

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2018

A. Petrescu
CEA, LIST
N. Benamar
Moulay Ismail University
J. Haerri
Eurecom
J. Lee
Sangmyung University
T. Ernst
YoGoKo
October 16, 2017

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-11.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

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

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

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

This Internet-Draft will expire on April 19, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Terminology	3
3. Communication Scenarios where IEEE 802.11-OCB Links are Used	5
4. IPv6 over 802.11-OCB	5
4.1. Maximum Transmission Unit (MTU)	5
4.2. Frame Format	5
4.2.1. Ethernet Adaptation Layer	6
4.3. Link-Local Addresses	8
4.4. Address Mapping	8
4.4.1. Address Mapping -- Unicast	8
4.4.2. Address Mapping -- Multicast	8
4.5. Stateless Autoconfiguration	9
4.6. Subnet Structure	9
5. Security Considerations	10
6. IANA Considerations	11
7. Contributors	11
8. Acknowledgements	11
9. References	12
9.1. Normative References	12
9.2. Informative References	14
Appendix A. ChangeLog	16
Appendix B. 802.11p	22
Appendix C. Aspects introduced by the OCB mode to 802.11	22
Appendix D. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver	26
Appendix E. EtherType Protocol Discrimination (EPD)	27
Appendix F. Design Considerations	28
F.1. Vehicle ID	28
F.2. Reliability Requirements	29
F.3. Multiple interfaces	29
F.4. MAC Address Generation	30

Appendix G. IEEE 802.11 Messages Transmitted in OCB mode	31
Appendix H. Implementation Status	31
H.1. Capture in Monitor Mode	32
H.2. Capture in Normal Mode	34
Authors' Addresses	36

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:

- o 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 in Section 4.2.1. The operation of IP on Ethernet is described in [RFC1042], [RFC2464] and [I-D.hinden-6man-rfc2464bis].
- o 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].

WiFi: Wireless Fidelity.

OBRU (On-Board Router Unit): an OBRU is almost always situated in a vehicle; it is a computer with at least two IP real or virtual

interfaces; at least one IP interface runs in OCB mode of 802.11. It MAY be an IP Router.

OBU (On-Board Unit): term defined outside the IETF.

RSRU (Road-Side Router Unit): an RSRU is almost always situated in a box fixed along the road. An RSRU 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 RSRU 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 RSRU communicates with the OBRU in the vehicle over 802.11 wireless link operating in OCB mode. An RSRU MAY be connected to the Internet, and MAY be an IP Router. When it is connected to the Internet, the term V2I (Vehicle to Internet) is relevant.

RSU (Road-Side Unit): an RSU operates in 802.11-OCB mode. A RSU broadcasts data to OBUs or exchanges data with OBUs in its communications zone. An RSU may provide channel assignments and operating instructions to OBUs in its communications zone, when required. The basic functional blocks of an RSU are: internal computer processing, permanent storage capability, an integrated GPS receiver for positioning and timing and an interface that supports both IPv4 and IPv6 connectivity, compliant with 802.3at. An OCB interface of an RSU MAY be IP-enabled simultaneously to being WAVE-enabled or GeoNetworking-enabled (MAY support simultaneously EtherTypes 0x86DD for IPv6 _and_ 0x88DC for WAVE and 0x8947 for GeoNetworking). The difference between RSU and RSRU is that an RSU is likely to have one single OCB interface which is likely not IP enabled, whereas an RSRU is likely to have one or more OCB interfaces which are almost always IP-enabled; moreover, an RSRU does IP forwarding, whereas an RSU does not.

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 dot11OCBActivated is true. The OCB mode requires transmission of QoS data frames (IEEE Std 802.11e), half-clocked operation (IEEE Std 802.11j), and use of 5.9 GHz frequency band. Nota: any implementation should comply with standards and regulations set in the different countries for using that frequency band.

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 RSRUs and/or OBRUs. 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 is 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). If IPv6 packets of size larger than 1500 bytes are sent on an 802.11-OCB interface card then the IP stack will fragment. In case there are IP fragments, the field "Sequence number" of the 802.11 Data header containing the IP fragment field is increased.

Non-IP packets such as WAVE Short Message Protocol (WSMP) can be delivered on 802.11-OCB links. Specifications of these packets are out of scope of this document, and do not impose any limit on the MTU size, allowing an arbitrary number of 'containers'. Non-IP packets such as ETSI GeoNetworking packets have an MTU of 1492 bytes. The operation of IPv6 over GeoNetworking is specified at [ETSI-IPv6-GeoNetworking].

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 is 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 is 0x86DD (hexadecimal 86DD, or otherwise #86DD).

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

1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 1

is the binary representation of the EtherType value 0x86DD.

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 Data 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.

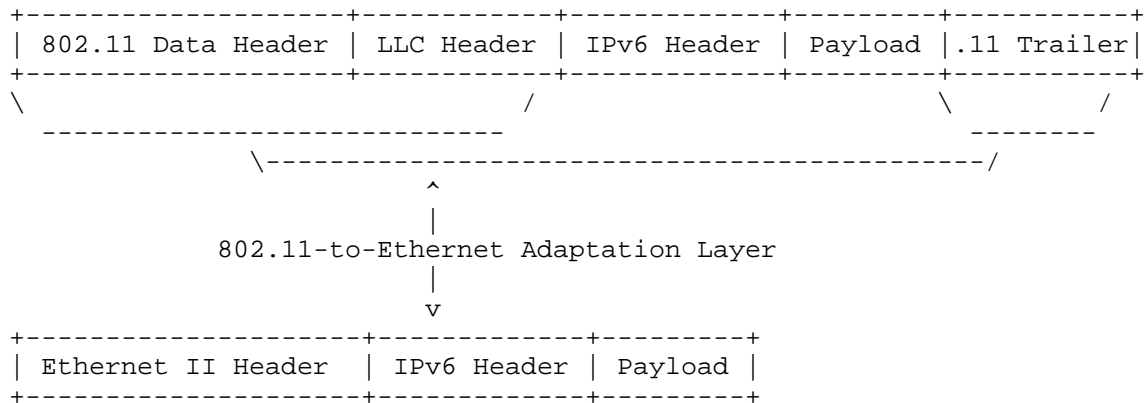


Figure 1: Operation of the Ethernet Adaptation Layer

The Receiver and Transmitter Address fields in the 802.11 Data Header 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 is 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.

Additionally, the Ethernet Adaptation Layer performs operations in relation to IP fragmentation and MTU. One of these operations is briefly described in Section 4.1.

In OCB mode, IPv6 packets MAY be transmitted either as "IEEE 802.11 Data" or alternatively as "IEEE 802.11 QoS Data", as illustrated in Figure 2.

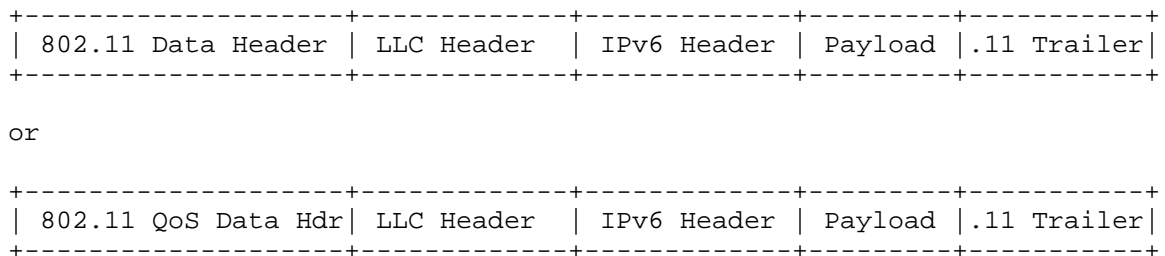


Figure 2: 802.11 Data Header or 802.11 QoS Data Header

The distinction between the two formats is given by the value of the field "Type/Subtype". The value of the field "Type/Subtype" in the 802.11 Data header is 0x0020. The value of the field "Type/Subtype" in the 802.11 QoS header is 0x0028.

The mapping between qos-related fields in the IPv6 header (e.g. "Traffic Class", "Flow label") and fields in the "802.11 QoS Data Header" (e.g. "QoS Control") are not specified in this document. Guidance for a potential mapping is provided in [I-D.ietf-tsvwg-ieee-802-11], although it is not specific to OCB mode.

The placement of IPv6 networking layer on Ethernet Adaptation Layer is illustrated in Figure 3.

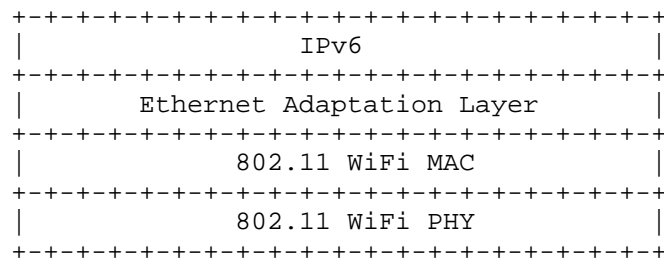


Figure 3: Ethernet Adaptation Layer stacked with other layers

(in the above figure, a WiFi profile is represented; this is used also for 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

For unicast as for multicast, there is no change from the unicast and multicast address mapping format of Ethernet interfaces, as defined by 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 OBRU 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].

An addressing model involves several types of addresses, like Globally-unique Addresses (GUA), Link-Local Addresses (LL) and Unique Local Addresses (ULA). The subnet structure in 'ad-hoc' networks may have characteristics that lead to difficulty of using GUAs derived from a received prefix, but the LL addresses may be easier to use since the prefix is constant.

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 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-IPv6-GeoNetworking]
"ETSI EN 302 636-6-1 v1.2.1 (2014-05), ETSI, European Standard, Intelligent Transportation Systems (ITS); Vehicular Communications; Geonetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over Geonetworking Protocols. Downloaded on September 9th, 2017, freely available from ETSI website at URL http://www.etsi.org/deliver/etsi_en/302600_302699/30263601/01.02.01_60/en_30263601v010201p.pdf".
- [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.ietf-tsvwg-ieee-802-11]

Szigeti, T., Henry, J., and F. Baker, "Diffserv to IEEE 802.11 Mapping", draft-ietf-tsvwg-ieee-802-11-09 (work in progress), September 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-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".
- o Checked the entire document for a consistent use of terms OBU and OBRU.
- o Added note saying that "'p' is a letter identifying the Amendment".
- o Substituted lower case for capitals SHALL or MUST in the Appendices.
- o 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.
- o Added figure captions, figure numbers, and references to figure numbers instead of 'below'. Replaced "section Section" with "section" throughout.
- o Minor typographical errors.

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

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

- o Moved the EPD description to an Appendix on its own.
- o Shortened the Introduction and the Abstract.
- o Moved the tutorial section of OCB mode introduced to .11, into an appendix.
- o Removed the statement that suggests that for routing purposes a prefix exchange mechanism could be needed.
- o 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.
- o Updated a reference from individual submission to now a WG item in IPWAVE: the survey document.
- o Added term definition for WiFi.
- o Updated the authorship and expanded the Contributors section.
- o Corrected typographical errors.

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

- o Removed the per-channel IPv6 prohibition text.
- o Corrected typographical errors.

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

- o Added new terms: OBRU and RSRU ('R' for Router). Refined the existing terms RSU and OBU, which are no longer used throughout the document.
- o Improved definition of term "802.11-OCB".
- o Clarified that OCB does not "strip" security, but that the operation in OCB mode is "stripped off of all .11 security".
- o Clarified that theoretical OCB bandwidth speed is 54mbits, but that a commonly observed bandwidth in IP-over-OCB is 12mbit/s.
- o Corrected typographical errors, and improved some phrasing.

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

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

- o Lengthened the title and cleaned the abstract.
- o Added text suggesting LLs may be easy to use on OCB, rather than GUAs based on received prefix.
- o Added the risks of spoofing and hijacking.
- o Removed the text speculation on adoption of the TSA message.
- o Clarified that the ND protocol is used.
- o 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-80211locb-03 to draft-ietf-ipwave-ipv6-over-80211locb-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-80211locb-02 to draft-ietf-ipwave-ipv6-over-80211locb-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 occurrences 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 (OBRU and RSRU) receive all the messages transmitted (OBRU and RSRU) within the radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

The message exchange diagram in Figure 4 illustrates a comparison between traditional 802.11 and 802.11 in OCBmode. 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.

