IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 21, 2018

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

June 19, 2018

Transmission of IPv6 Packets over IEEE 802.11 Networks operating in mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB) draft-ietf-ipwave-ipv6-over-80211ocb-25

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 December 21, 2018.

Copyright Notice

Table of Contents

1. Introduction

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

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

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

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

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

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

IP-OBU (Internet Protocol On-Board Unit): an IP-OBU is a computer situated in a vehicle such as an automobile, bicycle, or similar. It

has at least one IP interface that runs in mode OCB of 802.11, and that has an "OBU" transceiver. See the definition of the term "OBU" in section Appendix I.

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

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

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

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

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

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

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

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

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

4.2. Frame Format

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

The IPv6 packet transmitted on 802.11-OCB MUST be 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), the value of the Type field MUST be set to 0x86DD (IPv6). In the 802.11 header, the value of the Subtype sub-field in the Frame Control field MUST be set to 8 (i.e. 'QoS Data'); the value of the Traffic Identifier (TID) sub-field of the QoS Control field of the 802.11 header MUST be set to binary 001 (i.e. User Priority 'Background', QoS Access Category 'AC_BK').

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers MAY implement an Ethernet Adaptation Layer that translates Ethernet II frames to the 802.11 format and vice versa. An Ethernet Adaptation Layer is described in Section 4.2.1.

4.2.1. Ethernet Adaptation Layer

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

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

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

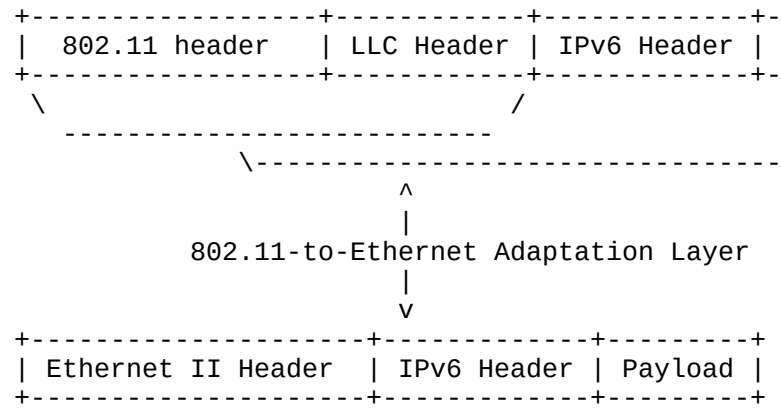


Figure 1: Operation of the Ethernet Adaptation Layer

The Receiver and Transmitter Address fields in the 802.11 header MUST contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header MUST be the same as the value of the Type field in the Ethernet II Header. That value MUST be set to 0x86DD (IPv6).

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

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

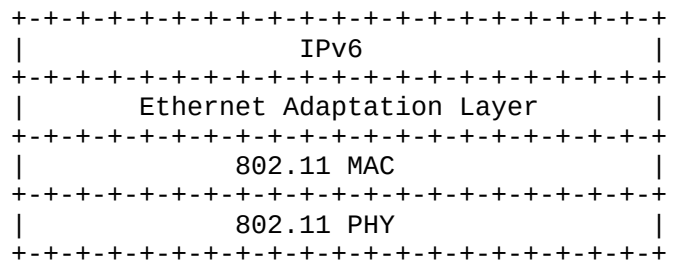


Figure 2: Ethernet Adaptation Layer stacked with other layers

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

4.3. Link-Local Addresses

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

4.4. Address Mapping

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

4.4.1. Address Mapping -- Unicast

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

4.4.2. Address Mapping -- Multicast

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

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

4.5. Stateless Autoconfiguration

The Interface Identifier for an 802.11-OCB interface is formed using the same rules as the Interface Identifier for an Ethernet interface; 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.

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

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

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

4.6. Subnet Structure

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

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

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

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

5. Security Considerations

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

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

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

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

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

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

hence dynamically change the affected IP address), in the way the IPv6 Privacy addresses were used, and other effects.

6. IANA Considerations

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

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

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

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

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

8. Acknowledgements

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

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

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

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

9. References

9.1. Normative References

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

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

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

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

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

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

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

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

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

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

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

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

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

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <https://www.rfc-editor.org/info/rfc5889>.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011, <https://www.rfc-editor.org/info/rfc6275>.

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

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

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

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

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

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

9.2. Informative References

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

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

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

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

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

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

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

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

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

Appendix A. ChangeLog

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

-25: added a reference to 'IEEE Management Information Base', instead of just 'Management Information Base'; added ref to further appendices in the introductory phrases; improved text for IID formation for SLAAC, inserting recommendation for RFC8064 before RFC2464.

From draft-ietf-ipwave-ipv6-over-80211ocb-23 to draft-ietf-ipwave-ipv6-over-80211ocb-24

- Nit: wrote "IPWAVE Working Group" on the front page, instead of "Network Working Group".

