4862] [RFC8106].

For these IoT devices, the manual configuration of DNS names will be cumbersome and time-consuming as the number of them increases rapidly in a network. It will be good for such DNS names to be automatically configured such that they are readable to human users.

Multicast DNS (mDNS) in [RFC6762] can provide DNS service for networked devices on a local link (e.g., home network and office network) without any conventional recursive DNS server. mDNS also supports the autoconfiguration of a device’s DNS name without the intervention of the user. mDNS aims at the DNS naming service for the local DNS names of the networked devices on the local link rather than the DNS naming service for the global DNS names of such devices in the Internet. However, for IoT devices accessible from the Internet, mDNS cannot be used. Thus, a new autoconfiguration scheme becomes required for the global DNS names of IoT devices.

This document proposes an autoconfiguration scheme for the global (or local) DNS names of IoT devices. Since an autoconfigured DNS name contains the model identifier (ID) of a device, IoT users in the Internet (or local network) can easily identify such a device. The autoconfigured DNS names and corresponding IP addresses of the IoT devices are registered into local or remote authoritative DNS servers that manage the DNS suffixes of the DNS domain names. With these DNS names, they will be able to monitor and remote-control their IoT devices with their smart devices (e.g., smartphone and tablet PC) by resolving their DNS names into the corresponding IP addresses.

For cloud-based DNS naming services of IoT devices, a cloud server can collect DNS zone files having the global DNS names and IP addresses of the IoT devices from multiple DNS servers and provide IoT users with such global DNS names of IoT devices relevant to the IoT users. These IoT users can monitor and remote-control their IoT devices in the Internet with the global DNS names and IP addresses, using their smart devices.

1.1. Applicability Statements

It is assumed that IoT devices have networking capability through wired or wireless communication media, such as Ethernet [IEEE-802.3], WiFi [IEEE-802.11][IEEE-802.11a][IEEE-802.11b][IEEE-802.11g] [IEEE-802.11n], Dedicated Short-Range Communications (DSRC) [DSRC-WAVE][IEEE-802.11p], Bluetooth [IEEE-802.15.1], and ZigBee [IEEE-802.15.4] in a local area network (LAN) or personal area network (PAN). Note that IEEE 802.11p was renamed IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012.

Also, it is assumed that each IoT device has a factory configuration (called device configuration) having device model information by manufacturer ID and model ID (e.g., vehicle, road-side unit, smart TV, smartphone, tablet, and refrigerator). This device configuration can be read by the device for DNS name autoconfiguration.

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:

- Device Configuration: A factory configuration that has device model information by manufacturer ID and model ID (e.g., vehicle, road-side unit, smart TV, smartphone, tablet, and refrigerator).

- DNS Search List (DNSSL): The list of DNS suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names [RFC8106].

- DNSSL Option: IPv6 RA option to deliver the DNSSL information to IPv6 hosts [RFC8106].

4. Overview

This document specifies an autoconfiguration scheme for an IoT device using device configuration and DNS search list. Device configuration has device model information (e.g., device's manufacturer and model). DNS search list has DNS suffix domain names that represent the DNS domains of a network having the IoT device [RFC8106].

As an IPv6 host, the IoT device can obtain DNS search list through IPv6 Router Advertisement (RA) with DNS Search List (DNSSL) Option [RFC4861][RFC8106] or DHCPv6 with Domain Search List Option [RFC3315][RFC3736][RFC3646].

The IoT device can construct its DNS name with the concatenation of manufacturer ID, model ID, and domain name. Since there exist more than one device with the same model, the DNS name should have a unique identification (e.g., unique ID or serial ID) to differentiate multiple devices with the same model.

Since both RA and DHCPv6 can be simultaneously used for the parameter configuration for IPv6 hosts, this document considers the DNS name autoconfiguration in the coexistence of RA and DHCP.

5. DNS Name Autoconfiguration

The DNS name autoconfiguration for an IoT device needs the acquisition of DNS search list through either RA [RFC8106] or DHCPv6 [RFC3646]. Once the DNS search list is obtained, the IoT device autonomously constructs its DNS name(s) with the DNS search list and its device information.

5.1. DNS Name Format with Object Identifier

A DNS name for an IoT device can have the following format with object identifier (OID), which is defined in [oneM2M-OID], as in Figure 1:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   unique_id.object_identifier.OID.domain_name   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: IoT Device DNS Name Format with OID

Fields:

unique_id unique identifier to guarantee the uniqueness of the DNS name in ASCII characters. The identifier MAY be alphanumeric with readability, e.g., product name plus a sequence number.

object_identifier device's object identifier that consists of a higher arc, that is, M2M node indication ID (i.e., the concatenation of the managing organization, administration, data country code, and M2M node) and a sequence of four arcs (i.e., manufacturer ID, model ID, serial ID, and expanded ID) as defined in [oneM2M-OID]. The fields are seperated by an underscore '_'.

OID subdomain for the keyword of OID to indicate that object_identifier is used.

domain_name domain name that represents a DNS domain for the network having the IoT devices.

Note each subdomain (i.e., unique_id, object_identifier, OID, and domain_name) in the domain name format in Figure 1 is expressed using the name syntax described in [RFC1035].

5.2. Procedure of DNS Name Autoconfiguration

The procedure of DNS name autoconfiguration is performed through a DNSSL option delivered by either RA [RFC8106] or DHCPv6 [RFC3646].

5.2.1. DNS Name Generation

When as an IPv6 host a device receives a DNSSL option through either RA or DHCPv6, it checks the validity of the DNSSL option. If the option is valid, the IPv6 host performs the DNS name autoconfiguration with each DNS suffix domain name in the DNSSL option as follows:

1. The host constructs its DNS name with the DNS suffix domain name along with device configuration (i.e., manufacturer ID, model ID, and serial ID) and a selected identifier (as unique_id) that is considered unique, which is human-friendly, as shown in Figure 1.

2. The host constructs an IPv6 unicast address as a tentative address with a 64-bit network prefix and the last 64 bits of the MD5 hashed value of the above DNS name.

3. The host constructs the solicited-node multicast address in [RFC4861] corresponding to the tentative IPv6 address.

4. The host performs Duplicate Address Detection (DAD) for the IPv6 address with the solicited-node multicast address [RFC4861] [RFC4862].

5. If there is no response from the DAD, the host sets the IPv6 tentative address as its IPv6 unicast address and regards the constructed DNS name as unique on the local link. Otherwise, since the DAD fails because of DNS name conflict, go to Step 1 for a new DNS name generation with another identifier for unique_id.

6. Since the DNS name is proven to be unique, it is used as the device's DNS name and the DNS autoconfiguration is done for the given DNS suffix domain name. Also, the host joins the solicited-node multicast address for the verified DNS name in order to prevent other hosts from using this DNS name.