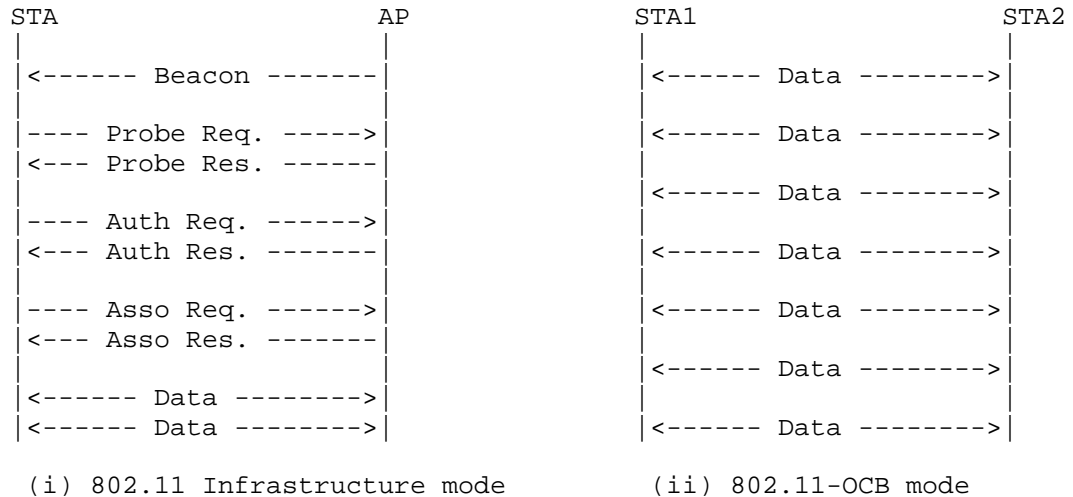


Figure 4: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

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 WiFi and Ethernet layers do (802.11a/b/g/n and 802.3). A packet sent by an OBRU may be received by one or multiple RSRUs. 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 0xfffffffffff (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).

- o '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.
- o 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:

- o 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.
- o The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.
- o The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).

- o 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 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 5. 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).

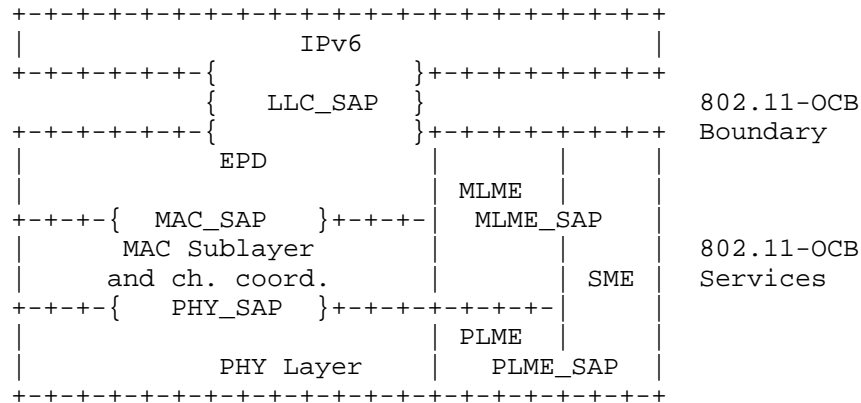


Figure 5: EtherType Protocol Discrimination

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, implicitly 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 mechanism 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

When designing the IPv6 over 802.11-OCB address mapping, we assume that the MAC Addresses change during well defined "renumbering events". The 48 bits randomized MAC addresses will have the following characteristics:

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

The way to meet the randomization requirements is to retain 46 bits from the output of a strong hash function, such as SHA256, taking as 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:

- o 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 6, 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.

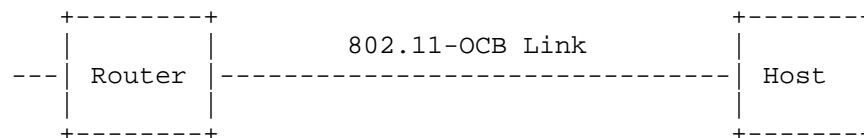


Figure 6: Topology for capturing IP packets on 802.11-OCB

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.

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
Internet-Draft
Intended status: Standards Track
Expires: February 10, 2020

N. Benamar
Moulay Ismail University of Meknes
J. Haerri
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.

Status of This Memo

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

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

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

This Internet-Draft will expire on February 10, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	3
2. Terminology	3
3. Communication Scenarios where IEEE 802.11-OCB Links are Used	4
4. IPv6 over 802.11-OCB	4
4.1. Maximum Transmission Unit (MTU)	4
4.2. Frame Format	5
4.3. Link-Local Addresses	5
4.4. Stateless Autoconfiguration	5
4.5. Address Mapping	6
4.5.1. Address Mapping -- Unicast	6
4.5.2. Address Mapping -- Multicast	6
4.6. Subnet Structure	7
5. Security Considerations	8
5.1. Privacy Considerations	8
5.1.1. Privacy Risks of Meaningful info in Interface IDs . .	9
5.2. MAC Address and Interface ID Generation	9
5.3. Pseudonymization impact on confidentiality and trust . .	10
6. IANA Considerations	10
7. Contributors	10
8. Acknowledgements	11
9. References	12
9.1. Normative References	12
9.2. Informative References	14
Appendix A. 802.11p	16
Appendix B. Aspects introduced by the OCB mode to 802.11	16
Appendix C. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver	20
Appendix D. Protocol Layering	21
Appendix E. Design Considerations	22
Appendix F. IEEE 802.11 Messages Transmitted in OCB mode	22
Appendix G. Examples of Packet Formats	23
G.1. Capture in Monitor Mode	24
G.2. Capture in Normal Mode	26
Appendix H. Extra Terminology	28
Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links	29

Authors' Addresses	31
--------------------	----

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:

- o 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].
- o 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 dot11OCBActivated 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, similarly 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 wish 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 subnet 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:

- o Bit "Local/Global" set to "locally administered".
- o Bit "Unicast/Multicast" set to "Unicast".
- o 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 STAion 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 OCBmode. 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.

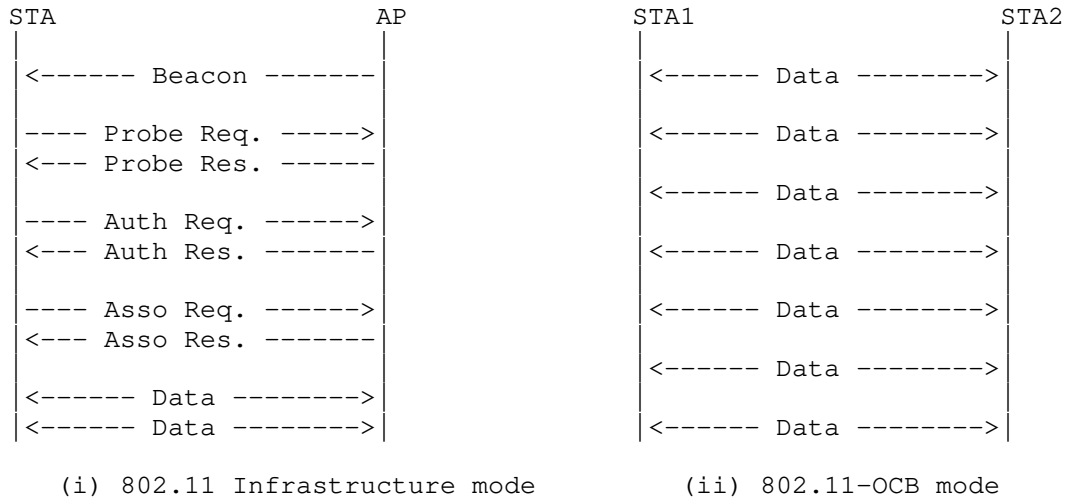


Figure 1: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

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-OBUS 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 0xfffffffffff (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).

- o '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.
- o 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:

- o 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.
- o The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.
- o The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).
- o 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).

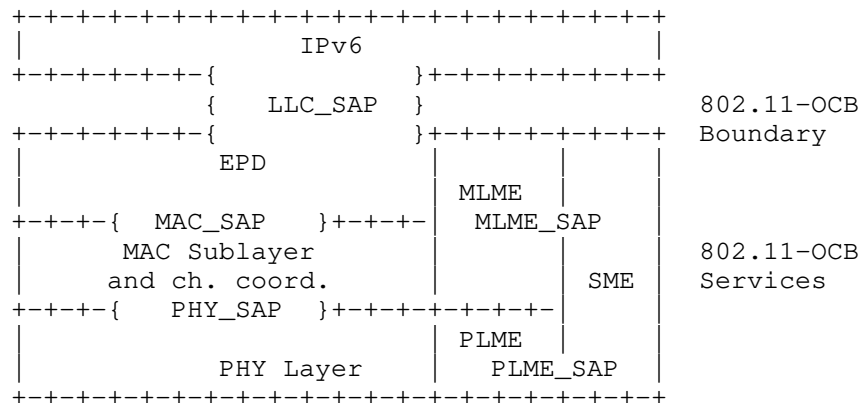


Figure 2: EtherType Protocol Discrimination

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:

- o 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 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).

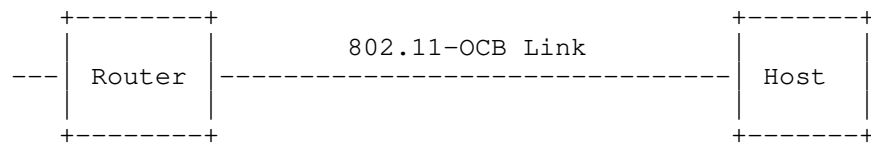


Figure 3: Topology for capturing IP packets on 802.11-OCB

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 |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