- Addressed the comments on 6MAN: replaced a sentence about ND problem with "is used over 802.11-OCB".

From draft-ietf-ipwave-ipv6-over-80211ocb-22 to draft-ietf-ipwave-ipv6-over-80211ocb-23

- No content modifications, but check the entire draft chain on IPv6-only: xml2rfc, submission on tools.ietf.org and datatracker.

From draft-ietf-ipwave-ipv6-over-80211ocb-21 to draft-ietf-ipwave-ipv6-over-80211ocb-22

- Corrected typo, use dash in "802.11-OCB" instead of space.

- Improved the Frame Format section: MUST use QoSData, specify the values within; clarified the Ethernet Adaptation Layer text.

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

- Corrected a few nits and added names in Acknowledgments section.

- Removed unused reference to old Internet Draft tsvwg about QoS.

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

- Reduced the definition of term "802.11-OCB".

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

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

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

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

- Improved the MTU and fragmentation paragraph.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 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

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

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

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

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

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

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

- 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."

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

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

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

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

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

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

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

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

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

- Minor typographical errors.

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

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

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

- Shortened the Introduction and the Abstract.

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

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

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

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

- Added term definition for WiFi.

- Updated the authorship and expanded the Contributors section.

- Corrected typographical errors.

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

- Removed the per-channel IPv6 prohibition text.

- Corrected typographical errors.

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

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

- Improved definition of term "802.11-OCB".
- Clarified that OCB does not "strip" security, but that the operation in OCB mode is "stripped off of all .11 security".
- Clarified that theoretical OCB bandwidth speed is 54mbits, but that a commonly observed bandwidth in IP-over-OCB is 12mbit/s.
- Corrected typographical errors, and improved some phrasing.

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

- Updated references of 802.11-OCB document from -2012 to the IEEE 802.11-2016.
- In the LL address section, and in SLAAC section, added references to 7217 opaque IIDs and 8064 stable IIDs.

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

- Lengthened the title and cleanded the abstract.
- Added text suggesting LLs may be easy to use on OCB, rather than GUAs based on received prefix.
- Added the risks of spoofing and hijacking.
- Removed the text speculation on adoption of the TSA message.
- Clarified that the ND protocol is used.
- Clarified what it means "No association needed".
- Added some text about how two STAs discover each other.
- Added mention of external (OCB) and internal network (stable), in the subnet structure section.
- Added phrase explaining that both .11 Data and .11 QoS Data headers are currently being used, and may be used in the future.
- Moved the packet capture example into an Appendix Implementation Status.
- Suggested moving the reliability requirements appendix out into another document.

- Added a IANA Consiserations section, with content, requesting for a new multicast group "all OCB interfaces".
- 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.
- 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.
- Updated the affiliation of one author.
- Reformulation of some phrases for better readability, and correction of typographical errors.

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

- Removed a few informative references pointing to Dx draft IEEE 1609 documents.
- Removed outdated informative references to ETSI documents.
- Added citations to IEEE 1609.2, .3 and .4-2016.
- Minor textual issues.

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

- Keep the previous text on multiple addresses, so remove talk about MIP6, NEMOv6 and MCoA.
- Clarified that a 'Beacon' is an IEEE 802.11 frame Beacon.

- Clarified the figure showing Infrastructure mode and OCB mode side by side.
- Added a reference to the IP Security Architecture RFC.
- Detailed the IPv6-per-channel prohibition paragraph which reflects the discussion at the last IETF IPWAVE WG meeting.
- Added section "Address Mapping -- Unicast".
- Added the ".11 Trailer" to pictures of 802.11 frames.
- Added text about SNAP carrying the Ethertype.
- New RSU definition allowing for it be both a Router and not necessarily a Router some times.
- Minor textual issues.

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

- Replaced almost all occurences of 802.11p with 802.11-OCB, leaving only when explanation of evolution was necessary.
- Shortened by removing parameter details from a paragraph in the Introduction.
- Moved a reference from Normative to Informative.
- Added text in intro clarifying there is no handover spec at IEEE, and that 1609.2 does provide security services.
- Named the contents the fields of the EthernetII header (including the Ethertype bitstring).
- Improved relationship between two paragraphs describing the increase of the Sequence Number in 802.11 header upon IP fragmentation.
- Added brief clarification of "tracking".