When the DNS search list has more than one DNS suffix domain name, the IPv6 host repeats the above procedure until all of the DNS suffixes are used for the DNS name autoconfiguration along with the IPv6 unicast autoconfiguration corresponding to the DNS name.

5.2.2. DNS Name Collection

Once as IPv6 hosts the devices have autoconfigured their DNS names, as a collector, any IPv6 node (i.e., router or host) in the same subnet can collect the device DNS names using IPv6 Node Information (NI) protocol [RFC4620].

For a collector to collect the device DNS names without any prior node information, a new NI query needs to be defined. That is, a new ICMPv6 Code (e.g., 3) SHOULD be defined for the collection of the IPv6 host DNS names. The Data field is not included in the ICMPv6 header since the NI query is for all the IPv6 hosts in the same subnet. The Qtype field for NI type is set to 2 for Node Name.

The query SHOULD be transmitted by the collector to a link-local multicast address for this NI query. Assume that a link-local scope multicast address (e.g., all-nodes multicast address, FF02::1) SHOULD be defined for device DNS name collection such that all the IPv6 hosts join this link-local multicast address for the device DNS name collection service.

When an IPv6 host receives this query sent by the collector in multicast, it transmits its Reply with its DNS name with a random interval between zero and Query Response Interval, as defined by Multicast Listener Discovery Version 2 [RFC3810]. This randomly delayed Reply allows the collector to collect the device DNS names with less frame collision probability by spreading out the Reply time instants.

After the collector collects the device DNS names, it resolves the DNS names into the corresponding IPv6 addresses by NI protocol [RFC4620] with the ICMPv6 Code 1 of NI Query. This code indicates that the Data field of the NI Query has the DNS name of an IoT device. The IoT device that receives this NI query sends the collector an NI Reply with its IPv6 address in the Data field.

For DNS name resolution service, the collector can register the pair(s) of DNS name and IPv6 address for each IPv6 host into an appropriate designated DNS server for the DNS domain suffix of the DNS name. It is assumed that the collector is configured to register DNS names into the designated DNS server in a secure way based on DNSSEC [RFC4033][RFC6840]. This registration of the DNS name and IPv6 address can be performed by DNS dynamic update [RFC2136]. Before registering the DNS name into the designated DNS server, the collector SHOULD verify the uniqueness of the DNS name in the intended DNS domain by sending a DNS query for the resolution of the DNS name. If there is no corresponding IPv6 address for the queried DNS name, the collector registers the DNS name and the corresponding IPv6 address for each IPv6 host into the designated DNS server. On the other hand, if there is such a corresponding IPv6 address, the DNS name is regarded as duplicate (i.e., not unique), and so the corresponder notifies the corresponding IoT device with the duplicate DNS name of an error message of DNS name duplication using NI protocol. When an IoT device receives such a DNS name duplication error, it needs to construct a new DNS name and repeats the procedure of device DNS name generation along with the uniqueness test of the device DNS name in its subnet.

The two separate procedures of the DNS name collection and IPv6 address resolution in the above NI protocol can be consolidated into a single collection for the pairs of DNS names and the corresponding IPv6 addresses. For such an optimization, a new ICMPv6 Code (e.g., 4) is defined for the NI Query to query the pair of a DNS name and the corresponding IPv6 address. With this code, the collector can collect the pairs of each IoT device’s DNS name and IPv6 address in one NI query message rather than two NI query messages.

For DNS name collection for IoT devices as IPv6 hosts, DHCPv6 [RFC3315] can be used instead of the NI protocol. For this purpose, a new DHCP option (called DNSNA option) needs to be defined to collect the pair of a DNS name and the corresponding IPv6 address of an IoT device. As a DNS information collector, a DHCPv6 server (or a router running a DHCPv6 server) sends a request message for the DHCP DNSNA option to IoT devices as its DHCPv6 clients under its address pool. The clients respond to this request message by sending the DHCPv6 server a reply message with their DNS information. Thus, the DHCPv6 server can collect the pairs of DNS names and the corresponding IPv6 addresses of the IoT devices. Then, as a collector, the DHCPv6 server can register the DNS names and the corresponding IPv6 addresses of IoT devices into the designated DNS server.

5.2.3. DNS Name Retrieval

A smart device like smartphone can retrieve the DNS names of IoT devices by contacting a global (or local) DNS server having the IoT device DNS names. If the smart device can retrieve the zone file with the DNS names, it can display the information of IoT devices in a target network, such as home network and office network. With this information, the user can monitor and control the IoT devices in the Internet (or local network). To monitor or remote-control IoT devices, Constrained Application Protocol (CoAP) can be used [RFC7252].

6. Location-Aware DNS Name Configuration

If the DNS name of an IoT device includes location information, it allows users to easily identify the physical location of each device. This document proposes the representation of a location in a DNS name. In this document, the location in a DNS name consists of two levels for a detailed location specification, such as macro-location for a large area and micro-location for a small area.

To denote both macro-location (i.e., mac_loc) and micro-location (i.e., mic_loc) into a DNS name, the following format is described as in Figure 2:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| unique_id.object_identifier.OID.mic_loc.mac_loc.LOC.domain_name |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Location-Aware Device DNS Name Format

Fields:

unique_id unique identifier to guarantee the uniqueness of the DNS name in ASCII characters. The identifier MAY be alphanumeric with readability, such as product name plus a sequence number.

object_identifier device's object identifier that consists of a higher arc, that is, M2M node indication ID (i.e., the concatenation of the managing organization, administration, data country code, and M2M node) and a sequence of four arcs (i.e., manufacturer ID, model ID, serial ID, and expanded ID) as defined in [oneM2M-OID]. The fields are seperated by an underscore '_'.

OID subdomain for the keyword of OID to indicate that object_identifier is used.

mic_loc device's micro-location, such as center, edge, and corner.

mac_loc device's macro-location, such as road segment.

LOC subdomain for the keyword of LOC to indicate that mac_loc and mic_loc are used.

domain_name domain name that represents a DNS domain for the network having the IoT devices.

Note each subdomain (e.g., mic_loc and mac_loc) in the domain name format in Figure 2 is expressed using the name syntax described in [RFC1035].

7. Macro-Location-Aware DNS Name

If location information (such as cross area, intersection, and road segment in a road network) is available to an IoT device, a keyword, coordinate, or location ID for the location information can be used to construct a DNS name as subdomain name. This location information lets users track the position of mobile devices (such as vehicle, smartphone, and tablet). The physical location of the device is defined as macro-location for DNS naming.

A subdomain name for macro-location (denoted as mac_loc) MAY be placed between micro-location (denoted as mic_loc) and the keyword LOC of the DNS name format in Figure 2. For the localization of macro-location, a localization scheme for indoor or outdoor can be used [SALA].