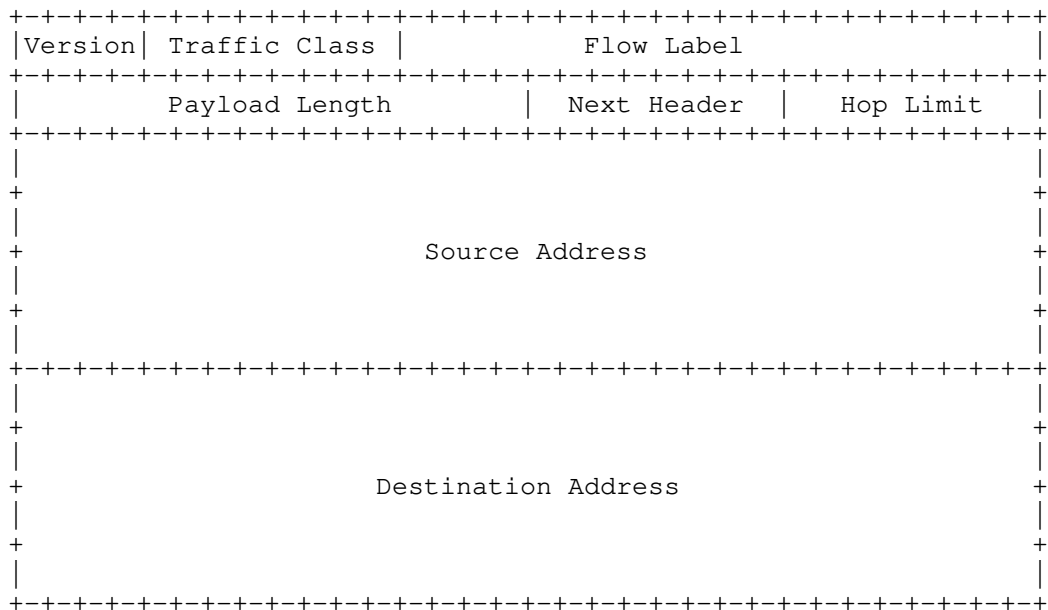
Logical-Link Control Header

```

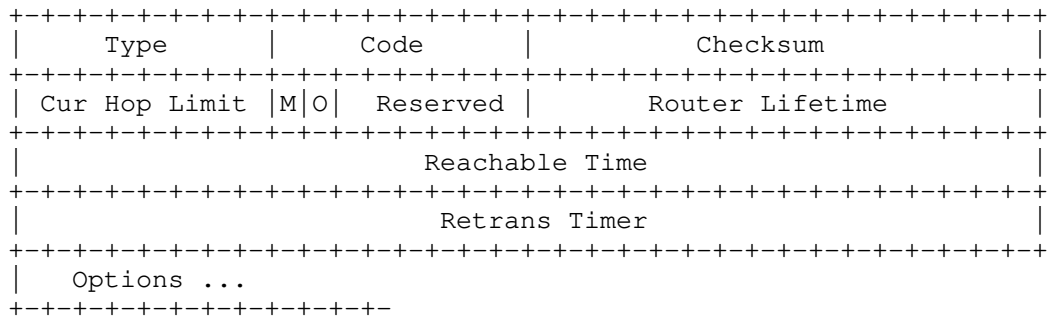
+-----+-----+-----+-----+-----+-----+-----+-----+
| DSAP | I | SSAP | C | Control field | Org. code...
+-----+-----+-----+-----+-----+-----+-----+-----+
... Organizational Code | Type |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

IPv6 Base Header



Router Advertisement



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 DSRC 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 respective 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
Internet-Draft
Intended status: Informational
Expires: May 3, 2018

J. Jeong, Ed.
Sungkyunkwan University
October 30, 2017

IP-based Vehicular Networking: Use Cases, Survey and Problem Statement
draft-ietf-ipwave-vehicular-networking-00

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

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on May 3, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	5
2. Terminology	5
3. Use Cases	6
3.1. V2V Use Cases	6
3.2. V2I Use Cases	7
4. Vehicular Network Architectures	8
4.1. Existing Architectures	8
4.1.1. VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks	8
4.1.2. IPv6 Operation for WAVE - Wireless Access in Vehicular Environments	9
4.1.3. A Framework for IP and non-IP Multicast Services for Vehicular Networks	10
4.1.4. Joint IP Networking and Radio Architecture for Vehicular Networks	10
4.1.5. Mobile Internet Access in FleetNet	11
4.1.6. A Layered Architecture for Vehicular Delay-Tolerant Networks	12
4.2. Problem Statement	13
4.2.1. V2I-based Internetworking	14
4.2.2. V2V-based Internetworking	17
5. Standardization Activities	17
5.1. IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture	17
5.2. IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services	18
5.3. ETSI Intelligent Transport Systems: Transmission of IPv6 Packets over GeoNetworking Protocols	19
5.4. ISO Intelligent Transport Systems: Communications	

Access for Land Mobiles (CALM) Using IPv6 Networking . . .	19
6. IP Address Autoconfiguration	20
6.1. Existing Protocols	20
6.1.1. Automatic IP Address Configuration in VANETs	20
6.1.2. Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network	21
6.1.3. GeoSAC: Scalable Address Autoconfiguration for VANET Using Geographic Networking Concepts	21
6.1.4. Cross-layer Identities Management in ITS Stations	22
6.2. Problem Statement	23
6.2.1. Neighbor Discovery	23
6.2.2. IP Address Autoconfiguration	23
7. Routing	25
7.1. Existing Protocols	25
7.1.1. Experimental Evaluation for IPv6 over VANET Geographic Routing	25
7.1.2. Location-Aided Gateway Advertisement and Discovery Protocol for VANets	25
7.2. Problem Statement	26
8. Mobility Management	26
8.1. Existing Protocols	26
8.1.1. An IP Passing Protocol for Vehicular Ad Hoc Networks with Network Fragmentation	26
8.1.2. A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users	27
8.1.3. A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility	28
8.1.4. NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios	29
8.1.5. Network Mobility Protocol for Vehicular Ad Hoc Networks	30
8.1.6. Performance Analysis of PMIPv6-Based Network Mobility for Intelligent Transportation Systems	30
8.1.7. A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks and Fixed IP Networks	31
8.1.8. SDN-based Distributed Mobility Management for 5G Networks	31
8.1.9. IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions	32
8.2. Problem Statement	34
9. DNS Naming Service	34
9.1. Existing Protocols	34
9.1.1. Multicast DNS	34
9.1.2. DNS Name Autoconfiguration for Internet-of-Things Devices	34
9.2. Problem Statement	35
10. Service Discovery	36
10.1. Existing Protocols	36

10.1.1. mDNS-based Service Discovery	36
10.1.2. ND-based Service Discovery	36
10.2. Problem Statement	36
11. Security and Privacy	37
11.1. Existing Protocols	37
11.1.1. Securing Vehicular IPv6 Communications	37
11.1.2. Providing Authentication and Access Control in Vehicular Network Environment	38
11.2. Problem Statement	39
12. Discussions	39
12.1. Summary and Analysis	39
12.2. Deployment Issues	40
13. Security Considerations	41
14. Informative References	41
Appendix A. Acknowledgments	48
Appendix B. Contributors	48

1. Introduction

Nowadays vehicular networks have been focused on the driving safety, driving efficiency, and entertainment in road networks. Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (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 the driving safety service 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 finalized 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 statement on IP-based vehicular networking for Intelligent Transportation Systems (ITS). First, This document surveys the use cases 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 defines the following new terms:

- o Road-Side Unit (RSU): A node that has Dedicated Short-Range Communications (DSRC) device for wireless communications 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.
- 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. Exemplary functions of TCC include the management of evacuation routes, the monitoring of pedestrians and bike traffic, the monitoring of real-time transit operations, and real-time responsive traffic signal systems. Thus, TCC is the nerve center of most freeway management systems 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.

3. Use Cases

This section shows use cases of V2V and V2I networking.

3.1. V2V 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 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 efficient detour paths to vehicles around the accidents spots.

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, but DSRC-based vehicular networks can be used in near future.

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. V2I Use Cases

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

Context-Aware 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 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, 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-Cruise-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: On the Feasibility of IP Communications 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 does not support Duplicate Address Detection (DAD), seamless communications for Internet services, and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU). 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 - Wireless Access in Vehicular Environments

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 works under certain assumptions for the link model that do not necessarily hold in WAVE. For instance, IPv6 assumes 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 pseudonymity through MAC address change along with the suitability of traditional TCP applications are discussed by the authors since they require the design of appropriate solutions.

4.1.3. A Framework for IP and non-IP Multicast Services 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, 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 in 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, this study lacks simulations related to performance assessment.

4.1.4. Joint IP Networking and Radio Architecture for Vehicular Networks

Petrescu et al. defined the joined 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.

Considering a toy 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 this paper is to join the IP-layer relaying with radio-link channels. This paper suggests to separate 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 statement is similar to multi-channel topology management proposals in multi-hop sensor networks, yet adapted to an IP topology.

In conclusion, this paper proposes to classify an IP multi-hop vehicular network in three classes of vehicles: Leaf Vehicle (LV), Range Extending Vehicle (REV), and Internet Vehicle (IV). It suggests 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 paper is most probably one of the first paper 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 IP4/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 cranked-up 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/IGW 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 Delay-Tolerant Networks

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 the DTN architectures evolved since the paper has been written, this paper addresses IP mobility management from a different approach. 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. 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 problems focus on the network layer (i.e., IPv6 protocol stack) rather than the MAC layer and the transport layer (e.g., TCP, UDP, and SCTP).

Figure 1 shows a vehicular network 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.

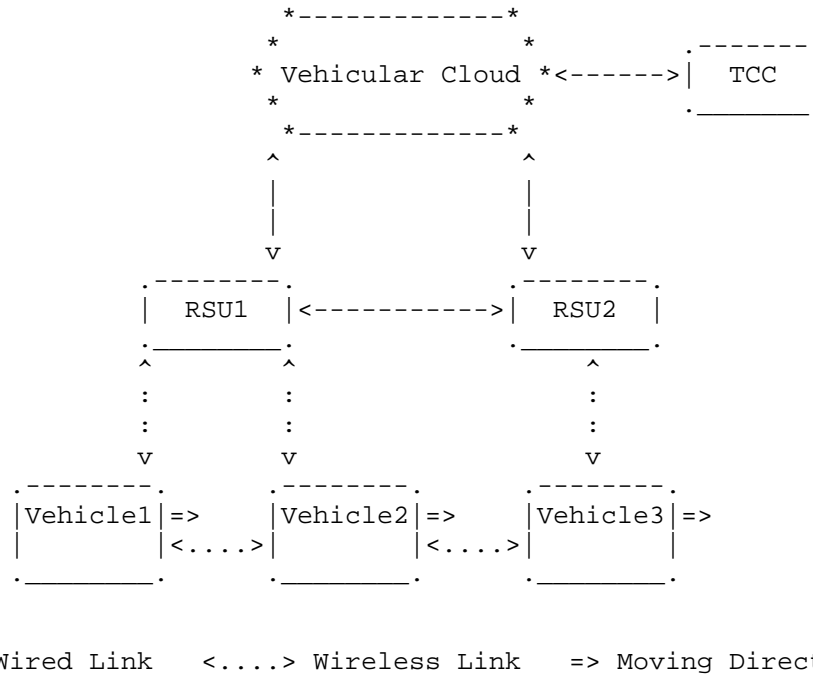


Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

In vehicular networks, unidirectional links exist and must be considered. Control Plane must be separated from Data Plane. ID/Pseudonym change requires a lightweight DAD. IP tunneling should be avoided. Vehicles do not have a Home Network. Protocol-based mobility must be kept hidden to both the vehicle and the correspondent node (CN). A vehicular network architecture may be composed of three types of vehicles: 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 internal networks having multiple subnets and having an edge router for the communication with another vehicle or RSU. The method of prefix assignment for each subnet inside the vehicle's mobile network and the RSU's fixed network is out of scope for this document. The internetworking between two internal networks via either V2I or V2V communication requires an exchange of network prefix and other parameters.

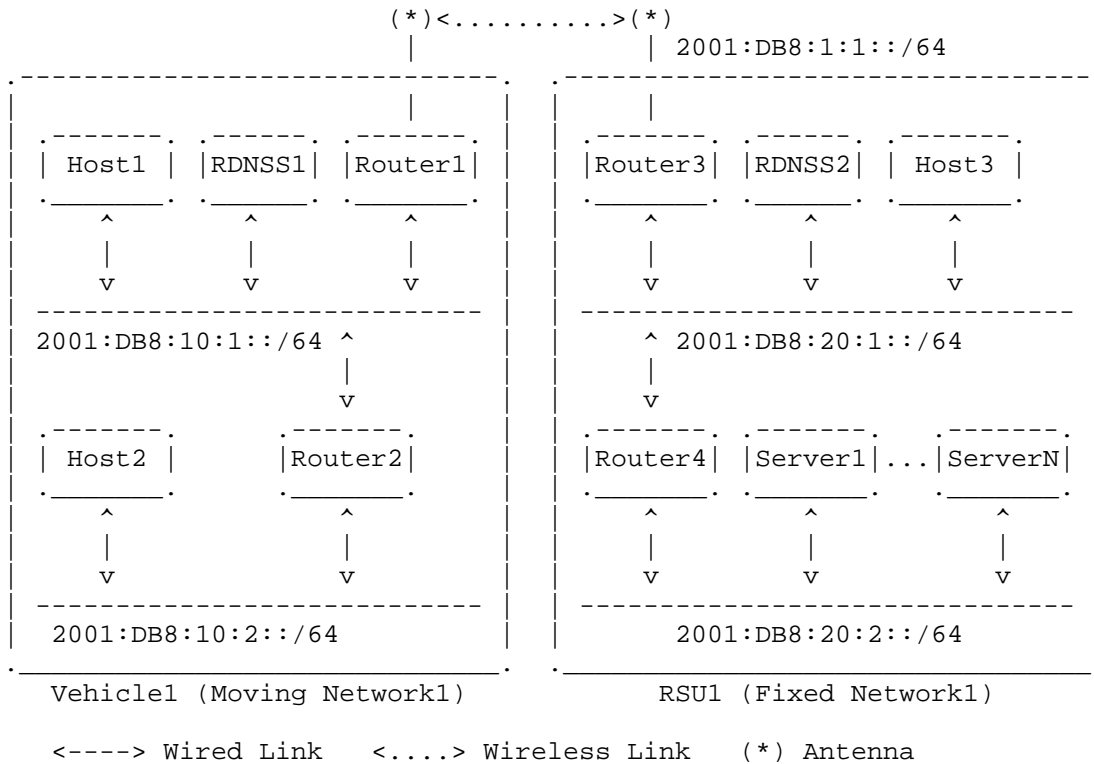


Figure 2: Internetworking between Vehicle Network and RSU Network

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

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

Figure 2 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 service.

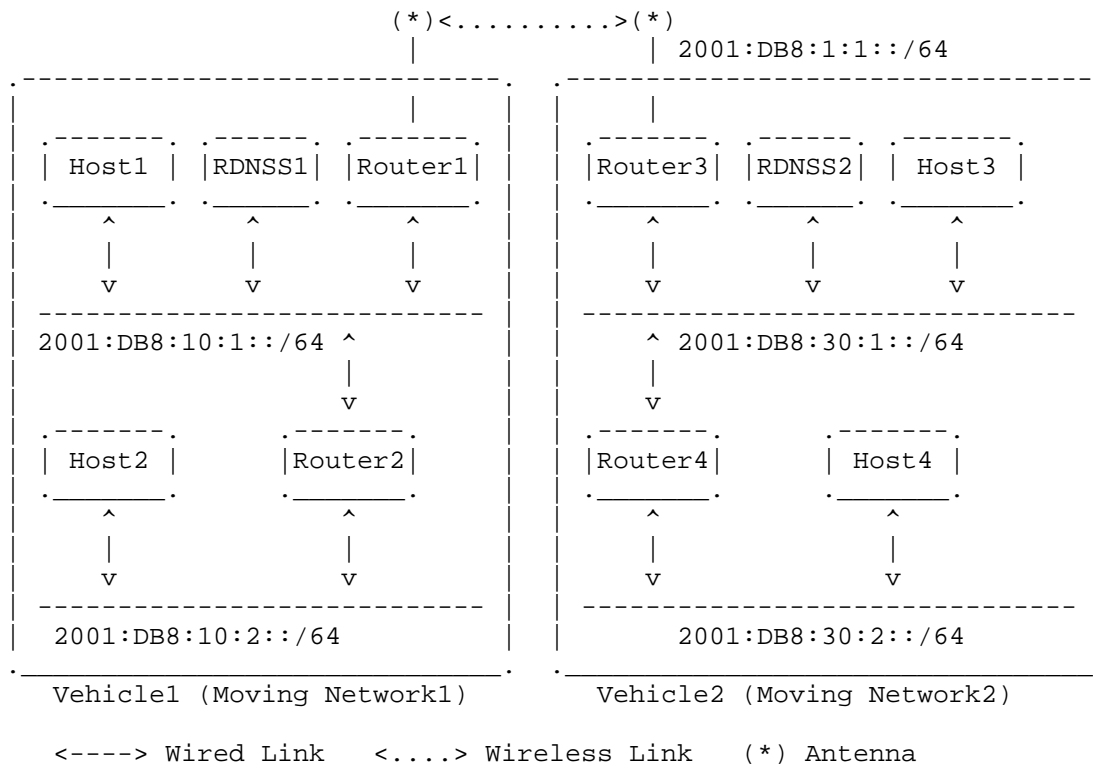


Figure 3: Internetworking between Two Vehicle Networks

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 service.

5. Standardization Activities

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

5.1. IEEE Guide for Wireless Access in Vehicular Environments (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 Wireless Access in Vehicular Environments (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 an IPv6 Router Advertisement message, which are based on ICMPv6.

5.3. ETSI Intelligent Transport Systems: Transmission of IPv6 Packets over GeoNetworking Protocols

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 Stateless Address Autoconfiguration (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: Communications Access for Land Mobiles (CALM) Using IPv6 Networking

ISO published a standard specifying the IPv6 network protocols and services [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 the addressing 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

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 with the 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 the concept of SCOPE as a delimited geographic area where IP addresses are guaranteed to be unique. When it is allocated an IP address from a leader-vehicle with a scope, a vehicle 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. Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network

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 much overhead in the case where vehicles change their lanes frequently in highway.

6.1.3. GeoSAC: Scalable Address Autoconfiguration for VANET Using Geographic Networking Concepts

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.

This paper identifies four 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 (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 simultaneously. 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. This dynamically changing IPv6 address can prevent the ITS station from being tracked by a hacker. However, this address renewal cannot be applied at any time because in some situations, the continuity of the knowledge about the surrounding vehicles is required.

Also, this 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 and 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

This section discusses IP addressing for the V2I and V2V networking. There are two approaches for IPv6 addressing in vehicular networks. The first is to use unique local IPv6 unicast addresses (ULAs) for vehicular networks [RFC4193]. The other is to use global IPv6 addresses for the interoperability with the Internet [RFC4291]. The former approach is often used by Mobile Ad Hoc Networks (MANET) for an isolated subnet. This approach can support the emergency notification service and navigation service in road networks. However, for general Internet services (e.g., email access, web surfing and entertainment services), the latter approach is required.