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

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

- Introduced an appendix listing for information the set of 802.11 messages that may be transmitted in OCB mode.
- Removed appendix sections "Privacy Requirements", "Authentication Requirements" and "Security Certificate Generation".
- Removed appendix section "Non IP Communications".
- Introductory phrase in the Security Considerations section.
- Improved the definition of "OCB".
- Introduced theoretical stacked layers about IPv6 and IEEE layers including EPD.
- Removed the appendix describing the details of prohibiting IPv6 on certain channels relevant to 802.11-OCB.
- Added a brief reference in the privacy text about a precise clause in IEEE 1609.3 and .4.
- Clarified the definition of a Road Side Unit.
- Removed the discussion about security of WSA (because is non-IP).
- Removed mentioning of the GeoNetworking discussion.
- 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 IEEE Management Information Base (MIB) attribute "OCBActivated" [IEEE-802.11-2016]. Whenever OCBActivated is set to true the IEEE Std 802.11-OCB state is activated. For example, an 802.11 STAtion operating outside the context of a basic service set has the OCBActivated flag set. Such a station, when it has the flag set, uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

Appendix 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:

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

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

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

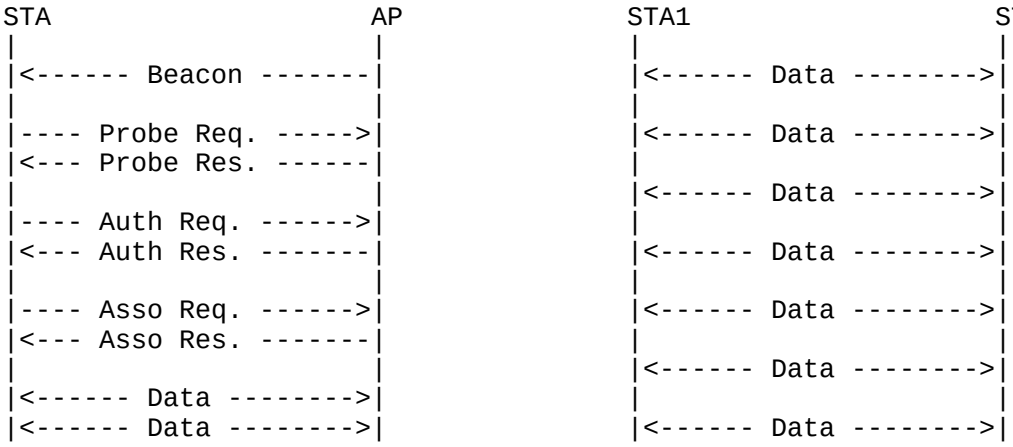


Figure 3: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

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

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

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

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

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

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

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

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

...) or by a cellular system. This message is optional for implementation.

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

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

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

Other aspects particular to 802.11-OCB, which are also particular to 802.11 (e.g. the 'hidden node' operation), may have an influence on

the use of transmission of IPv6 packets on 802.11-OCB networks. The OCB subnet structure is described in Section 4.6.

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

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

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

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

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

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

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

Changes needed on the network stack in OCB mode:

- Physical layer:

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

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

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

  MAC layer:

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

* No encryption key or method must be used.

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

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

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

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

Appendix E. EtherType Protocol Discrimination (EPD)

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

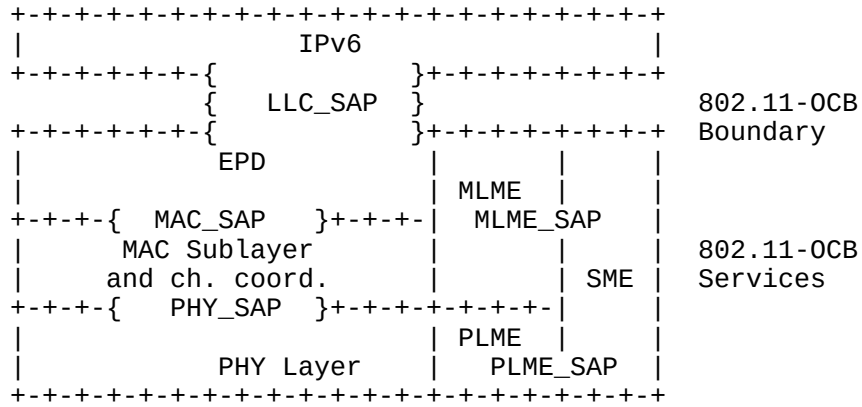


Figure 4: EtherType Protocol Discrimination

Appendix F. Design Considerations

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

F.1. Vehicle ID

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

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

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

F.2. Reliability Requirements

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

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

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

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

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

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

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

F.3. Multiple interfaces

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

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

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

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

F.4. MAC Address Generation

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

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

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

Appendix G. IEEE 802.11 Messages Transmitted in OCB mode

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

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;
- The STA may send data frames of subtype Data, Null, QoS Data, and QoS Null.