8. Micro-Location-Aware DNS Name

An IoT device can be located in the center or edge in a place that is specified by macro-location. For example, assume that a loop-detector is located in the start or end position of a road segment. If the DNS name for the loop-detector contains the start or end position of the road segment, a road network administrator can find it easily. In this document, for this DNS naming, the detailed location for an IoT device can be specified as a micro-location subdomain name.

A subdomain name for micro-location (denoted as mic_loc) MAY be placed between the keyword OID and macro-location (denoted as mac_loc) of the DNS name format in Figure 2. For the localization of micro-location, a localization scheme for indoor or outdoor can be used [SALA].

9. DNS Name Management for Mobile IoT Devices

Some IoT devices can have mobility, such as vehicle, smartphone, tablet, laptop computer, and cleaning robot. This mobility allows the IoT devices to move from a subnet to another subnet where subnets can have different domain suffixes, such as coordinate.road_segment.road, coordinate.intersection.road, living_room.home and garage.home. The DNS name change (or addition) due to the mobility should be considered.

To deal with DNS name management in mobile environments, whenever an IoT device enters a new subnet and receives DNS suffix domain names, it generates its new DNS names and registers them into a designated DNS server, specified by RDNSS option.

When the IoT device recognizes the movement to another subnet, it can delete its previous DNS name(s) from the DNS server having the DNS name(s), using DNS dynamic update [RFC2136]. For at least one DNS name to remain in a DNS server for the location management in Mobile IPv6 [RFC6275], the IoT device does not delete its default DNS name in its home network in Mobile IPv6.

10. Service Discovery for IoT Devices

DNS SRV resource record (RR) can be used to support the service discovery of the services provided by IoT devices [RFC2782]. This SRV RR specifies a service name, a transport layer protocol, the corresponding port number, and an IP address of a process running in an IP host as a server to provide a service. An instance for a service can be specified in this SRV RR in DNS-based service discovery [RFC6763]. After the DNS name registration in Section 5.2, IoT devices can register their services in the DNS server via a router with DNS SRV RRs for their services.

After the service registration, an IoT user can retrieve services available in his/her target network through service discovery, which can fetch the SRV RRs from the DNS server in the target network. Once (s)he retrieves the list of the SRV RRs, (s)he can monitor or remote-control the devices or their services by using the known protocols and domain information of the devices or their services. For this monitoring or remote-controlling of IoT devices, Constrained Application Protocol (CoAP) can be used [RFC7252].

11. Security Considerations

This document shares all the security issues of the NI protocol that are specified in the "Security Considerations" section of [RFC4620].

To prevent the disclosure of location information for privacy concern, the subdomains related to location can be encrypted by a shared key or public-and-private keys. For example, a DNS name of vehicle1.oid1.OID.coordinate1.road_segment_id1.LOC.road can be represented as vehicle1.oid1.OID.xxx.yyy.LOC.road where vehicle1 is unique ID, oid1 is object ID, xxx is a string of the encrypted representation of the coordinate (denoted as coordinate1) in a road segment, and yyy is a string of the encrypted representation of the road segment ID (denoted as road_segment_id1). Thus, the location of the vehicle1 can be protected from unwanted users by encryption.

12. Acknowledgments

This work was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2017M3C4A7065980). This work was supported in part by the Global Research Laboratory Program (2013K1A1A2A02078326) through NRF and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science and ICT.

13. Contributors

This document is the group work of IPWAVE working group. This document has the following contributing authors considered co-authors:

- Keuntae Lee (Sungkyunkwan University)
- Seokhwa Kim (Sungkyunkwan University)

14. References

14.1. Normative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

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

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

[RFC4033] Arends, R., Ed., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[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.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, February 2013.

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

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

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

[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-802.11b]
IEEE Std 802.11b, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band", September 1999.

[IEEE-802.11g]
IEEE P802.11g/D8.2, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Further Higher Data Rate Extension in the 2.4 GHz Band", April 2003.

[IEEE-802.11n]
IEEE P802.11n/D9.0, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 5: Enhancements for Higher Throughput", March 2009.

[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", July 2010.

[IEEE-802.15.1]
IEEE Std 802.15.1, "Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPANs)", June 2005.

[IEEE-802.15.4]
IEEE Std 802.15.4, "Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", September 2011.

[IEEE-802.3]
IEEE Std 802.3, "IEEE Standard for Ethernet", December 2012.

[oneM2M-OID]
oneM2M, "Object Identifier based M2M Device Identification Scheme", February 2014.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4620] Crawford, M. and B. Haberman, Ed., "IPv6 Node Information Queries", RFC 4620, August 2006.

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

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

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

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

[SALA] Jeong, J., Yeon, S., Kim, T., Lee, H., Kim, S., and S. Kim, "SALA: Smartphone-Assisted Localization Algorithm for Positioning Indoor IoT Devices", Springer Wireless Networks, Vol. 24, No. 1, January 2018.

Appendix A. Changes from draft-jeong-ipwave-iot-dns-autoconf-01

The following changes are made from draft-jeong-ipwave-iot-dns-autoconf-01:

- Section 1 includes the registration of the DNS names of IoT devices into DNS servers and the retrieval of those DNS names from the DNS server for monitoring and remote-controlling the IoT devices.

- In Section 1, cloud-based DNS naming services are explained, where IoT users can monitor or remote-control their IoT devices in the Internet.

- In Sections 5.2.3 and 10, it is explained that CoAP can be used to monitor or remote-control IoT devices.

Authors' Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
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

Sejun Lee
Ericsson-LG
77, Heungan-Daero 81 Beon-Gil, Dongan-Gu
Anyang-Si, Gyeonggi-Do 14117
Republic of Korea

Phone: +82 31 450 4099
EMail: prosejun14@gmail.com

Jung-Soo Park
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu
Daejeon 34129
Republic of Korea

Phone: +82 42 860 6514
EMail: pjs@etri.re.kr

IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 6, 2021

J. Jeong
Sungkyunkwan University
S. Lee
Ericsson-LG
J. Park
ETRI

November 2, 2020

DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks

draft-jeong-ipwave-iot-dns-autoconf-09

Abstract

This document specifies an autoconfiguration scheme for device discovery and service discovery in IP-based vehicular networks. Through the device discovery, this document supports the global (or local) DNS naming of Internet-of-Things (IoT) devices, such as sensors, actuators, and in-vehicle units. By this scheme, the DNS name of an IoT device can be autoconfigured with the device's model information in wired and wireless target networks (e.g., vehicle, road network, home, office, shopping mall, and smart grid). Through the service discovery, IoT users (e.g., drivers, passengers, home residents, and customers) in the Internet (or local network) can easily identify each device for monitoring and remote-controlling it in a target network.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Many Internet-of-Things (IoT) devices (e.g., sensors, actuators, and in-vehicle units) have begun to have wireless communication capability (e.g., WiFi, Bluetooth, and ZigBee) for monitoring and remote-controlling in a local network or the Internet. According to the capacity, such IoT devices can be categorized into high-capacity devices and low-capacity devices. High-capacity devices have a high-power processor and a large storage, such as vehicles, road infrastructure devices (e.g., road-side unit, traffic light, and loop-detector), appliances (e.g., television, refrigerator, air conditioner, and washing machine), and smart devices (smartphone and tablet). They are placed in environments (e.g., vehicle, road network, home, office, shopping mall, and smart grid) for the direct use for human users, and they require the interaction with human users. Low-capacity devices have a low-power processor and a small storage, such as sensors (e.g., in-vehicle units, light sensor, meter, and fire detector) and actuators (e.g., vehicle engine, signal light, street light, and room temperature controller). They are installed for the easy management of environments (e.g., vehicle, road network, home, office, store, and factory), and they do not require the interaction with human users.