For global IP addresses, there are two choices: a multi-link subnet approach for multiple RSUs and a single subnet approach per RSU. In the multi-link subnet approach, which is similar to ULA for MANET, RSUs play a role of layer-2 (L2) switches and the router interconnected with the RSUs is required. The router maintains the location of each vehicle belonging to an RSU for L2 switching. In the single subnet approach per RSU, which is similar to the legacy subnet in the Internet, each RSU plays the role of a (layer-3) router.

6.2.1. Neighbor Discovery

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

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

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 crosses the communication coverages of multiple RSUs. Some modifications are required for both stateless address autoconfiguration and DHCPv6. Mobile IPv6 (MIPv6) can be used for the fast update of a vehicle's care-of address for the current RSU to communicate with the vehicle [RFC6275].

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 should 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 Protocols

7.1.1. Experimental Evaluation for IPv6 over VANET Geographic Routing

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 C2C-CC architecture, C2CNet layer is located between IPv6 and link layers. Thus, an IPv6 packet is delivered with 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 these 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 this protocol, 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 Protocol for VANets

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 considers location and velocity of a vehicle.

A gateway sends advertisement (GAdv) messages periodically to one-hop 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. Then, 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 packets 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. Problem Statement

IP address autoconfiguration should be manipulated to support the efficient networking. Due to network fragmentation, vehicles 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 work probably when the density of vehicle in a road network is not sparse. A sparse vehicular network challenges the gateway discovery since the 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. An IP Passing Protocol for 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. A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users

Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support highly mobile vehicles [H-DMM]. The legacy DMM is not suitable for high-speed scenarios because it requires additional registration delay proportional to the distance

between a vehicle and its anchor network. H-DMM is designed to satisfy a set of requirements, such as service disruption time, end-to-end delay, packet delivery cost, and tunneling cost.

H-DMM adopts 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 take a delay. 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.

8.1.1.3. A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility

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. In particular cases, such as the signaling cost, H-NEMO is 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 for Internet Access in Automotive Scenarios

In [NEMO-LMS], authors proposed an architecture to enable IP mobility for moving networks in a network-based mobility scheme based on PMIPv6. In PMIPv6, only mobile terminals are provided with IP mobility. Different 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 with the standardized signaling of PMIPv6. 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 mMAGr. 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 Protocol 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 entitled to assist the vehicle to perform a pre-handoff.

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 PMIPv6-Based Network MObility for Intelligent Transportation Systems

Lee et al. proposed P-NEMO, which is an 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 the 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, so that 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 only evaluated through an analytical model that is compared 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. A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks 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 Distributed 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 (MF) through the network instead of concentrating them in one bottleneck MF, or in a hierarchically organized backbone of MF. Highly mobile vehicular networks impose frequent IP route optimizations that lead to suboptimal routes (detours) between CN and vehicles. The suboptimality critically increases by 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 et 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 recently appeared and gained a big 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.

This paper makes several observations leading to a strong suggestions that IP mobility management should be based on an SDN architecture. First, SDN will be integrated into future Internet and 5G in a 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 Management for Vehicular Communication Networks: 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, the detour taken to pass by the MR's HA even if the CN is nearby, or the

route optimization 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 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

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 components 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 Internet-of-Things 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. Providing Authentication and Access Control in Vehicular Network Environment

Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks [VNET-AAA]. This security 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

- [RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.
- [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5949] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., and F. Xia, "Fast Handovers for Proxy Mobile IPv6", RFC 5949, September 2010.
- [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.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
- [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

- [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.
- [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.
- [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.
- [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.
- [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.
- [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.
- [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.
- [IPv6-WAVE] Baccelli, E., Clausen, T., and R. Wakikawa, "IPv6 Operation for WAVE - Wireless Access in Vehicular Environments", IEEE Vehicular Networking Conference, December 2010.
- [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.
- [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.
- [FleetNet] Bechler, M., Franz, W., and L. Wolf, "Mobile Internet Access in FleetNet", 13th Fachtagung Kommunikation in verteilten Systemen, February 2001.
- [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.
- [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.
- [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.
- [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.

- [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.
- [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. Chilamkurthi, "Performance Analysis of PMIPv6-Based Network MObility for Intelligent Transportation Systems", IEEE Transactions on Vehicular Technology, January 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.
- [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.
- [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.

- [Securing-VCOMM] Fernandez, P., Santa, J., Bernal, F., and A. Skarmeta, "Securing Vehicular IPv6 Communications", IEEE Transactions on Dependable and Secure Computing, January 2016.
- [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.
- [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.
- [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.
- [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.
- [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.
- [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.
- [ISO-ITS-IPv6] ISO/TC 204, "Intelligent Transport Systems - Communications Access for Land Mobiles (CALM) - IPv6 Networking", ISO 21210:2012, June 2012.
- [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.
- [FirstNet] U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", [Online] Available: <https://www.firstnet.gov/>, 2012.
- [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.
- [CA-Cruise-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.
- [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.
- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", RFC 4086, June 2005.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.
- [RFC1034] Mockapetris, P., "Domain Names - Concepts and Facilities", RFC 1034, November 1987.
- [RFC1035] Mockapetris, P., "Domain Names - Implementation and Specification", RFC 1035, November 1987.
- [ID-DNSNA] Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-01 (work in progress), October 2017.
- [ID-Vehicular-ND] Jeong, J., Ed., Shen, Y., Jo, Y., Jeong, J., and J. Lee, "IPv6 Neighbor Discovery for Prefix and Service Discovery in Vehicular Networks", draft-jeong-ipwave-vehicular-neighbor-discovery-01 (work in progress), October 2017.
- [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.

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

Appendix A. 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 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 Lozano (Universidad of Murcia), Richard Roy (MIT), and Francois Simon (Pilot). The authors sincerely appreciate their contributions.

The following are contributing authors of this document as co-authors:

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.ldap@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

Alex 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 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: 1 October 2022

J. Jeong, Ed.
Sungkyunkwan University
30 March 2022

IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem
Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-28

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 enumerates requirements for the extensions of those IPv6 protocols for IPv6-based vehicular networking.

Status of This Memo

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

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

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

This Internet-Draft will expire on 1 October 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Terminology	4
3. Use Cases	7
3.1. V2V	8
3.2. V2I	10
3.3. V2X	12
4. Vehicular Networks	13
4.1. Vehicular Network Architecture	14
4.2. V2I-based Internetworking	16
4.3. V2V-based Internetworking	19
5. Problem Statement	22
5.1. Neighbor Discovery	23
5.1.1. Link Model	25
5.1.2. MAC Address Pseudonym	27
5.1.3. Routing	27
5.2. Mobility Management	29
6. Security Considerations	31
6.1. Security Threats in Neighbor Discovery	32
6.2. Security Threats in Mobility Management	33
6.3. Other Threats	33
7. IANA Considerations	35
8. References	35
8.1. Normative References	35
8.2. Informative References	40
Appendix A. Support of Multiple Radio Technologies for V2V	46
Appendix B. Support of Multihop V2X Networking	46
Appendix C. Support of Mobility Management for V2I	48
Appendix D. Support of MTU Diversity for IP-based Vehicular Networks	49
Appendix E. Acknowledgments	50
Appendix F. Contributors	51
Author's Address	52

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]. Most countries and regions in the world have adopted the same frequency allocation for vehicular networks.

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], Network Mobility (NEMO) [RFC3963], Locator/ID Separation Protocol (LISP) [I-D.ietf-lisp-rfc6830bis], and Automatic Extended Route Optimization based on the Overlay Multilink Network Interface (AERO/OMNI) [I-D.templin-6man-aero] [I-D.templin-6man-omni]). 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 enumerates 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, motorcycle, and a similar one). 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]. It can play a role of a router connecting multiple computers (or in-vehicle devices) inside a vehicle. 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 the third IP-enabled wireless interface running in 3GPP C-V2X in addition to the IP-RSU defined in [RFC8691]. 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 dot11OCBActivated 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 tablet 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.
- * Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network forwarding elements (e.g., switch and router).
- * V2D: "Vehicle to Device". It is the wireless communication between a vehicle and a device (e.g., smartphone and IoT device).
- * 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).
- * 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).

- * 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).
- * 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.
- * VIP: "Vehicular Internet Protocol". It is an IPv6 extension for vehicular networks including V2V, V2I, and V2X.
- * VMM: "Vehicular Mobility Management". It is an IPv6-based mobility management for vehicular networks.
- * VND: "Vehicular Neighbor Discovery". It is an IPv6 ND extension for vehicular networks.
- * VSP: "Vehicular Security and Privacy". It is an IPv6-based security and privacy term for vehicular networks.
- * 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 augment 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.

3.1. V2V

The use cases of V2V networking discussed in this section include

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

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 [I-D.templin-ipwave-uam-its]. 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].

To support applications of these V2V use cases, the required functions of IPv6 include IPv6-based packet exchange and secure, safe communication between two vehicles. For the support of V2V under multiple radio technologies (e.g., DSRC and 5G V2X), refer to Appendix A.

3.2. V2I

The use cases of V2I networking discussed in this section include

- * Navigation service;
- * Energy-efficient speed recommendation service;
- * Accident notification service;
- * Electric vehicle (EV) charging service;
- * 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 equivalent project in Europe is called Public Safety Communications Europe (PSCE) [PSCE], which is developing a network for emergency communications.

An EV charging service with V2I can facilitate 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 or be notified that the charging station is out of service 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 plan 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.

In some scenarios such as vehicles moving in highways or staying in parking lots, a V2V2I network is necessary for vehicles to access the Internet since some vehicles may not be covered by an RSU. For those vehicles, a few relay vehicles can help to build the Internet access. For the nested NEMO described in [RFC4888], hosts inside a vehicle shown in Figure 3 for the case of V2V2I may have the same issue in the nested NEMO scenario.

To better support these use cases, the existing IPv6 protocol must be augmented either through protocol changes or by including a new adaptation layer in the architecture that efficiently maps IPv6 to a diversity of link layer technologies. Augmentation is necessary 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 as packet forwarders. Thus, IPv6 needs to be extended for multihop V2I communications.

To support applications of these V2I use cases, the required functions of IPv6 include IPv6 communication enablement with neighborhood discovery and IPv6 address management, reachability with adapted network models and routing methods, transport-layer session continuity, and secure, safe communication between a vehicle and an infrastructure node (e.g., IP-RSU) in the vehicular network.

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. Note that it is true that a pedestrian or a cyclist may have a higher risk of being hit by a vehicle if they are not with a smartphone in the current setting. For this case, other human sensing technologies (e.g., moving object detection in images and wireless signal-based human movement detection [LIFS] [DFC]) can be used to provide the motion information of them to vehicles. A vehicle by V2V2I networking can obtain the motion information of a vulnerable road user via an IP-RSU that either employs or connects to a human sensing technology.

The existing IPv6 protocol must be augmented through 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) as packet forwarders. Thus, IPv6 needs to be extended for multihop V2X or V2I2X communications.

To support applications of these V2X use cases, the required functions of IPv6 include 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 the context for vehicular networks supporting V2V, V2I, and V2X communications. 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.

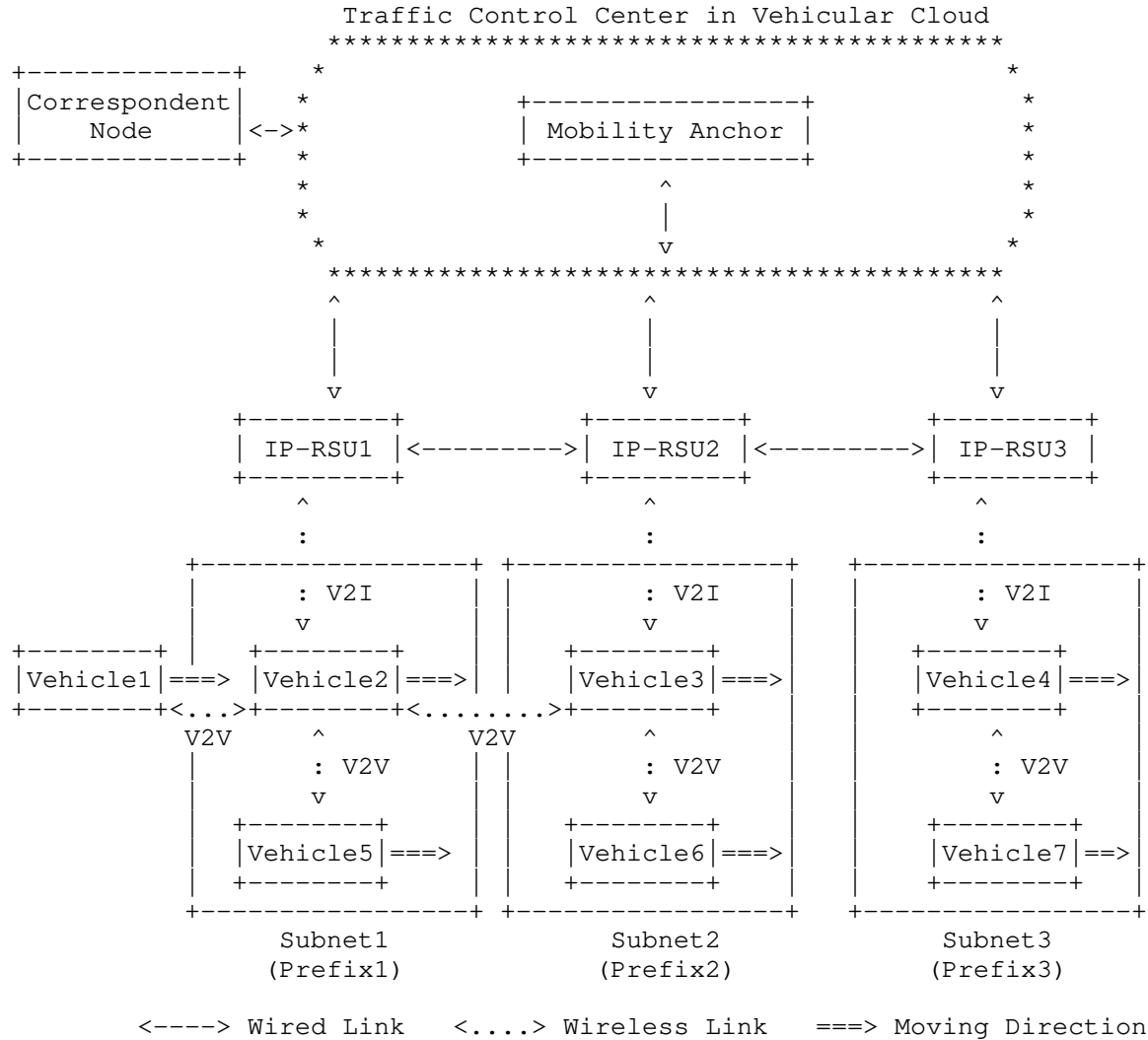


Figure 1: An Example Vehicular Network Architecture for V2I and V2V

4.1. Vehicular Network Architecture

Figure 1 shows an example vehicular network architecture for V2I and V2V in a road network. The vehicular network architecture contains vehicles (including IP-OBUs), IP-RSUs, Mobility Anchor, Traffic Control Center, and Vehicular Cloud as 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.

Existing network architectures, such as the network architectures of PMIPv6 [RFC5213], RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550], and AERO/OMNI [I-D.templin-6man-aero][I-D.templin-6man-omni], can be extended to a vehicular network architecture for multihop V2V, V2I, and V2X, as shown in Figure 1. Refer to Appendix B for the detailed discussion on multihop V2X networking by RPL and OMNI. Also, refer to Appendix A for the description of how OMNI is designed to support the use of multiple radio technologies in V2X.

As shown in this figure, IP-RSUs as routers and vehicles with IP-OBUs 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.

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 just as 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 a "Bring-Your-Own-Addresses (BYOA)" (or "Bring-Your-Own-Prefix (BYOP)") technique using their own IPv6 Unique Local Addresses (ULAs) [RFC4193] over the wireless network, which does not require the messaging (e.g., Duplicate Address Detection (DAD)) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862].

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.

As a basic definition 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 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 correspondent 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], NEMO [RFC3963][RFC4885] [RFC4888], and AERO [I-D.templin-6man-aero]). This document describes issues in mobility management for vehicular networks in Section 5.2.

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle's internal network (i.e., mobile 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. Note that it is dangerous if the internal network of a vehicle is controlled by a malicious party. To minimize this kind of risk, a reinforced identification and verification protocol shall be implemented.

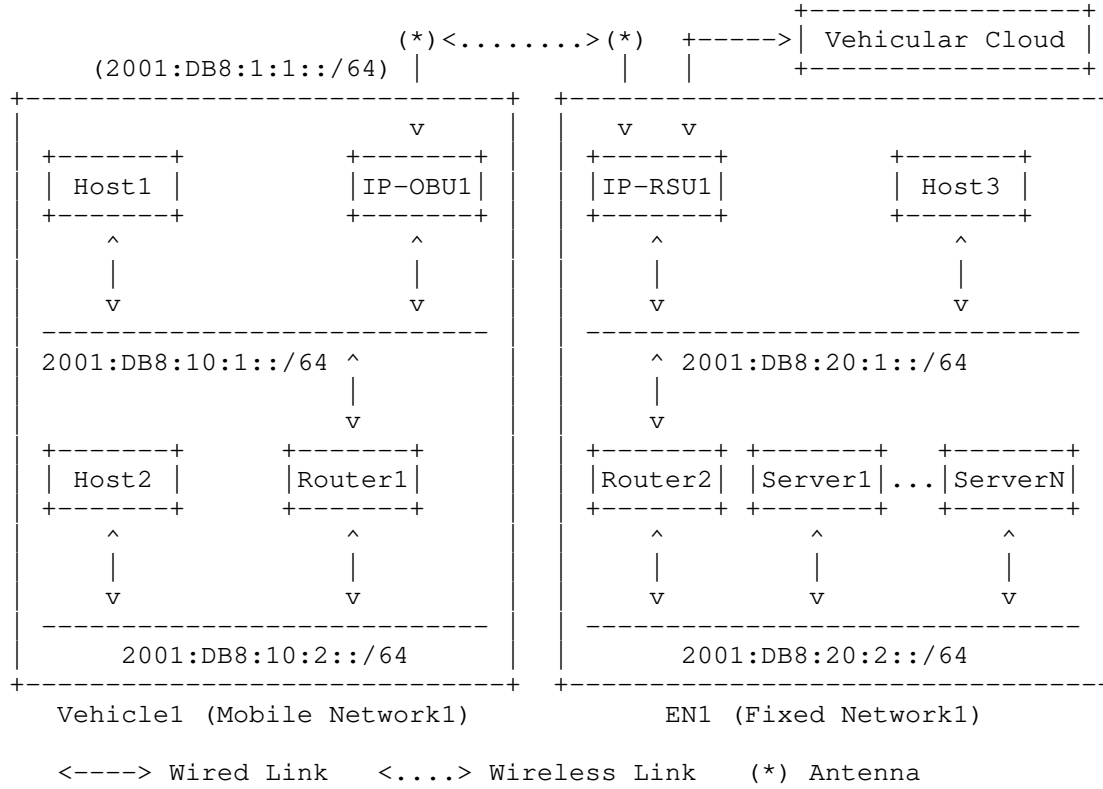


Figure 2: Internetworking between Vehicle and Edge Network

As shown in Figure 2, as internal networks, a vehicle's mobile 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 mobile network) in a vehicle need to be delegated and configured automatically. Note that a mobile network's network prefix can be called a Mobile Network Prefix (MNP) [RFC3963].

Figure 2 also shows the internetworking between the vehicle's mobile network and the EN's fixed network. There exists an internal network (Mobile 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 2, the addresses used for IPv6 transmissions over the wireless link interfaces for IP-OBU and IP-RSU can be link-local IPv6 addresses, ULAs, or global IPv6 addresses. When global IPv6 addresses are used, wireless interface configuration and control overhead for DAD [RFC4862] and Multicast Listener Discovery (MLD) [RFC2710][RFC3810] should be minimized to support V2I and V2X communications for vehicles moving fast along roadways.

Let us consider the upload/download time of a ground vehicle when it passes through the wireless communication coverage of an IP-RSU. For a given typical setting where 1km is the maximum DSRC communication range [DSRC] and 100km/h is the speed limit in highway for ground vehicles, the dwelling time can be calculated to be 72 seconds by dividing the diameter of the 2km (i.e., two times of DSRC communication range where an IP-RSU is located in the center of the circle of wireless communication) by the speed limit of 100km/h (i.e., about 28m/s). For the 72 seconds, a vehicle passing through the coverage of an IP-RSU can upload and download data packets to/from the IP-RSU. For special cases such as emergency vehicles moving above the speed limit, the dwelling time is relatively shorter than that of other vehicles. For cases of airborne vehicles, considering a higher flying speed and a higher altitude, the dwelling time can be much shorter.

4.3. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles via V2V communication.

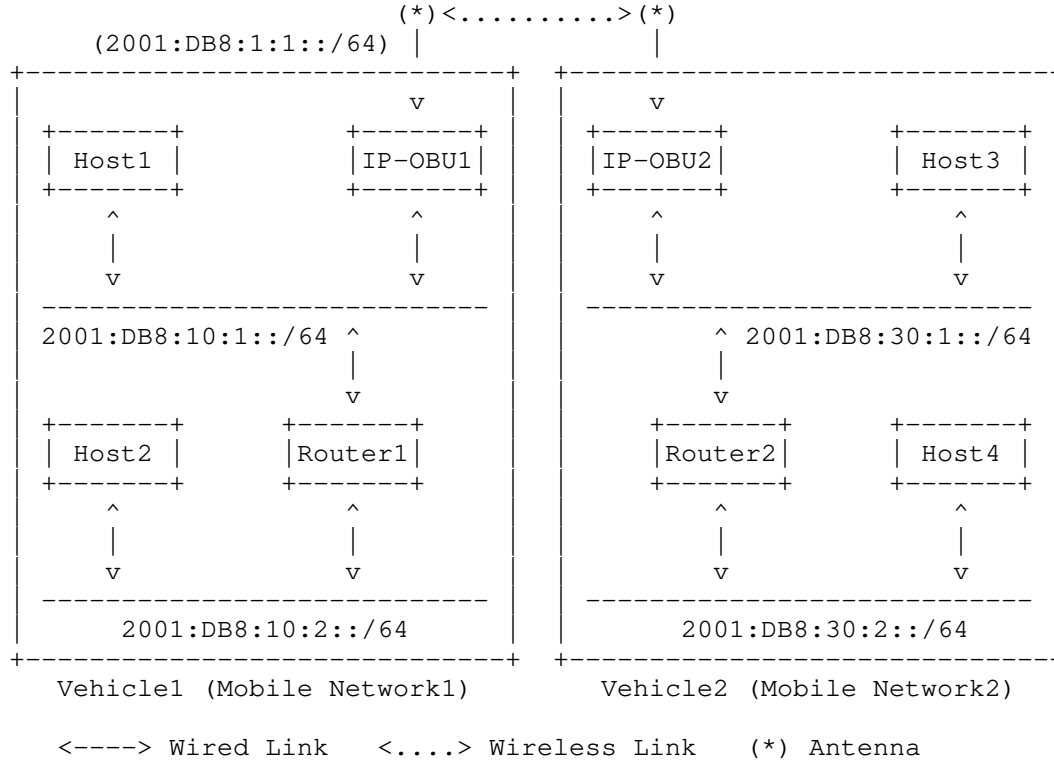


Figure 3: Internetworking between Two Vehicles

Figure 3 shows the internetworking between the mobile networks of two neighboring vehicles. There exists an internal network (Mobile Network1) inside Vehicle1. Vehicle1 has two hosts (Host1 and Host2), and two routers (IP-OBU1 and Router1). There exists another internal network (Mobile 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. Thus, a host (Host1) in Vehicle1 can communicate with another host (Host3) in Vehicle2 for a vehicular service through Vehicle1's mobile network, a wireless link between IP-OBU1 and IP-OBU2, and Vehicle2's mobile network.

As a V2V use case in Section 3.1, Figure 4 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.

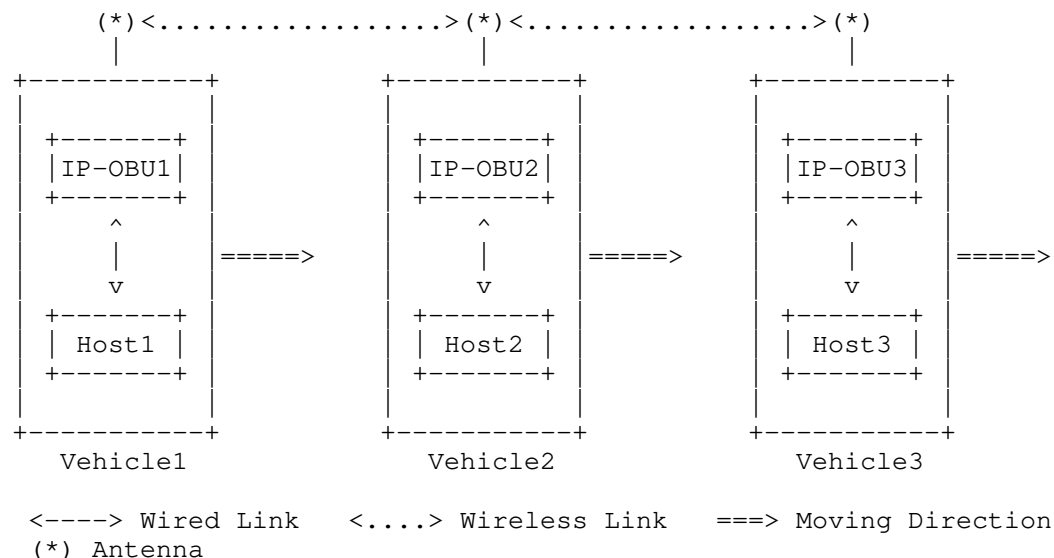


Figure 4: Multihop Internetworking between Two Vehicle Networks

As shown in Figure 4, multihop internetworking is feasible among the mobile 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 VANET, as shown in the figure.

In this section, the link between two vehicles is assumed to be stable for single-hop wireless communication regardless of the sight relationship such as line of sight and non-line of sight, as shown in Figure 3. Even in Figure 4, the three vehicles are connected to each other with a linear topology, however, multihop V2V communication can accommodate any network topology (i.e., an arbitrary graph) over VANET routing protocols.

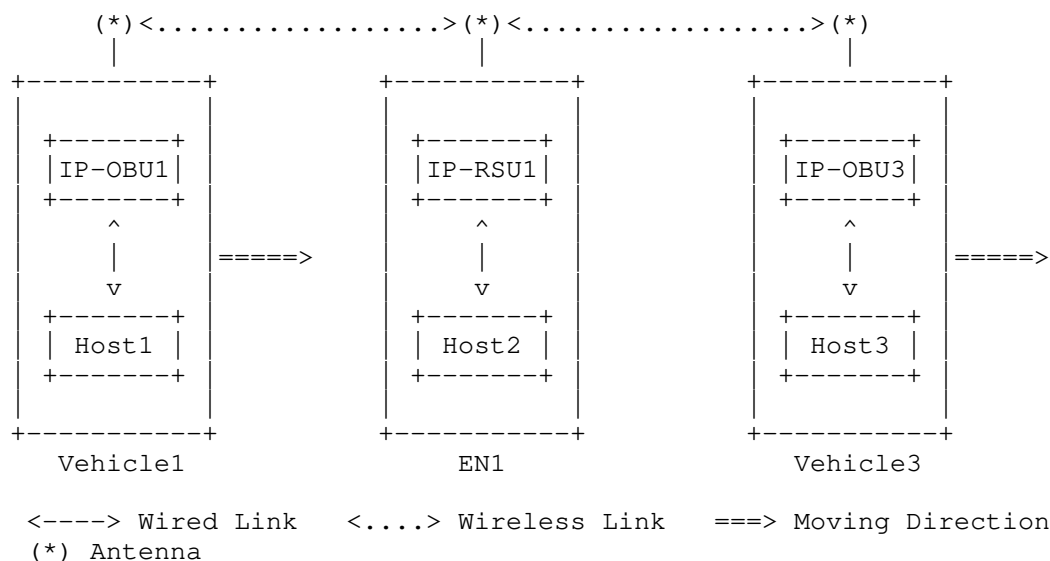


Figure 5: Multihop Internetworking between Two Vehicle Networks via IP-RSU (V2I2V)

As shown in Figure 5, multihop internetworking between two vehicles is feasible via an infrastructure node (i.e., IP-RSU) with wireless connectivity among the mobile networks of two vehicles and the fixed network of an edge network (denoted as EN1) in the same VANET. For example, Host1 in Vehicle1 can communicate with Host3 in Vehicle3 via IP-OBU1 in Vehicle1, IP-RSU1 in EN1, and IP-OBU3 in Vehicle3 in the VANET, as shown in the figure.

For the reliability required in V2V networking, the ND optimization defined in MANET [RFC6130] [RFC7466] improves the classical IPv6 ND in terms of tracking neighbor information with up to two hops and introducing several extensible Information Bases, which serves the MANET routing protocols such as the different versions of Optimized Link State Routing Protocol (OLSR) [RFC3626] [RFC7181], Open Shortest Path First (OSPF) derivatives (e.g., [RFC5614]), and Dynamic Link Exchange Protocol (DLEP) [RFC8175] with its extensions [RFC8629] [RFC8757]. In short, the MANET ND mainly deals with maintaining extended network neighbors to enhance the link reliability. However, an ND protocol in vehicular networks shall consider more about the geographical mobility information of vehicles as an important resource for serving various purposes to improve the reliability, e.g., vehicle driving safety, intelligent transportation implementations, and advanced mobility services. For a more reliable V2V networking, some redundancy mechanisms should be provided in L3 in cases of the failure of L2. For different use cases, the optimal

solution to improve V2V networking reliability may vary. For example, a group of vehicles in platooning may have stabler neighbors than freely moving vehicles, as described in Section 3.1.

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 relatively short time compared to the lifetime of a link between a vehicle and an IP-RSU, or between two vehicles.