Appendix H. Implementation Status

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

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

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

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

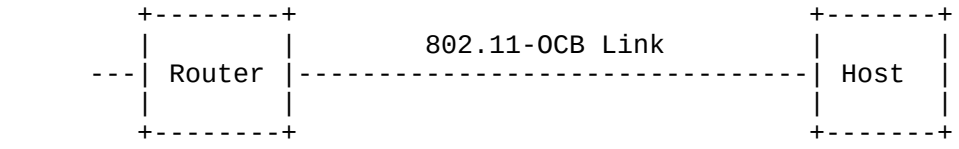


Figure 5: Topology for capturing IP packets on 802.11-OCB

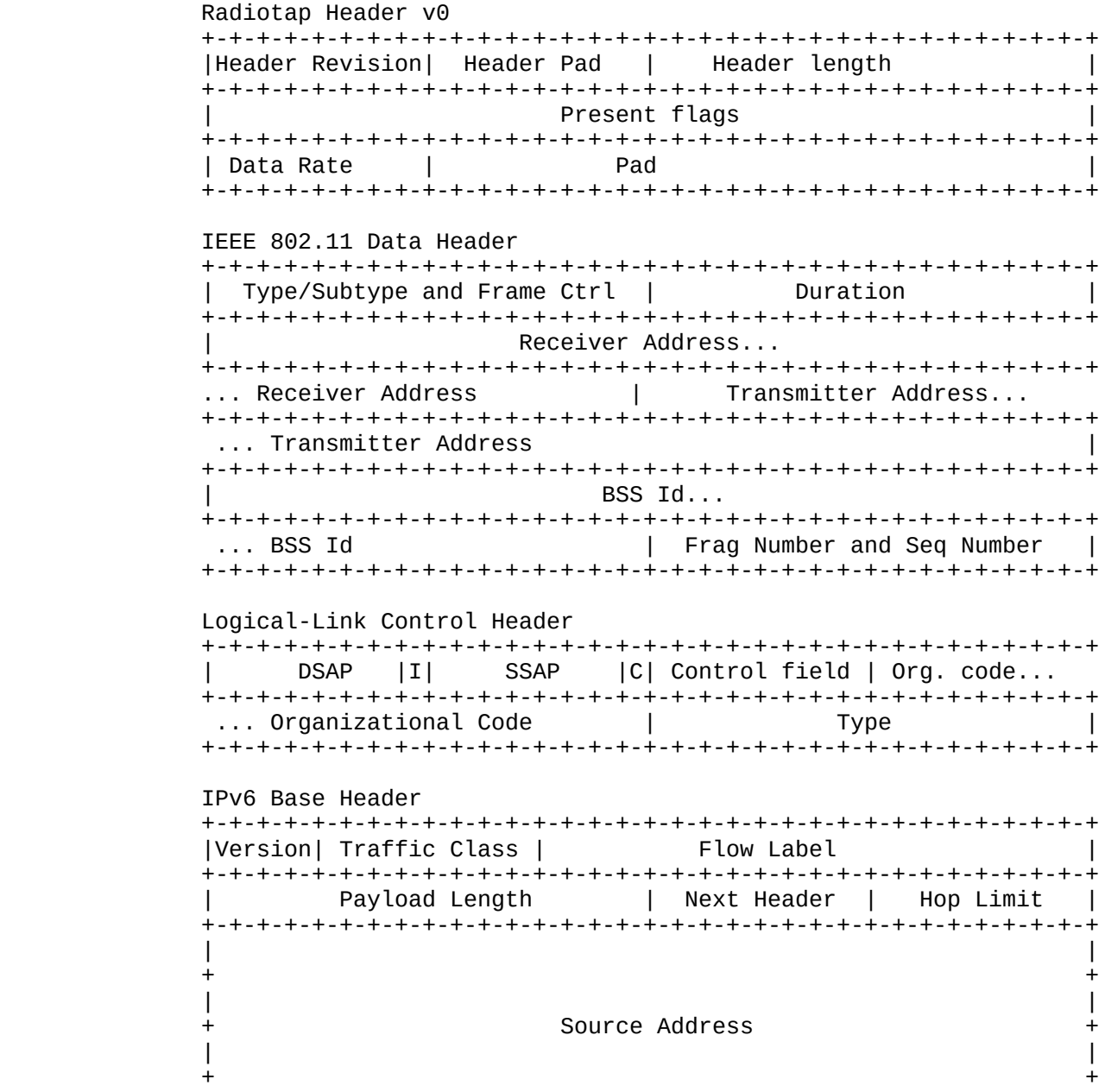
During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