For the Internet connectivity of IoT devices, a variety of parameters (e.g., address prefixes, default routers, and DNS servers) can be automatically configured by Neighbor Discovery (ND) for IP Version 6, IPv6 Stateless Address Autoconfiguration, and IPv6 Router Advertisement (RA) Options for DNS Configuration [RFC4861][RFC4862] [RFC8106].

For these IoT devices, the manual configuration of DNS names will be cumbersome and time-consuming as the number of them increases rapidly in a network. It will be good for such DNS names to be automatically configured such that they are readable to human users.

Multicast DNS (mDNS) in [RFC6762] can provide DNS service for networked devices on a local link (e.g., home network and office network) without any conventional recursive DNS server. mDNS also supports the autoconfiguration of a device's DNS name without the intervention of the user. mDNS aims at the DNS naming service for the local DNS names of the networked devices on the local link rather than the DNS naming service for the global DNS names of such devices in the Internet. However, for IoT devices accessible from the Internet, mDNS cannot be used. Thus, a new autoconfiguration scheme becomes required for the global DNS names of IoT devices.

This document proposes an autoconfiguration scheme for the global (or local) DNS names of IoT devices in IP-based vehicular networks. Since an autoconfigured DNS name contains the model identifier (ID) of a device, IoT users in the Internet (or local network) can easily identify such a device. The autoconfigured DNS names and the corresponding IP addresses of the IoT devices are registered with local or remote authoritative DNS servers that manage the DNS suffixes of the DNS domain names. With these DNS names, they will be able to monitor and remote-control their IoT devices with their smart devices (e.g., smartphone and tablet PC) by resolving their DNS names into the corresponding IP addresses.

For cloud-based DNS naming services of IoT devices, a cloud server can collect DNS zone files having the global DNS names and IP addresses of the IoT devices from multiple DNS servers and provide IoT users with such global DNS names of IoT devices relevant to the IoT users. These IoT users can monitor and remote-control their IoT devices in the Internet with the global DNS names and IP addresses, using their smart devices.

1.1. Applicability Statements

It is assumed that IoT devices have networking capability through wired or wireless communication media, such as Ethernet [IEEE-802.3], WiFi [IEEE-802.11][IEEE-802.11a][IEEE-802.11b][IEEE-802.11g] [IEEE-802.11n], Dedicated Short-Range Communications (DSRC) [DSRC-WAVE][IEEE-802.11p], Bluetooth [IEEE-802.15.1], and ZigBee [IEEE-802.15.4] in a local area network (LAN) or personal area network (PAN). Note that IEEE 802.11p was renamed IEEE 802.11 Outside the Context of a Basic Service Set [IEEE-802.11-OCB] in 2012. IPv6 packet delivery over an IEEE 802.11-OCB link is defined in [RFC8691].

Also, it is assumed that each IoT device has a factory configuration (called device configuration) having device model information by manufacturer ID and model ID (e.g., vehicle, road-side unit, smart TV, smartphone, tablet, and refrigerator). This device configuration can be read by the device for DNS name autoconfiguration.

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:

- o Device Configuration: A factory configuration that has device model information by manufacturer ID and model ID (e.g., vehicle, road-side unit, smart TV, smartphone, tablet, and refrigerator).

o DNS Search List (DNSSL): The list of DNS suffix domain names used by IPv6 hosts when they perform DNS query searches for short, unqualified domain names [RFC8106].

o DNSSL Option: IPv6 RA option to deliver the DNSSL information to IPv6 hosts [RFC8106].

4. Overview

This document specifies an autoconfiguration scheme for an IoT device using device configuration and DNS search list. Device configuration has device model information (e.g., device's manufacturer and model). DNS search list has DNS suffix domain names that represent the DNS domains of a network having the IoT device [RFC8106].

As an IPv6 host, the IoT device can obtain DNS search list through IPv6 Router Advertisement (RA) with DNS Search List (DNSSL) Option [RFC4861][RFC8106] or DHCPv6 with Domain Search List Option [RFC3315][RFC3736][RFC3646].

The IoT device can construct its DNS name with the concatenation of manufacturer ID, model ID, and domain name. Since there exist more than one device with the same model, the DNS name should have a unique identification (e.g., unique ID or serial ID) to differentiate multiple devices with the same model.

Since both RA and DHCPv6 can be simultaneously used for the parameter configuration for IPv6 hosts, this document considers the DNS name autoconfiguration in the coexistence of RA and DHCP.

5. DNS Name Autoconfiguration

The DNS name autoconfiguration for an IoT device needs the acquisition of DNS search list through either RA [RFC8106] or DHCPv6 [RFC3646]. Once the DNS search list is obtained, the IoT device autonomously constructs its DNS name(s) with the DNS search list and its device information.

5.1. DNS Name Format with Object Identifier

A DNS name for an IoT device can have the following format with object identifier (OID), which is defined in [oneM2M-OID], as in Figure 1:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   unique_id.object_identifier.OID.domain_name   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 1: IoT Device DNS Name Format with OID

Fields:

unique_id — unique identifier to guarantee the uniqueness of the DNS name in ASCII characters. The identifier MAY be alphanumeric with readability, e.g., product name plus a sequence number.

object_identifier — device's object identifier that consists of a higher arc, that is, M2M node indication ID (i.e., the concatenation of the managing organization, administration, data country code, and M2M node) and a sequence of four arcs (i.e., manufacturer ID, model ID, serial ID, and expanded ID) as defined in [oneM2M-OID]. The fields are separated by an underscore '_'.

OID — subdomain for the keyword of OID to indicate that object_identifier is used.

domain_name — domain name that represents a DNS domain for the network having the IoT devices.

Note each subdomain (i.e., unique_id, object_identifier, OID, and domain_name) in the domain name format in Figure 1 is expressed using the name syntax described in [RFC1035].

5.2. Procedure of DNS Name Autoconfiguration

The procedure of DNS name autoconfiguration is performed through a DNSSL option delivered by either RA [RFC8106] or DHCPv6 [RFC3646].