For safe driving, vehicles need to exchange application messages every 0.5 second [NHTSA-ACAS-Report] to let drivers take an action to avoid a dangerous situation (e.g., vehicle collision), so IPv6 protocol exchanges need to support this order of magnitude for application message exchanges. Also, considering the communication range of DSRC (up to 1km) and 100km/h as the speed limit in highway, the lifetime of a link between a vehicle and an IP-RSU is in the order of a minute (e.g., about 72 seconds), and the lifetime of a link between two vehicles is about a half minute. 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. This relative speed leads the half of the link lifetime between the vehicle and the IP-RSU. In reality, the DSRC communication range is around 500m, so the link lifetime will be a half of the maximum time. The time constraint of a wireless link between two nodes (e.g., vehicle and IP-RSU) 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, DNS query, and context-aware navigation (in Section 3.1). Regardless of a session's type, to guide all the IPv6 packets to their destination host(s), IP mobility should be supported for the session. In a V2V scenario (e.g., context-aware navigation), the IPv6 packets of a vehicle should be delivered to relevant vehicles in an efficient way (e.g., multicasting). With this observation, IPv6 protocol exchanges need to be done as short as possible to support the message exchanges of various applications in vehicular networks.

Therefore, 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. Meanwhile, the bandwidth of the wireless link determined by the lower layers

(i.e., link and PHY layers) can affect the transmission time of control messages of the upper layers (e.g., IPv6) and the continuity of sessions in the higher layers (e.g., IPv6, TCP, and UDP). Hence the bandwidth selection according to Modulation and Coding Scheme (MCS) also affects the vehicular network connectivity. Note that usually the higher bandwidth gives the shorter communication range and the higher packet error rate at the receiving side, which may reduce the reliability of control message exchanges of the higher layers (e.g., IPv6). This section presents key topics such as neighbor discovery and mobility management for links and sessions in IPv6-based vehicular networks.

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 IPv6 addresses to 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 DAD packets during a vehicle's travel in a road network, which can guarantee 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 can guarantee 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. An address lookup operation may be conducted by an MA or IP-RSU (as

Registrar in RPL) to check the uniqueness of an IPv6 address that will be configured by a vehicle as DAD. Also, the partitioning of a VANET may make vehicles with the same prefix be physically unreachable. An address lookup operation may be conducted by an MA or IP-RSU (as Registrar in RPL) to check the existence of a vehicle under the network coverage of the MA or IP-RSU as NUD. Thus, SLAAC needs to prevent IPv6 address duplication due to the merging of VANETs, and IPv6 ND needs to detect unreachable neighboring vehicles due to the partitioning of a VANET. According to the merging and partitioning, a destination vehicle (as an IPv6 host) needs to be distinguished as either an on-link host or a not-onlink host even though the source vehicle can use the same prefix as the destination vehicle [I-D.ietf-intarea-ippl].

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.

For vehicular networks with high mobility and density, DAD needs to be performed efficiently with minimum overhead so that the vehicles can exchange driving safety messages (e.g., collision avoidance and accident notification) with each other with a short interval suggested by NHTSA (National Highway Traffic Safety Administration) [NHTSA-ACAS-Report]. Since the partitioning and merging of vehicular networks may require re-perform DAD process repeatedly, the link scope of vehicles may be limited to a small area, which may delay the exchange of driving safety messages. Driving safety messages can include a vehicle's mobility information (i.e., position, speed, direction, and acceleration/deceleration) that is critical to other vehicles. The exchange interval of this message is recommended to be less than 0.5 second, which is required for a driver to avoid an emergency situation, such as a rear-end crash.

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. The ND time-related parameters can be an operational setting or an optimization point particularly for vehicular networks.

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.

From the interoperability point of view, in IPv6-based vehicular networking, IPv6 ND should have minimum changes with the legacy IPv6 ND used in the Internet, including DAD and NUD operations, so that IPv6-based vehicular networks can be seamlessly connected to other intelligent transportation elements (e.g., traffic signals, pedestrian wearable devices, electric scooters, and bus stops) that use the standard IPv6 network settings.

5.1.1. Link Model

A subnet 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 subnet 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.

[I-D.thubert-6man-ipv6-over-wireless] introduces other issues in an IPv6 subnet model.

IPv6 protocols work under certain assumptions that do not necessarily hold for vehicular wireless access link types [VIP-WAVE][RFC5889]. 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, unique-local, and global types of IPv6 addresses. In an IPv6 link, it is defined 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 4. 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. Considering that two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, if they are not in one hop (that is, they have the multihop network connectivity between them), then they may not be able to communicate with each other. 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 4.

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 not-onlink 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 not-onlink. In most cases in vehicular networks, due to the partitioning and merging of VANETs, and the multihop network topology of VANETS, not-onlink prefixes will be used for vehicles as default.

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.

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 DAD procedure.

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 [RFC9119].

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.

RPL [RFC6550] defines a routing protocol for low-power and lossy networks, which constructs and maintains Destination-Oriented Directed Acyclic Graphs (DODAGs) optimized by an Objective Function (OF). A defined OF provides route selection and optimization within

an RPL topology. The RPL nodes use an anisotropic Distance Vector (DV) approach to form a DODAG by discovering and aggressively maintaining the upward default route toward the root of the DODAG. Downward routes follow the same DODAG, with lazy maintenance and stretched Peer-to-Peer (P2P) routing in the so-called storing mode. It is well-designed to reduce the topological knowledge and routing state that needs to be exchanged. As a result, the routing protocol overhead is minimized, which allows either highly constrained stable networks or less constrained, highly dynamic networks. Refer to Appendix B for the detailed description of RPL for multihop V2X networking.

An address registration extension for 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Network) in [RFC8505] can support light-weight mobility for nodes moving through different parents. [RFC8505], as opposed to [RFC4861], is stateful and proactively installs the ND cache entries, which saves broadcasts and provides a deterministic presence information for IPv6 addresses. Mainly it updates the Address Registration Option (ARO) of ND defined in [RFC6775] to include a status field that can indicate the movement of a node and optionally a Transaction ID (TID) field, i.e., a sequence number that can be used to determine the most recent location of a node. Thus, RPL can use the information provided by the Extended ARO (EARO) defined in [RFC8505] to deal with a certain level of node mobility. When a leaf node moves to the coverage of another parent node, it should de-register its addresses to the previous parent node and register itself with a new parent node along with an incremented TID.

RPL can be used in IPv6-based vehicular networks, but it is primarily designed for lossy networks, which puts energy efficiency first. For using it in IPv6-based vehicular networks, there have not been actual experiences and practical implementations for vehicular networks, though it was tested in IoT low-power and lossy networks (LLN) scenarios.

Moreover, due to bandwidth and energy constraints, RPL does not suggest to use a proactive mechanism (e.g., keepalive) to maintain accurate routing adjacencies such as Bidirectional Forwarding Detection [RFC5881] and MANET Neighborhood Discovery Protocol [RFC6130]. As a result, due to the mobility of vehicles, network fragmentation may not be detected quickly and the routing of packets between vehicles or between a vehicle and an infrastructure node may fail.

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 domain, 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, DAD is not required. On the other hand, for a mobility management scheme with a unique prefix per mobile node (e.g., PMIPv6 [RFC5213]), 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.

Even though the SLAAC with classic ND costs a DAD during mobility management, the SLAAC with [RFC8505] and/or AERO/OMNI do not cost a DAD. SLAAC for vehicular networks needs to consider the minimization of the cost of DAD with the help of an infrastructure node (e.g., IP-RSU and MA). Using an infrastructure prefix over VANET allows direct routability to the Internet through the multihop V2I toward an IP-RSU. On the other hand, a BYOA does not allow such direct routability to the Internet since the BYOA is not topologically correct, that is, not routable in the Internet. In addition, a vehicle configured with a BYOA needs a tunnel home (e.g., IP-RSU) connected to the Internet, and the vehicle needs to know which neighboring vehicle is reachable inside the VANET toward the tunnel home. There is nonnegligible control overhead to set up and maintain routes to such a tunnel home [RFC4888] over the VANET.

For the case of a multihomed network, a vehicle can follow the first-hop router selection rule described in [RFC8028]. For example, an IP-OBUS inside a vehicle may connect to an IP-RSU that has multiple routers behind. In this scenario, because the IP-OBUS can have multiple prefixes from those routers, the default router selection, source address selection, and packet redirect process should follow the guidelines in [RFC8028]. That is, the vehicle should select its default router for each prefix by preferring the router that advertised the prefix.

Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275], PMIPv6 [RFC5213], and NEMO [RFC3963], so the TCC (or an MA inside the TCC) maintains the mobility information of vehicles for location management. Also, in vehicular networks, asymmetric links sometimes exist and must be considered for wireless communications such as V2V and V2I.

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 paramount in V2I, V2V, and V2X networking along with neighbor discovery and mobility management.

Vehicles and infrastructure must be authenticated in order to participate in vehicular networking. For the authentication in vehicular networks, vehicular cloud needs to support a kind of Public Key Infrastructure (PKI) in an efficient way. To provide safe interaction between vehicles or between a vehicle and infrastructure, only authenticated nodes (i.e., vehicle and infrastructure node) can participate in vehicular networks. 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. Note that when driver/passenger's mobile devices are connected to a vehicle's internal network, the vehicle may be more vulnerable to possible attacks from external networks.

For secure V2I communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBUE) in a vehicle and a fixed router (i.e., IP-RSU) in an EN needs to be established, as shown in Figure 2 [RFC4301][RFC4302] [RFC4303][RFC4308] [RFC7296]. Also, for secure V2V communication, a secure channel (e.g., IPsec) between a mobile router (i.e., IP-OBUE) in a vehicle and a mobile router (i.e., IP-OBUE) in another vehicle needs to be established, as shown in Figure 3. 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). IEEE 1609.2 [WAVE-1609.2] specifies security services for applications and management messages, but this WAVE specification is optional. Thus, if the link layer 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.