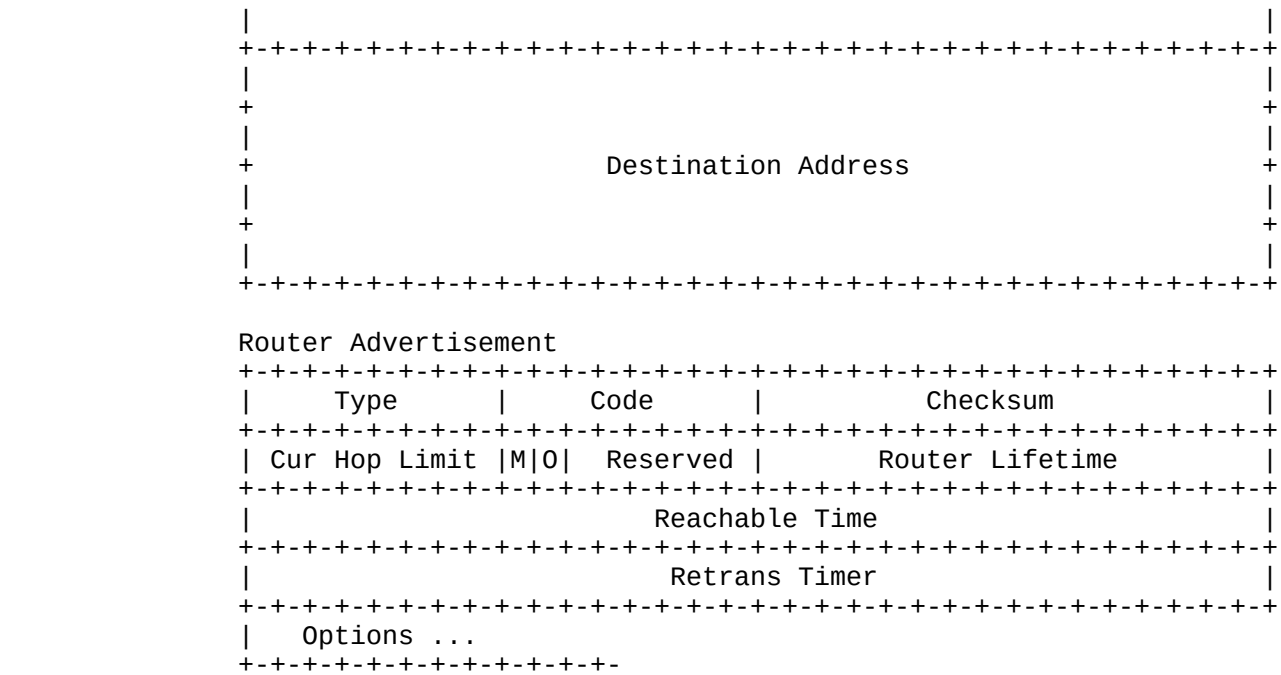
Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

H.1. Capture in Monitor Mode

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

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





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.

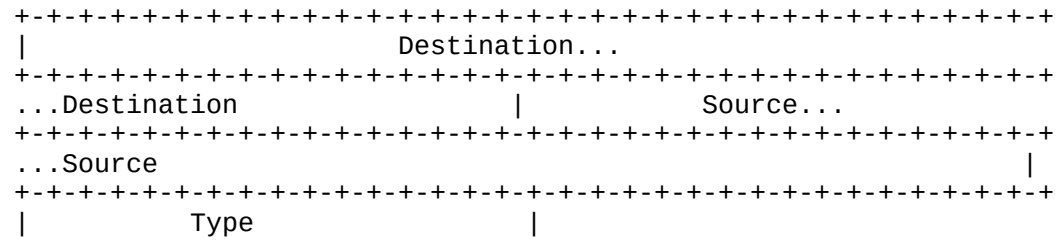
Wireshark) provide additional informations for an IP address, if a geolocalization database is present. In this example, the geolocalization database is absent, and the "GeoIP" information is set to unknown for both source and destination addresses (although the IPv6 source and destination addresses 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.