5.2.1. DNS Name Generation

When as an IPv6 host a device receives a DNSSL option through either RA or DHCPv6, it checks the validity of the DNSSL option. If the option is valid, the IPv6 host performs the DNS name autoconfiguration with each DNS suffix domain name in the DNSSL option as follows:

1. The host constructs its DNS name with the DNS suffix domain name along with device configuration (i.e., manufacturer ID, model ID,

and serial ID) and a selected identifier (as unique_id) that is considered unique, which is human-friendly, as shown in Figure 1.

2. The host constructs an IPv6 unicast address as a tentative address with a 64-bit network prefix and the last 64 bits of the MD5 hashed value of the above DNS name.

3. The host constructs the solicited-node multicast address in [RFC4861] corresponding to the tentative IPv6 address.

4. The host performs Duplicate Address Detection (DAD) for the IPv6 address with the solicited-node multicast address [RFC4861] [RFC4862].

5. If there is no response from the DAD, the host sets the IPv6 tentative address as its IPv6 unicast address and regards the constructed DNS name as unique on the local link. Otherwise, since the DAD fails because of DNS name conflict, go to Step 1 for a new DNS name generation with another identifier for unique_id.

6. Since the DNS name is proven to be unique, it is used as the device's DNS name and the DNS autoconfiguration is done for the given DNS suffix domain name. Also, the host joins the solicited-node multicast address for the verified DNS name in order to prevent other hosts from using this DNS name.

When the DNS search list has more than one DNS suffix domain name, the IPv6 host repeats the above procedure until all of the DNS suffixes are used for the DNS name autoconfiguration along with the IPv6 unicast autoconfiguration corresponding to the DNS name.

5.2.2. DNS Name Registration

Once as IPv6 hosts the devices have autoconfigured their DNS names, as a collector, any IPv6 node (i.e., router or host) in the same subnet can collect the device DNS names using IPv6 Node Information (NI) protocol [RFC4620].

For a collector to collect the device DNS names without any prior node information, a new NI query needs to be defined. That is, a new ICMPv6 Code (e.g., 3) SHOULD be defined for the collection of the IPv6 host DNS names. The Data field is not included in the ICMPv6 header since the NI query is for all the IPv6 hosts in the same subnet. The Qtype field for NI type is set to 2 for Node Name.

The query SHOULD be transmitted by the collector to a link-local multicast address for this NI query. Assume that a link-local scope multicast address (e.g., all-nodes multicast address, FF02::1) SHOULD be defined for device DNS name collection such that all the IPv6 hosts join this link-local multicast address for the device DNS name collection service.

When an IPv6 host receives this query sent by the collector in multicast, it transmits its Reply with its DNS name with a random interval between zero and Query Response Interval, as defined by Multicast Listener Discovery Version 2 [RFC3810]. This randomly delayed Reply allows the collector to collect the device DNS names with less frame collision probability by spreading out the Reply time instants.

After the collector collects the device DNS names, it resolves the DNS names into the corresponding IPv6 addresses by NI protocol [RFC4620] with the ICMPv6 Code 1 of NI Query. This code indicates that the Data field of the NI Query has the DNS name of an IoT device. The IoT device that receives this NI query sends the collector an NI Reply with its IPv6 address in the Data field.

For DNS name resolution service, the collector can register the pair(s) of DNS name and IPv6 address for each IPv6 host with an appropriate designated DNS server for the DNS domain suffix of the DNS name. It is assumed that the collector is configured to register DNS names with the designated DNS server in a secure way based on DNSSEC [RFC4033][RFC6840]. This registration of the DNS name and IPv6 address can be performed by DNS dynamic update [RFC2136]. Before registering the DNS name with the designated DNS server, the collector SHOULD verify the uniqueness of the DNS name in the intended DNS domain by sending a DNS query for the resolution of the DNS name. If there is no corresponding IPv6 address for the queried DNS name, the collector registers the DNS name and the corresponding IPv6 address for each IPv6 host with the designated DNS server. On the other hand, if there is such a corresponding IPv6 address, the DNS name is regarded as duplicate (i.e., not unique), and so the collector notifies the corresponding IoT device with the duplicate DNS name of an error message of DNS name duplication using NI protocol. When an IoT device receives such a DNS name duplication error, it needs to construct a new DNS name and repeats the procedure of device DNS name generation along with the uniqueness test of the device DNS name in its subnet.

The two separate procedures of the DNS name collection and IPv6 address resolution in the above NI protocol can be consolidated into a single collection for the pairs of DNS names and the corresponding IPv6 addresses. For such an optimization, a new ICMPv6 Code (e.g., 4) is defined for the NI Query to query the pair of a DNS name and the corresponding IPv6 address. With this code, the collector can collect the pairs of each IoT device's DNS name and IPv6 address in one NI query message rather than two NI query messages.

For DNS name registration of IoT devices as IPv6 hosts, DHCPv6 [RFC3315] can be used instead of the NI protocol. For this purpose, a new DHCP option (called DNSNA option) needs to be defined to collect the pair of a DNS name and the corresponding IPv6 address of an IoT device. As a DNS information collector, a DHCPv6 server (or a router running a DHCPv6 server) sends a request message for the DHCP DNSNA option to IoT devices as its DHCPv6 clients under its address pool. The clients respond to this request message by sending the DHCPv6 server a reply message with their DNS information. Thus, the DHCPv6 server can collect the pairs of DNS names and the corresponding IPv6 addresses of the IoT devices. Then, as a collector, the DHCPv6 server can register the DNS names and the corresponding IPv6 addresses of IoT devices with the designated DNS server.

To allow only a legitimate IoT device to register its DNS name and IPv6 address with the designated DNS server via a router (or DHCPv6 server), the IoT device can sign its registration message with its private key through a digital signature, and the router (or DHCPv6 server) can verify the message with the IoT device's public key. For the detailed authentication based on a digital signature, refer to [DNSNA-FGCS].

5.2.3. DNS Name Retrieval

For device discovery, a smart device (e.g., smartphone) can retrieve the DNS names of IoT devices by contacting a global (or local) DNS server having the IoT device DNS names. If the smart device can retrieve the zone file with the DNS names, it can display the information of IoT devices in a target network, such as a vehicle's internal network, home network, and office network. With this information, the user can monitor and control the IoT devices in the Internet (or local network). To monitor or remote-control IoT devices, Constrained Application Protocol (CoAP) can be used [RFC7252].

6. Location-Aware DNS Name Configuration

If the DNS name of an IoT device includes location information, it allows users to easily identify the physical location of each device. This document proposes the representation of a location in a DNS name. In this document, the location in a DNS name consists of two levels for a detailed location specification, such as macro-location for a large area and micro-location for a small area.