6.1. Security Threats in Neighbor Discovery

For the classical IPv6 ND, 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. [RFC6959] introduces threats enabled by IP source address spoofing. This possibility indicates that vehicles and IP-RSUs need to filter out suspicious ND traffic in advance. [RFC8928] introduces a mechanism that protects the ownership of an address for 6LoWPAN ND from address theft and impersonation attacks. Based on the SEND [RFC3971] mechanism, the authentication for routers (i.e., IP-RSUs) can be conducted by only selecting an IP-RSU that has a certification path toward trusted parties. For authenticating other vehicles, the cryptographically generated address (CGA) can be used to verify the true owner of a received ND message, which requires to use the CGA ND option in the ND protocols. For a general protection of the ND mechanism, the RSA Signature ND option can also be used to protect the integrity of the messages by public key signatures. For a more advanced authentication mechanism, a distributed blockchain-based approach [Vehicular-BlockChain] can be used. However, for a scenario where a trustable router or an authentication path cannot be obtained, it is desirable to find a solution in which vehicles and infrastructures can authenticate each other without any support from a third party.

When applying the classical IPv6 ND process to VANET, one of the security issues is that an IP-RSU (or an IP-OBUE) as a router may receive deliberate or accidental DoS attacks from network scans that probe devices on a VANET. In this scenario, the IP-RSU can be overwhelmed for processing the network scan requests so that the capacity and resources of IP-RSU are exhausted, causing the failure of receiving normal ND messages from other hosts for network address resolution. [RFC6583] describes more about the operational problems in the classical IPv6 ND mechanism that can be vulnerable to deliberate or accidental DoS attacks and suggests several implementation guidelines and operational mitigation techniques for those problems. Nevertheless, for running IPv6 ND in VANET, those issues can be more acute since the movements of vehicles can be so diverse that it leaves a large room for rogue behaviors, and the failure of networking among vehicles may cause grave consequences.

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. Since cyber security issues in vehicular networks may cause physical vehicle safety issues, it may be necessary to consider those physical security concerns when designing protocols in IPWAVE.

To identify malicious vehicles among vehicles, an authentication method may be 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 2, 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.

6.2. Security Threats in Mobility Management

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).

6.3. Other Threats

For the setup of a secure channel over IPsec or TLS, the multihop V2I communications over DSRC or 5G V2X (or LTE V2X) is required in a highway. In this case, multiple intermediate vehicles as relay nodes can help forward association and authentication messages toward an IP-RSU (gNodeB, or eNodeB) connected to an authentication server in the vehicular cloud. In this kind of process, the authentication messages forwarded by each vehicle can be delayed or lost, which may

increase the construction time of a connection or some vehicles may not be able to be authenticated.

Even though vehicles can be authenticated with valid certificates by an authentication server in the vehicular cloud, the authenticated vehicles may harm other vehicles. To deal with this kind of security issue, for monitoring suspicious behaviors, vehicles' communication activities can be recorded 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. To solve the issue ultimately, we need a solution where, without privacy breakage, vehicles may observe activities of each other to identify any misbehavior. Once identifying a misbehavior, a vehicle shall have a way to either isolate itself from others or isolate a suspicious vehicle by informing other vehicles. Alternatively, for completely secure vehicular networks, we shall embrace the concept of "zero-trust" for vehicles in which no vehicle is trustable and verifying every message is necessary. For doing so, we shall have an efficient zero-trust framework or mechanism for vehicular networks.

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 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][RFC8981]. 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. Privacy concerns for excessively collecting vehicle activities from roadway operators such as public transportation administrators and private contractors may also pose threats on violating privacy rights of vehicles. It might be interesting to find a solution from a technology point of view along with public policy development for the issue.

7. IANA Considerations

This document does not require any IANA actions.

8. References

8.1. Normative References

- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999, <<https://www.rfc-editor.org/info/rfc2710>>.
- [RFC3626] Clausen, T., Ed. and P. Jacquet, Ed., "Optimized Link State Routing Protocol (OLSR)", RFC 3626, DOI 10.17487/RFC3626, October 2003, <<https://www.rfc-editor.org/info/rfc3626>>.
- [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>>.
- [RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <<https://www.rfc-editor.org/info/rfc3810>>.

- [RFC3849] Huston, G., Lord, A., and P. Smith, "IPv6 Address Prefix Reserved for Documentation", RFC 3849, DOI 10.17487/RFC3849, July 2004, <<https://www.rfc-editor.org/info/rfc3849>>.
- [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>>.
- [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>>.
- [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>>.
- [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>>.
- [RFC4308] Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, DOI 10.17487/RFC4308, December 2005, <<https://www.rfc-editor.org/info/rfc4308>>.
- [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>>.
- [RFC4885] Ernst, T. and H-Y. Lach, "Network Mobility Support Terminology", RFC 4885, DOI 10.17487/RFC4885, July 2007, <<https://www.rfc-editor.org/info/rfc4885>>.
- [RFC4888] Ng, C., Thubert, P., Watari, M., and F. Zhao, "Network Mobility Route Optimization Problem Statement", RFC 4888, DOI 10.17487/RFC4888, July 2007, <<https://www.rfc-editor.org/info/rfc4888>>.
- [RFC5213] Gundavelli, S., Ed., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, DOI 10.17487/RFC5213, August 2008, <<https://www.rfc-editor.org/info/rfc5213>>.
- [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, DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [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>>.
- [RFC5614] Ogier, R. and P. Spagnolo, "Mobile Ad Hoc Network (MANET) Extension of OSPF Using Connected Dominating Set (CDS) Flooding", RFC 5614, DOI 10.17487/RFC5614, August 2009, <<https://www.rfc-editor.org/info/rfc5614>>.
- [RFC5881] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)", RFC 5881, DOI 10.17487/RFC5881, June 2010, <<https://www.rfc-editor.org/info/rfc5881>>.
- [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>>.

- [RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, DOI 10.17487/RFC6130, April 2011, <<https://www.rfc-editor.org/info/rfc6130>>.
- [RFC6250] Thaler, D., "Evolution of the IP Model", RFC 6250, DOI 10.17487/RFC6250, May 2011, <<https://www.rfc-editor.org/info/rfc6250>>.
- [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>>.
- [RFC6550] Winter, T., Ed., Thubert, P., Ed., 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, DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.
- [RFC6583] Gashinsky, I., Jaeggli, J., and W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583, DOI 10.17487/RFC6583, March 2012, <<https://www.rfc-editor.org/info/rfc6583>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.
- [RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, DOI 10.17487/RFC7149, March 2014, <<https://www.rfc-editor.org/info/rfc7149>>.
- [RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <<https://www.rfc-editor.org/info/rfc7181>>.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <<https://www.rfc-editor.org/info/rfc7296>>.

- [RFC7333] Chan, H., Ed., Liu, D., Seite, P., Yokota, H., and J. Korhonen, "Requirements for Distributed Mobility Management", RFC 7333, DOI 10.17487/RFC7333, August 2014, <<https://www.rfc-editor.org/info/rfc7333>>.
- [RFC7429] Liu, D., Ed., Zuniga, JC., Ed., Seite, P., Chan, H., and CJ. Bernardos, "Distributed Mobility Management: Current Practices and Gap Analysis", RFC 7429, DOI 10.17487/RFC7429, January 2015, <<https://www.rfc-editor.org/info/rfc7429>>.
- [RFC7466] Dearlove, C. and T. Clausen, "An Optimization for the Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 7466, DOI 10.17487/RFC7466, March 2015, <<https://www.rfc-editor.org/info/rfc7466>>.
- [RFC8028] Baker, F. and B. Carpenter, "First-Hop Router Selection by Hosts in a Multi-Prefix Network", RFC 8028, DOI 10.17487/RFC8028, November 2016, <<https://www.rfc-editor.org/info/rfc8028>>.
- [RFC8175] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <<https://www.rfc-editor.org/info/rfc8175>>.
- [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>>.
- [RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <<https://www.rfc-editor.org/info/rfc8446>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.
- [RFC8629] Cheng, B. and L. Berger, Ed., "Dynamic Link Exchange Protocol (DLEP) Multi-Hop Forwarding Extension", RFC 8629, DOI 10.17487/RFC8629, July 2019, <<https://www.rfc-editor.org/info/rfc8629>>.

- [RFC8691] Benamar, N., Härri, 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, DOI 10.17487/RFC8691, December 2019, <<https://www.rfc-editor.org/info/rfc8691>>.
- [RFC8757] Cheng, B. and L. Berger, Ed., "Dynamic Link Exchange Protocol (DLEP) Latency Range Extension", RFC 8757, DOI 10.17487/RFC8757, March 2020, <<https://www.rfc-editor.org/info/rfc8757>>.
- [RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November 2020, <<https://www.rfc-editor.org/info/rfc8928>>.
- [RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <<https://www.rfc-editor.org/info/rfc8981>>.
- [RFC9119] Perkins, C., McBride, M., Stanley, D., Kumari, W., and JC. Zúñiga, "Multicast Considerations over IEEE 802 Wireless Media", RFC 9119, DOI 10.17487/RFC9119, October 2021, <<https://www.rfc-editor.org/info/rfc9119>>.

8.2. Informative References

- [RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, DOI 10.17487/RFC4821, March 2007, <<https://www.rfc-editor.org/info/rfc4821>>.
- [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>>.
- [RFC8899] Fairhurst, G., Jones, T., Tüxen, M., Rüngeler, I., and T. Völker, "Packetization Layer Path MTU Discovery for Datagram Transports", RFC 8899, DOI 10.17487/RFC8899, September 2020, <<https://www.rfc-editor.org/info/rfc8899>>.

[I-D.ietf-intarea-ippl]

Nordmark, E., "IP over Intentionally Partially Partitioned Links", Work in Progress, Internet-Draft, draft-ietf-intarea-ippl-00, 30 March 2017, <<https://www.ietf.org/archive/id/draft-ietf-intarea-ippl-00.txt>>.

[I-D.ietf-lisp-rfc6830bis]

Farinacci, D., Fuller, V., Meyer, D., Lewis, D., and A. Cabellos, "The Locator/ID Separation Protocol (LISP)", Work in Progress, Internet-Draft, draft-ietf-lisp-rfc6830bis-36, 18 November 2020, <<https://www.ietf.org/archive/id/draft-ietf-lisp-rfc6830bis-36.txt>>.

[I-D.templin-6man-aero]

Templin, F. L., "Automatic Extended Route Optimization (AERO)", Work in Progress, Internet-Draft, draft-templin-6man-aero-40, 7 March 2022, <<https://www.ietf.org/archive/id/draft-templin-6man-aero-40.txt>>.

[I-D.templin-6man-omni]

Templin, F. L., "Transmission of IP Packets over Overlay Multilink Network (OMNI) Interfaces", Work in Progress, Internet-Draft, draft-templin-6man-omni-55, 7 March 2022, <<https://www.ietf.org/archive/id/draft-templin-6man-omni-55.txt>>.

[I-D.templin-ipwave-uam-its]

Templin, F. L., "Urban Air Mobility Implications for Intelligent Transportation Systems", Work in Progress, Internet-Draft, draft-templin-ipwave-uam-its-04, 4 January 2021, <<https://www.ietf.org/archive/id/draft-templin-ipwave-uam-its-04.txt>>.

[I-D.templin-intarea-parcels]

Templin, F. L., "IP Parcels", Work in Progress, Internet-Draft, draft-templin-intarea-parcels-09, 10 February 2022, <<https://www.ietf.org/archive/id/draft-templin-intarea-parcels-09.txt>>.