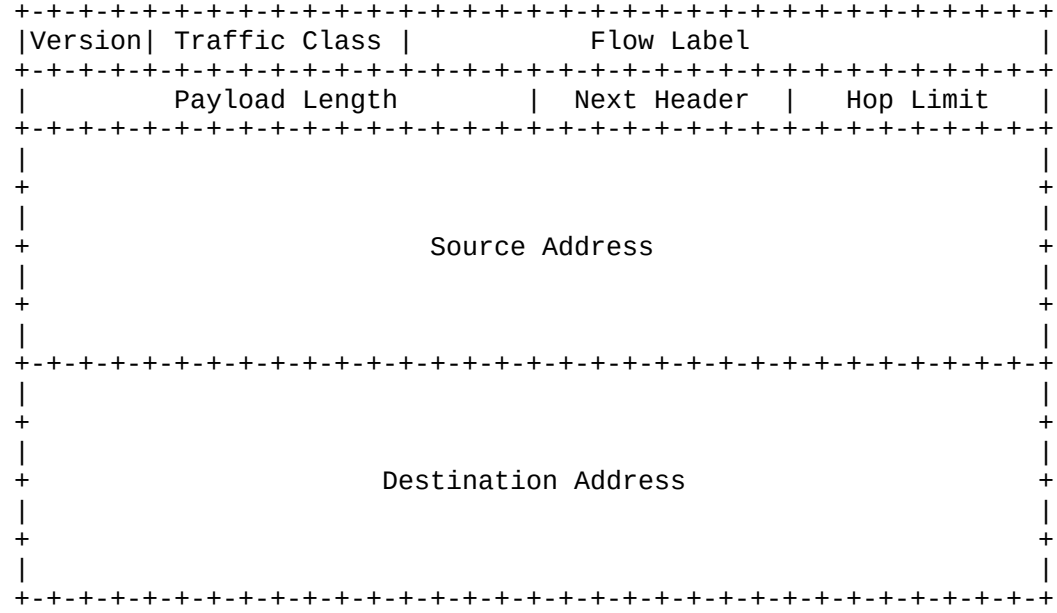
H.2. Capture in Normal Mode

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

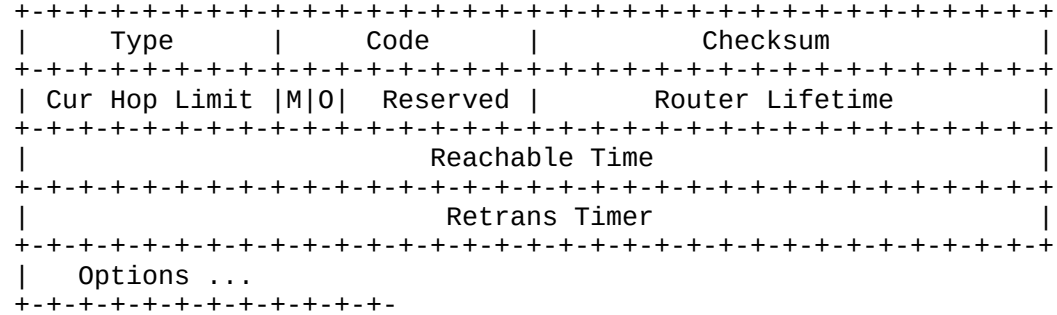
Ethernet II Header



IPv6 Base Header



Router Advertisement



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

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

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

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

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

Appendix I. Extra Terminology

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

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

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

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

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

Authors' Addresses

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

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

Nabil Benamar
Moulay Ismail University
Morocco

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

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

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

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

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr

IPWAVE Working Group
Internet-Draft
Intended status: Standards Track
Expires: June 21, 2019

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

December 18, 2018

Transmission of IPv6 Packets over IEEE 802.11 Networks operating in mode Outside the Context of a Basic Service Set (IPv6-over-80211-OCB) draft-ietf-ipwave-ipv6-over-80211ocb-34

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 June 21, 2019.

Table of Contents

1. Introduction

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

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

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

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

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

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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

that has an "OBU" transceiver. See the definition of the term "OBU" in section Appendix I.

IP-RSU (IP Road-Side Unit): an IP-RSU is situated along the road. 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): A mode of operation in which a STA is not a member of a BSS and does not utilize IEEE Std 802.11 authentication, association, or data confidentiality.

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

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

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

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

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

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

4.2. Frame Format

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

The IPv6 packet transmitted on 802.11-OCB MUST be 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 E), the value of the Type field MUST be set to 0x86DD (IPv6). In the 802.11 header, the value of the Subtype sub-field in the Frame Control field MUST be set to 8 (i.e. 'QoS Data'); the value of the Traffic Identifier (TID) sub-field of the QoS Control field of the 802.11 header MUST be set to binary 001 (i.e. User Priority 'Background', QoS Access Category 'AC_BK').

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers MAY implement an Ethernet Adaptation Layer that translates Ethernet II frames to the 802.11 format and vice versa. An Ethernet Adaptation Layer is described in Section 4.2.1.

4.2.1. Ethernet Adaptation Layer

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

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

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

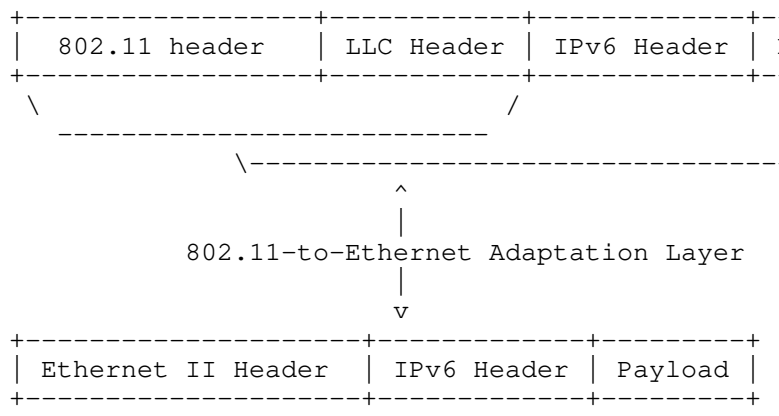


Figure 1: Operation of the Ethernet Adaptation Layer

The Receiver and Transmitter Address fields in the 802.11 header MUST contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header MUST be the same as the value of the Type field in the Ethernet II Header. That value MUST be set to 0x86DD (IPv6).

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

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

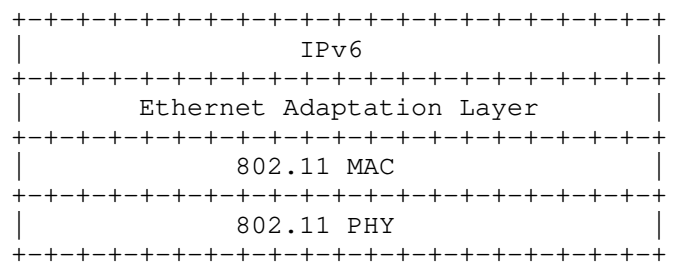


Figure 2: Ethernet Adaptation Layer stacked with other layers

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

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 MAY be formed using an EUI-64 identifier.