To denote both macro-location (i.e., mac_loc) and micro-location (i.e., mic_loc) into a DNS name, the following format is described as in Figure 2:

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| unique_id.object_identifier.OID.mic_loc.mac_loc.LOC.domain_name |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Location-Aware Device DNS Name Format

Fields:

unique_id — unique identifier to guarantee the uniqueness of the DNS name in ASCII characters. The identifier MAY be alphanumeric with readability, such as product name plus a sequence number.

object_identifier — device's object identifier that consists of a higher arc, that is, M2M node indication ID (i.e., the concatenation of the managing organization, administration, data country code, and M2M node) and a sequence of four arcs (i.e., manufacturer ID, model ID, serial ID, and expanded ID) as defined in [oneM2M-OID]. The fields are seperated by an underscore '_'.

OID — subdomain for the keyword of OID to indicate that object_identifier is used.

mic_loc — device's micro-location, such as an offset in a road segment and coordinates in 2-dimensional (or 3-dimensional) space.

mac_loc — device's macro-location, such as a road segment and 2-dimensional (or 3-dimensional) space.

LOC — subdomain for the keyword of LOC to indicate that mac_loc and mic_loc are used.

domain_name — domain name that represents a DNS domain for the network having the IoT devices.

Note each subdomain (e.g., mic_loc and mac_loc) in the domain name format in Figure 2 is expressed using the name syntax described in [RFC1035].

7. Macro-Location-Aware DNS Name

If location information (such as cross area, intersection, and road segment in a road network) is available to an IoT device, a keyword, coordinate, or location ID for the location information can be used to construct a DNS name as subdomain name. This location information lets users track the position of mobile devices (such as vehicle, smartphone, and tablet). The physical location of the device is defined as macro-location for DNS naming.

A subdomain name for macro-location (denoted as mac_loc) MAY be placed between micro-location (denoted as mic_loc) and the keyword LOC of the DNS name format in Figure 2. For the localization of macro-location, a localization scheme for indoor or outdoor can be used [SALA].

8. Micro-Location-Aware DNS Name

An IoT device can be located in the center or edge in a place that is specified by macro-location. For example, assume that a loop-detector is located in the start or end position of a road segment. If the DNS name for the loop-detector contains the start or end position of the road segment, a road network administrator can find it easily. In this document, for this DNS naming, the detailed location for an IoT device can be specified as a micro-location subdomain name.

A subdomain name for micro-location (denoted as mic_loc) MAY be placed between the keyword OID and macro-location (denoted as mac_loc) of the DNS name format in Figure 2. For the localization of micro-location, a localization scheme for indoor or outdoor can be used [SALA].

9. DNS Name Management for Mobile IoT Devices

Some IoT devices can have mobility, such as vehicle, smartphone, tablet, laptop computer, and cleaning robot. This mobility allows the IoT devices to move from a subnet to another subnet where subnets can have different domain suffixes, such as coordinate.road_segment.road, coordinate.intersection.road, living_room.home and garage.home. The DNS name change (or addition) due to the mobility should be considered.

To deal with DNS name management in mobile environments, whenever an IoT device enters a new subnet and receives DNS suffix domain names, it generates its new DNS names and registers them with a designated DNS server, specified by RDNSS option.

When the IoT device recognizes the movement to another subnet, it can delete its previous DNS name(s) from the DNS server having the DNS name(s), using DNS dynamic update [RFC2136]. For at least one DNS name to remain in a DNS server for the location management in Mobile IPv6 [RFC6275], the IoT device does not delete its default DNS name in its home network in Mobile IPv6.

10. Device Discovery for IoT Devices

DNSNA can facilitate the device discovery of a user for IoT devices using a global (or local) DNS server having the IoT device DNS information, as discussed in Section 5.2.3. This device discovery based on unicast outperforms mDNS [RFC6762] using multicast in terms of the discovery speed and the network bandwidth usage for discovery.

For example, a vehicle can have its own internal network having in-vehicle devices (e.g., Electronic Control Units (ECUs) such as engine control module, powertrain control module, transmission control module, and brake control module). When the vehicle's internal network is constructed by the Ethernet, those ECUs can autoconfigure their DNS names with the DNSNA and register them with the vehicle's local DNS server [ID-IPWAVE-PS]. The local DNS server can register them with a global DNS server accessible by the automotive service center to monitor and make on-line diagnosis on them.

11. Service Discovery for IoT Devices

DNS SRV resource record (RR) can be used to support the service discovery of the services provided by IoT devices [RFC2782]. This SRV RR specifies a service name, a transport layer protocol, the corresponding port number, and an IP address of a process running in an IP host as a server to provide a service. An instance for a service can be specified in this SRV RR in DNS-based service discovery [RFC6763]. After the DNS name registration in Section 5.2, IoT devices can register their services with the DNS server via a router with DNS SRV RRs for their services.

After the service registration, an IoT user can retrieve services available in his/her target network through service discovery, which can fetch the SRV RRs from the DNS server in the target network. Once (s)he retrieves the list of the SRV RRs, (s)he can monitor or remote-control the devices or their services by using the known protocols and domain information of the devices or their services. For this monitoring or remote-controlling of IoT devices, Constrained Application Protocol (CoAP) can be used [RFC7252].

12. Security Considerations

This document shares all the security issues of the NI protocol that are specified in the "Security Considerations" section of [RFC4620].

To prevent the disclosure of location information for privacy concern, the subdomains related to location can be encrypted by a shared key or public-and-private keys. For example, a DNS name of vehicle1.oid1.OID.coordinate1.road_segment_id1.LOC.road can be represented as vehicle1.oid1.OID.xxx.yyy.LOC.road where vehicle1 is unique ID, oid1 is object ID, xxx is a string of the encrypted representation of the coordinate (denoted as coordinate1) in a road segment, and yyy is a string of the encrypted representation of the road segment ID (denoted as road_segment_id1). Thus, the location of the vehicle1 can be protected from unwanted users by encryption.

13. Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

This work was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2017-0-01633) supervised by the IITP (Institute for Information & communications Technology Promotion).

14. Contributors

This document is the group work of IPWAVE working group. This document has the following contributing authors considered co-authors:

- o Keuntae Lee (Sungkyunkwan University)
- o Seokhwa Kim (Sungkyunkwan University)

15. References

15.1. Normative References

[ID-IPWAVE-PS]
Jeong, J., Ed., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", draft-ietf-ipwave-vehicular-networking-19 (work in progress), July 2020.

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[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.

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

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

[RFC4033] Arends, R., Ed., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[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.

[RFC6840] Weiler, S., Ed. and D. Blacka, Ed., "Clarifications and Implementation Notes for DNS Security (DNSSEC)", RFC 6840, February 2013.

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

[RFC8691] Benamar, N., Haerri, 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, December 2019.