- [I-D.ietf-dmm-fpc-cpdp]
Matsushima, S., Bertz, L., Liebsch, M., Gundavelli, S., Moses, D., and C. E. Perkins, "Protocol for Forwarding Policy Configuration (FPC) in DMM", Work in Progress, Internet-Draft, draft-ietf-dmm-fpc-cpdp-14, 22 September 2020, <<https://www.ietf.org/archive/id/draft-ietf-dmm-fpc-cpdp-14.txt>>.
- [I-D.thubert-6man-ipv6-over-wireless]
Thubert, P., "IPv6 Neighbor Discovery on Wireless Networks", Work in Progress, Internet-Draft, draft-thubert-6man-ipv6-over-wireless-11, 15 December 2021, <<https://www.ietf.org/archive/id/draft-thubert-6man-ipv6-over-wireless-11.txt>>.
- [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.
- [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.
- [IEEE-802.11-OCB]
"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, December 2016.
- [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.
- [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.
- [TS-23.285-3GPP]
3GPP, "Architecture Enhancements for V2X Services", 3GPP TS 23.285/Version 16.2.0, December 2019.
- [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.
- [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.
- [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.

- [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.
- [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.
- [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.
- [CA-Cruise-Control] California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", Available: <https://path.berkeley.edu/research/connected-and-automated-vehicles/cooperative-adaptive-cruise-control>, 2022.
- [Truck-Platooning] California Partners for Advanced Transportation Technology (PATH), "Automated Truck Platooning", Available: <https://path.berkeley.edu/research/connected-and-automated-vehicles/truck-platooning>, 2022.
- [FirstNet] U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", Available: <https://www.firstnet.gov/>, 2022.
- [PSCE] European Commission, "Public Safety Communications Europe (PSCE)", Available: <https://www.psc-europe.eu/>, 2022.

[FirstNet-Report]

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

[SignalGuru]

Koukoumidis, E., Peh, L., and M. Martonosi, "SignalGuru: Leveraging Mobile Phones for Collaborative Traffic Signal Schedule Advisory", ACM MobiSys, June 2011.

[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.

[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.

[NHTSA-ACAS-Report]

National Highway Traffic Safety Administration (NHTSA), "Final Report of Automotive Collision Avoidance Systems (ACAS) Program", DOT HS 809 080, August 2000.

[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.

[LIFS]

Wang, J., Xiong, J., Jiang, H., Jamieson, K., Chen, X., Fang, D., and C. Wang, "Low Human-Effort, Device-Free Localization with Fine-Grained Subcarrier Information", IEEE Transactions on Mobile Computing, November 2018.

[DFC]

Jeong, J., Shen, Y., Kim, S., Choe, D., Lee, K., and Y. Kim, "DFC: Device-free human counting through WiFi fine-grained subcarrier information", IET Communications, January 2021.

[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.

[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.

[Bitcoin] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash
System", URL: <https://bitcoin.org/bitcoin.pdf>, May 2009.

[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.

Appendix A. Support of Multiple Radio Technologies for V2V

Vehicular networks may consist of multiple radio technologies such as DSRC and 5G V2X. Although a Layer-2 solution can provide support for multihop communications in vehicular networks, the scalability issue related to multihop forwarding still remains when vehicles need to disseminate or forward packets toward multihop-away destinations. In addition, the IPv6-based approach for V2V as a network layer protocol can accommodate multiple radio technologies as MAC protocols, such as DSRC and 5G V2X. Therefore, the existing IPv6 protocol can be augmented through the addition of a virtual interface (e.g., OMNI [I-D.templin-6man-omni] and DLEP [RFC8175]) and/or protocol changes in order to support both wireless single-hop/multihop V2V communications and multiple radio technologies in vehicular networks. In such a way, vehicles can communicate with each other by V2V communications to share either an emergency situation or road hazard information in a highway having multiple kinds of radio technologies.

Appendix B. Support of Multihop V2X Networking

The multihop V2X networking can be supported by RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) [RFC6550] and Overlay Multilink Network Interface (OMNI) [I-D.templin-6man-omni].

RPL defines an IPv6 routing protocol for low-power and lossy networks (LLN), mostly designed for home automation routing, building automation routing, industrial routing, and urban LLN routing. It uses a Destination-Oriented Directed Acyclic Graph (DODAG) to construct routing paths for hosts (e.g., IoT devices) in a network. The DODAG uses an objective function (OF) for route selection and optimization within the network. A user can use different routing metrics to define an OF for a specific scenario. RPL supports

multipoint-to-point, point-to-multipoint, and point-to-point traffic, and the major traffic flow is the multipoint-to-point traffic. For example, in a highway scenario, a vehicle may not access an RSU directly because of the distance of the DSRC coverage (up to 1 km). In this case, the RPL 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.

RPL is primarily designed to minimize the control plane activity, which is the relative amount of routing protocol exchanges versus data traffic; this approach is beneficial for situations where the power and bandwidth are scarce (e.g., an IoT LLN where RPL is typically used today), but also in situations of high relative mobility between the nodes in the network (also known as swarming, e.g., within a variable set of vehicles with a similar global motion, or a variable set of drones flying toward the same direction).

To reduce the routing exchanges, RPL leverages a Distance Vector (DV) approach, which does not need a global knowledge of the topology, and only optimizes the routes to and from the root, allowing Peer-to-Peer (P2P) paths to be stretched. Although RPL installs its routes proactively, it only maintains them lazily, that is, in reaction to actual traffic, or as a slow background activity. Additionally, RPL leverages the concept of an objective function (called OF), which allows to adapt the activity of the routing protocol to use cases, e.g., type, speed, and quality of the radios. RPL does not need converge, and provides connectivity to most nodes most of the time. The default route toward the root is maintained aggressively and may change while a packet progresses without causing loops, so the packet will still reach the root. There are two modes for routing in RPL such as non-storing mode and storing mode. In non-storing mode, a node inside the mesh/swarm that changes its point(s) of attachment to the graph informs the root with a single unicast packet flowing along the default route, and the connectivity is restored immediately; this mode is preferable for use cases where Internet connectivity is dominant. On the other hand, in storing mode, the routing stretch is reduced, for a better P2P connectivity, while the Internet connectivity is restored more slowly, during the time for the DV operation to operate hop-by-hop. While an RPL topology can quickly scale up and down and fits the needs of mobility of vehicles, the total performance of the system will also depend on how quickly a node can form an address, join the mesh (including Authentication, Authorization, and Accounting (AAA)), and manage its global mobility to become reachable from another node outside the mesh.

OMNI defines a protocol for the transmission of IPv6 packets over Overlay Multilink Network Interfaces that are virtual interfaces governing multiple physical network interfaces. OMNI supports multihop V2V communication between vehicles in multiple forwarding hops via intermediate vehicles with OMNI links. It also supports multihop V2I communication between a vehicle and an infrastructure access point by multihop V2V communication. 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.

In OMNI protocol, each wireless media interface is configured with an IPv6 Unique Local Address (ULA) [RFC4193] that is assured unique within the vehicular network according to AERO/OMNI and [RFC5889]. The ULA supports both V2V and V2I multihop forwarding within the vehicular network (e.g., via a VANET routing protocol) while each vehicle can communicate with Internet correspondents using global IPv6 addresses via OMNI interface encapsulation over the wireless interface.

For the control traffic overhead for running both vehicular ND and a VANET routing protocol, the AERO/OMNI approach may avoid this issue by using MANET routing protocols only (i.e., no multicast of IPv6 ND messaging) in the wireless underlay network while applying efficient unicast IPv6 ND messaging in the OMNI overlay on an as-needed basis for router discovery and NUD. This greatly reduces the overhead for VANET-wide multicasting while providing agile accommodation for dynamic topology changes.

Appendix C. Support of Mobility Management for V2I

The seamless application communication between two vehicles or between a vehicle and an infrastructure node requires mobility management in vehicular networks. The mobility management schemes include a host-based mobility scheme, network-based mobility scheme, and software-defined networking scheme.

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][I-D.ietf-dmm-fpc-cpdp]. Note that Forwarding Policy Configuration (FPC) in [I-D.ietf-dmm-fpc-cpdp], 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.

Appendix D. Support of MTU Diversity for IP-based Vehicular Networks

The wireless and/or wired-line links in paths between both mobile nodes and fixed network correspondents may configure a variety of Maximum Transmission Units (MTUs), where all IPv6 links are required to support a minimum MTU of 1280 octets and may support larger MTUs. Unfortunately, determining the path MTU (i.e., the minimum link MTU in the path) has proven to be inefficient and unreliable due to the uncertain nature of the loss-oriented ICMPv6 messaging service used for path MTU discovery. Recent developments have produced a more reliable path MTU determination service for TCP [RFC4821] and UDP [RFC8899] however the MTUs discovered are always limited by the most restrictive link MTU in the path (often 1500 octets or smaller).

The AERO/OMNI service addresses the MTU issue by introducing a new layer in the Internet architecture known as the "OMNI Adaptation Layer (OAL)". The OAL allows end systems that configure an OMNI interface to utilize a full 65535 octet MTU by leveraging the IPv6 fragmentation and reassembly service during encapsulation to produce fragment sizes that are assured of traversing the path without loss due to a size restriction. (This allows end systems to send packets that are often much larger than the actual path MTU.)

Performance studies over the course of many decades have proven that applications will see greater performance by sending smaller numbers of large packets (as opposed to larger numbers of small packets) even if fragmentation is needed. The OAL further supports even larger packet sizes through the IP Parcels construct [I-D.templin-intarea-parcels] which provides "packets-in-packet" encapsulation for a total size up to 4MB. Together, the OAL and IP Parcels will provide a revolutionary new capability for greater efficiency in both mobile and fixed networks.

Appendix E. 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, Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-2017-0-01633) supervised by the IITP.

This work was supported in part by the IITP (2020-0-00395, Standard Development of Blockchain based Network Management Automation Technology).

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).

This work was supported in part by the Cisco University Research Program Fund, Grant # 2019-199458 (3696), and by ANID Chile Basal Project FB0008.

Appendix F. 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 Lozano (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 (Kaloomb), 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), Peter E. Yee (Akayla), and Erik Kline. 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:
scspede@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: <https://chrisshen.github.io>

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
Email: pauljeong@skku.edu
URI: <http://iotlab.skku.edu/people-jaehoon-jeong.php>