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. This mechanism is described in section 5 of [RFC2464].

For privacy, the link-local address MAY be formed according to the mechanisms described in Section 5.2.

4.4. Address Mapping

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

4.4.1. Address Mapping -- Unicast

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

4.4.2. Address Mapping -- Multicast

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

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

4.5. Stateless Autoconfiguration

There are several types of IPv6 addresses [RFC4291], [RFC4193], that MAY be assigned to an 802.11-OCB interface. This section describes the formation of Interface Identifiers for IPv6 addresses of type 'Global' or 'Unique Local'. For Interface Identifiers for IPv6 address of type 'Link-Local' see Section 4.3.

The Interface Identifier for an 802.11-OCB interface is formed using the same rules as the Interface Identifier for an Ethernet interface;

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.

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]. 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].

Semantically opaque Interface Identifiers, instead of meaningful Interface Identifiers derived from a valid and meaningful MAC address ([RFC2464], section 4), MAY be needed in order to avoid certain privacy risks.

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.

In order to avoid these risks, opaque Interface Identifiers MAY be formed according to rules described in [RFC7217]. These opaque Interface Identifiers are formed starting from identifiers different than the MAC addresses, and from cryptographically strong material. Thus, privacy sensitive information is absent from Interface IDs, and it is impossible to calculate the initial value from which the Interface ID was calculated.

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose Interface Identifiers don't change too often. It is RECOMMENDED to use the mechanisms described in RFC 7217 to permit the use of Stable Interface Identifiers 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.

The way Interface Identifiers are used MAY involve risks to privacy, as described in Section 5.1.

4.6. Subnet Structure

A subnet is formed by the external 802.11-OCB interfaces of vehicles that are in close range (not by their in-vehicle interfaces). This subnet MUST use at least the link-local prefix fe80::/10 and the interfaces MUST be assigned IPv6 addresses of type link-local.

The structure of this subnet is ephemeral, in that it is strongly influenced by the mobility of vehicles: the 802.11 hidden node 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 car 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 (a default route is absent), and the addressing peers are equally qualified (impossible to determine that some vehicle owns and distributes addresses to others) the use of link-local addresses is RECOMMENDED.

The Neighbor Discovery protocol (ND) [RFC4861] MUST be used over 802.11-OCB links.

Protocols like Mobile IPv6 [RFC6275] and DNAv6 [RFC6059], which depend on 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 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 Section 5.1.

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].

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 address 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 4.5. This may help mitigate privacy risks to a certain level.

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.

The policy dictating when the MAC address is changed on the 802.11-OCB interface is to-be-determined. For more information on the motivation of this policy please refer to the privacy discussion in Appendix C.

A 'randomized' MAC address has the following characteristics:

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

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

A randomized Interface ID has the same characteristics of a randomized MAC address, except the length in bits. A MAC address SHOULD be of length 48 decimal. An Interface ID SHOULD be of length 64 decimal for all types of IPv6 addresses. In the particular case of IPv6 link-local addresses, the length of the Interface ID MAY be 118 decimal.

5.3. Pseudonym Handling

The demand for privacy protection of vehicles' and drivers' identities, which could be granted by using a pseudonym or alias identity at the same time, may hamper the required confidentiality of messages and trust between participants - especially in safety critical vehicular communication.

- Particular challenges arise when the pseudonymization mechanism used relies on (randomized) re-addressing.
- A proper pseudonymization tool operated by a trusted third party may be needed to ensure both aspects simultaneously (privacy protection on one hand and trust between participants on another hand).
- This is discussed in Section 4.5 and Section 5 of this document.

- Pseudonymity is also discussed in [I-D.ietf-ipwave-vehicular-networking-survey] in its sections 4.2.4 and 5.1.2.

6. IANA Considerations

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

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

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

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

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

8. Acknowledgements

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

[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>.

[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>.

[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>.

[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>.

[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>.

[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>.

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

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

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

9.2. Informative References

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

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

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

[I-D.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-04 (work in progress), November 2018.

[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.

-33: substituted 'movement detection' for 'handover behaviour' in introductory text; removed redundant phrase referring to Security Considerations section; removed the phrase about forming mechanisms being left out, as IP is not much concerned about L2 forming; moved the Pseudonym section from main section to end of Security Considerations section (and clarified 'concurrently'); capitalized SHOULD consider OCB in WiFi multicast problems, and referred to more recent I-D on topic; removed several phrases in a paragraph about oui.txt and MAC presence in IPv6 address, as they are well known info, but clarified the example of privacy risk of Company ID in MAC addresses in public roads; clarified that ND MUST be used over 802.11-OCB.

-32: significantly shortened the relevant ND/OCB paragraph. It now just states ND is used over OCB, w/o detailing.