15.2. Informative References

[DNSNA-FGCS]
Lee, K., Kim, S., Jeong, J., Lee, S., Kim, H., and J. Park, "A Framework for DNS Naming Services for Internet-of-Things Devices", Elsevier Future Generation Computer Systems, Vol. 92, March 2019.

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

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

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

[IEEE-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-802.11b]
"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Higher-Speed Physical Layer Extension in the 2.4 GHz Band", September 1999.

[IEEE-802.11g]
"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Further Higher Data Rate Extension in the 2.4 GHz Band", April 2003.

[IEEE-802.11n]
"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 5: Enhancements for Higher Throughput", March 2009.

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

[IEEE-802.15.1]
"Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPANs)", June 2005.

[IEEE-802.15.4]
"Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)", September 2011.

[IEEE-802.3]
"IEEE Standard for Ethernet", December 2012.

[oneM2M-OID]
"Object Identifier based M2M Device Identification Scheme", February 2014.

[RFC2136] Vixie, P., Ed., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4620] Crawford, M. and B. Haberman, Ed., "IPv6 Node Information Queries", RFC 4620, August 2006.

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

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

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

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

[SALA] Jeong, J., Yeon, S., Kim, T., Lee, H., Kim, S., and S. Kim, "SALA: Smartphone-Assisted Localization Algorithm for Positioning Indoor IoT Devices", Springer Wireless Networks, Vol. 24, No. 1, January 2018.

Appendix A. Changes from draft-jeong-ipwave-iot-dns-autoconf-08

The following changes are made from draft-jeong-ipwave-iot-dns-autoconf-08:

- This version has a submission date update to maintain the active status of the draft.

- This version updates the version numbers of the referenced drafts.

- In the 6th paragraph of Section 5.2.2, a sentence is updated by replacing "corresponder" with "collector" as "On the other hand, if there is such a corresponding IPv6 address, the DNS name is regarded as duplicate (i.e., not unique), and so the collector notifies the corresponding IoT device with the duplicate DNS name of an error message of DNS name duplication using NI protocol."

- This version also updates other typos in the document.

Authors' Addresses

Jaehoon Paul Jeong
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
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Sejun Lee
Ericsson-LG
77, Heungan-Daero 81 Beon-Gil, Dongan-Gu
Anyang-Si, Gyeonggi-Do 14117
Republic of Korea

Phone: +82 31 450 4099
EMail: prosejun14@gmail.com

Jung-Soo Park
Electronics and Telecommunications Research Institute
218 Gajeong-Ro, Yuseong-Gu
Daejeon 34129
Republic of Korea

Phone: +82 42 860 6514
EMail: pjs@etri.re.kr

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 6, 2018

J. Jeong
Y. Shen
Y. Jo
Sungkyunkwan University
J. Jeong
Samsung Electronics
J. Lee
Sangmyung University

March 5, 2018

IPv6 Neighbor Discovery for Prefix and Service Discovery in Vehicular Networks

draft-jeong-ipwave-vehicular-neighbor-discovery-02

Abstract

This document specifies an extension of IPv6 Neighbor Discovery (ND) for rapid network prefix and service discovery in vehicular networks. It is assumed that a vehicle or a Road-Side Unit (RSU) have an external network interface and their internal network. The extended IPv6 ND called vehicular ND can support vehicle-to-infrastructure communications as well as vehicle-to-vehicle communications. This document defines new ND options to allow a vehicle to announce the network prefixes and services inside its internal network to another vehicle or RSU.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Vehicular Ad Hoc Networks (VANET) have been researched for the networking on intelligent services in road networks, such as driving safety, efficient driving, and entertainment. To enable this VANET in road networks, 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], considering the characteristics of vehicular networks, such as high-speed mobility and network fragmentation. Note that IEEE 802.11p was renamed IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012. For Wireless Access in Vehicular Environments (WAVE) [DSRC-WAVE][WAVE-1609.0], the IEEE has standardized IEEE 1609 family standards, such as IEEE 1609.2, 1609.3, and 1609.4 [WAVE-1609.2][WAVE-1609.3][WAVE-1609.4]. The IEEE 1609 standards specify IPv6 as the network-layer protocol [WAVE-1609.3].

Many automobile vendors are replacing Controller Area Networks (CANs) with Ethernet for high-speed interconnectivity among Electronic Control Units (ECUs) in a vehicle. The sensing information of the ECUs can be delivered to the service centers of those automobile ventors for remote diagnosis for driving safety using DSRC between vehicles and Road-Side Units (RSUs) having the Internet connectivity toward the service centers in a vehicular cloud.

With this trend, it is time to enable vehicular networking with IPv6 to let various Internet-based applications (e.g., remote vehicle diagnosis) run on top of transport-layer protocols, such as TCP, UDP, and SCTP. IPv6 [RFC2460] is suitable for a network layer in vehicular networks in that the protocol has abundant address space, autoconfiguration features, and protocol extension ability through extension headers.

To support the interaction between vehicles or between a vehicle and an RSU, this document specifies an extension of IPv6 ND [RFC4861] for rapid network prefix and service discovery in vehicular networks with new ND options. That is, the extended IPv6 ND in this document, which is called vehicular ND, can support not only vehicle-to-infrastructure (V2I) communications but also vehicle-to-vehicle (V2V) communications.

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:

- o 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.

- o 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.

- o 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 an IPv6 ND extension for vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) networking.

Figure 1 shows the V2V networking of two vehicles whose internal networks are Moving Network1 and Moving Network2, respectively. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). Vehicle2 has the DNS Server (RDNSS2), the two hosts (Host3 and Host4), and the two routers (Router3 and Router4).

It is assumed that Host1 and Host3 are running a Cooperative Adaptive Cruise Control (C-ACC) program for physical collision avoidance. Also, it is assumed that Host2 and Host4 are running a Cooperative On-board Camera Sharing (C-OCS) program for sharing road hazards or obstacles to avoid road accidents. Vehicle1's Router1 and Vehicle2's Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking for various vehicular services. The vehicular applications, such as C-ACC and C-BCS, can be registered into the DNS Server (i.e., RDNSS) through DNSNA protocol in [ID-DNSNA] along with IPv6 ND DNS options in [RFC6106].

Vehicle1's Router1 and Vehicle2's Router3 can know what vehicular applications exist in their internal network by referring to their own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know what network prefixes exist in their internal network through an intra-domain routing protocoli, such as OSFP. Each vehicle announces its network prefixes and services through ND options defined in Section 5.

```
                           (*)<..........>(*)
                            |              | 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|      | Host4 |     |
   | ._______.      ._______.     |  | ._______.      ._______.     |
   |     ^              ^         |  |     ^              ^         |
   |     |              |         |  |     |              |         |
   |     v              v         |  |     v              v         |
   | ---------------------------- |  | ---------------------------- |
   |  2001:DB8:10:2::/64          |  |       2001:DB8:20:2::/64     |
   .______________________________.  .______________________________.
      Vehicle1 (Moving Network1)        Vehicle2 (Moving Network2)

      <----> Wired Link   <....> Wireless Link   (*) Antenna
```

            Figure 1: Internetworking between Vehicle Networks

Figure 2 shows the V2I networking of a vehicle and an RSU whose internal networks are Moving Network1 and Fixed Network1, respectively. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). RSU1 has the DNS Server (RDNSS2), one host (Host3), the two routers (Router3 and Router4).

It is assumed that RSU1 has a collection of servers (Server1 to ServerN) for various services in the road networks, such as road emergency notification and navigation services. Vehicle1's Router1 and RSU1's Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for I2V networking for various vehicular services. The vehicular applications, such as road emergency notification and navigation services, can be registered into the DNS Server (i.e., RDNSS) through DNSNA protocol in [ID-DNSNA] along with IPv6 ND DNS options in [RFC6106].

Vehicle1's Router1 and RSU1's Router3 can know what vehicular applications exist in their internal network by referring to their own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know what network prefixes exist in their internal network through an intra-domain routing protocoli, such as OSFP. Each vehicle and each RSU announce their network prefixes and services through ND options defined in Section 5.

```
                        (*)<..........>(*)
                         |              | 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. ND Extension for Prefix and Service Discovery

This section defines two new ND options for prefix and service discovery: (i) the Vehicular Prefix Information (VPI) option and (ii) the Vehicular Service Information (VSI) option. It also describes the ND protocol for such prefix and service discovery.

5.1. Vehicular Prefix Information Option

The VPI option contains one IPv6 prefix in the internal network. Figure 3 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 3: 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.

5.2. Vehicular Service Information Option

The VSI option contains one vehicular service in the internal network. Figure 4 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 4: 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 the protocol.

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

5.3. Vehicular Neighbor Discovery

With VPI and VSI options, a node (e.g., vehicle or RSU) can announce the network prefixes and services in its internal network via ND messages, such as Neighbor Solicitation (NS) and Neighbor Advertisement (NA) [RFC4861].

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

Through this procedure, vehicles and RSUs can rapidly discover the network prefixes and services of the other party without any additional service discovery protocol.

6. Security Considerations

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

7. Acknowledgments

This work was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2017M3C4A7065980). This work was supported in part by the Global Research Laboratory Program (2013K1A1A2A02078326) through NRF and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science and ICT.

8. References

8.1. 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.

[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.

8.2. Informative References

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

[ID-DNSNA]
Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-02 (work in progress), March 2018.

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

[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-802.11p]
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.

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

[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.

Appendix A. Changes from draft-jeong-ipwave-vehicular-neighbor-discovery-01

The following changes are made from draft-jeong-ipwave-vehicular-neighbor-discovery-01:

- In Section 1, the following sentence is added: Note that IEEE 802.11p was renamed IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012.

- In Section 1, references for WAVE are added as follows: For Wireless Access in Vehicular Environments (WAVE) [DSRC-WAVE] [WAVE-1609.0], the IEEE has standardized IEEE 1609 family standards, such as IEEE 1609.2, 1609.3, and 1609.4 [WAVE-1609.2][WAVE-1609.3][WAVE-1609.4]. The IEEE 1609 standards specify IPv6 as the network-layer protocol [WAVE-1609.3].

Authors' Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
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

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
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu

Younghwa Jo
Department of Software Platform
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: movie_jo@naver.com

Junsik Jeong
Software R&D Center
Samsung Electronics
Seoul R&D Campus D-Tower, 56, Seongchon-Gil, Seocho-Gu
Seoul 06765
Republic of Korea

EMail: jun.jeong@samsung.com

Jong-Hyouk Lee
Sangmyung University
Sangmyung University
31, Sangmyeongdae-gil, Dongnam-gu
Cheonan, NY 31066
Republic of Korea

EMail: jonghyouk@smu.ac.kr

IPWAVE Working Group J. Jeong
Internet-Draft Y. Shen
Intended status: Standards Track Z. Xiang
Expires: May 6, 2021 Sungkyunkwan University
S. Cespedes
NIC Chile Research Labs
Nov 2, 2020

Vehicular Neighbor Discovery for IP-Based Vehicular Networks
draft-jeong-ipwave-vehicular-neighbor-discovery-10

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).

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 2012. IEEE has standardized a family standard suite of WAVE as IEEE 1609. This IEEE 1609 is considered as a key component in 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] to 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) [ID-IPWAVE-PS] 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 relatively long-time Neighbor Discovery (ND) process in IPv6 [RFC4861] is not suitable in VANET scenarios.

To 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 [ID-IPWAVE-VMM] .

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:

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

- o 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.

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

- o 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:

- o To perform prefix and service discovery through ND procedure;

- o 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;

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

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

- o To support multi-hop 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 multi-hop 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.

The 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 [ID-IPWAVE-PS].

```
                     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 informations 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 [ID-DNSNA]), 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 [ID-IPWAVE-VMM].

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 multi-hop 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 Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

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-2020-2017-0-01633) supervised by the IITP.

10. References

10.1. Normative References

[ID-IPWAVE-PS]
Jeong, J., Ed., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", draft-ietf-ipwave-vehicular-networking-19 (work in progress), July 2020.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[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.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

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

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

[RFC6775] Shelby, Z., Ed., "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 8200, July 2017.

[RFC8691] Benamar, N., Haerri, 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, December 2019.

10.2. Informative References

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

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

[ID-DNSNA]
Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet-of-Things Devices in IP-Based Vehicular Networks", draft-jeong-ipwave-iot-dns-autoconf-09 (work in progress), October 2020.

[ID-IPWAVE-VMM]
Jeong, J., Ed., Shen, Y., and Z. Xiang, "Vehicular Mobility Management for IP-Based Vehicular Networks", draft-jeong-ipwave-vehicular-mobility-management-04 (work in progress), October 2020.

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

[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.

[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.

[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.

Appendix A. Changes from draft-jeong-ipwave-vehicular-neighbor-discovery-09

The following changes are made from draft-jeong-ipwave-vehicular-neighbor-discovery-09:

- o This version updates the version numbers of the referenced drafts.
- o The abstract is updated to smooth the description.
- o In Section 1, the reference [DSRC-WAVE] for DSRC is moved to the initial appeared place.
- o In the last paragraph of Section 1, the first sentence is updated by adding "procedure" to "a Vehicular Neighbor Discovery (VND)" as "a Vehicular Neighbor Discovery (VND) procedure".
- o In Section 3, the reference [RFC8691] is added, and the terms and definitions of RSU and OBU are deleted due to duplicated definitions in [RFC8691].
- o In Section 4, the description is updated.
- o The uncited normative reference RFC8106 is deleted.

Authors' Addresses

Jaehoon Paul Jeong
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
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

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

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu

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
Fax: +82 31 290 7996
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