-31: filled in the section titled "Pseudonym Handling"; removed a 'MAY NOT' phrase about possibility of having other prefix than the LL on the link between cars; shortened and improved the paragraph about Mobile IPv6, now with DNAv6; improved the ND text about ND retransmissions with relationship to packet loss; changed the title of an appendix from 'EPD' to 'Protocol Layering'; improved the 'Aspects introduced by OCB' appendix with a few phrases about the channel use and references.

-30: a clarification on the reliability of ND over OCB and over 802.11.

-29:

o

-28:

- Created a new section 'Pseudonym Handling'.
- removed the 'Vehicle ID' appendix.
- improved the address generation from random MAC address.
- shortened Term IP-RSU definition.
- removed refs to two detail Clauses in IEEE documents, kept just these latter.

-27: part 1 of addressing Human Rights review from IRTF. Removed appendices F.2 and F.3. Shortened definition of IP-RSU. Removed reference to 1609.4. A few other small changes, see diff.

-26: moved text from SLAAC section and from Design Considerations appendix about privacy into a new Privacy Condiderations subsection of the Security section; reformulated the SLAAC and IID sections to stress only LLs can use EUI-64; removed the "GeoIP" wireshark explanation; reformulated SLAAC and LL sections; added brief mention of need of use LLs; clarified text about MAC address changes; dropped pseudonym discussion; changed title of section describing examples of packet formats.

-25: added a reference to 'IEEE Management Information Base', instead of just 'Management Information Base'; added ref to further appendices in the introductory phrases; improved text for IID formation for SLAAC, inserting recommendation for RFC8064 before RFC2464.

From draft-ietf-ipwave-ipv6-over-80211ocb-23 to draft-ietf-ipwave-ipv6-over-80211ocb-24

- Nit: wrote "IPWAVE Working Group" on the front page, instead of "Network Working Group".
- Addressed the comments on 6MAN: replaced a sentence about ND problem with "is used over 802.11-OCB".

From draft-ietf-ipwave-ipv6-over-80211ocb-22 to draft-ietf-ipwave-ipv6-over-80211ocb-23

- No content modifications, but check the entire draft chain on IPv6-only: xml2rfc, submission on tools.ietf.org and datatracker.

From draft-ietf-ipwave-ipv6-over-80211ocb-21 to draft-ietf-ipwave-ipv6-over-80211ocb-22

- Corrected typo, use dash in "802.11-OCB" instead of space.
- Improved the Frame Format section: MUST use QoSData, specify the values within; clarified the Ethernet Adaptation Layer text.

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

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

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

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

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

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

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

- Improved the MTU and fragmentation paragraph.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 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

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

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

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

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

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

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

- 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."

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

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

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

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

- Checked the entire document for a consistent use of terms OBU and OBRU.
- Added note saying that "'p' is a letter identifying the Ammendment".
- Substituted lower case for capitals SHALL or MUST in the Appendices.
- Added reference to RFC7042, helpful in the 3333 explanation. Removed reference to individual submission draft-petrescu-its-scenario-reqs and added reference to draft-ietf-ipwave-vehicular-networking-survey.
- Added figure captions, figure numbers, and references to figure numbers instead of 'below'. Replaced "section Section" with "section" throughout.
- Minor typographical errors.

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

- Significantly shortened the Address Mapping sections, by text copied from RFC2464, and rather referring to it.
- Moved the EPD description to an Appendix on its own.
- Shortened the Introduction and the Abstract.
- Moved the tutorial section of OCB mode introduced to .11, into an appendix.
- Removed the statement that suggests that for routing purposes a prefix exchange mechanism could be needed.
- Removed refs to RFC3963, RFC4429 and RFC6775; these are about ND, MIP/NEMO and oDAD; they were referred in the handover discussion section, which is out.
- Updated a reference from individual submission to now a WG item in IPWAVE: the survey document.
- Added term definition for WiFi.
- Updated the authorship and expanded the Contributors section.
- Corrected typographical errors.

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

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

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

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

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

- Updated references of 802.11-OCB document from -2012 to the IEEE 802.11-2016.
- In the LL address section, and in SLAAC section, added references to 7217 opaque IIDs and 8064 stable IIDs.

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

- Lengthened the title and cleanded the abstract.
- Added text suggesting LLs may be easy to use on OCB, rather than GUAs based on received prefix.
- Added the risks of spoofing and hijacking.
- Removed the text speculation on adoption of the TSA message.
- Clarified that the ND protocol is used.
- Clarified what it means "No association needed".

- Added some text about how two STAs discover each other.
- Added mention of external (OCB) and internal network (stable), in the subnet structure section.
- Added phrase explaining that both .11 Data and .11 QoS Data headers are currently being used, and may be used in the future.
- Moved the packet capture example into an Appendix Implementation Status.
- Suggested moving the reliability requirements appendix out into another document.
- Added a IANA Consiserations section, with content, requesting for a new multicast group "all OCB interfaces".
- 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.
- 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.
- Updated the affiliation of one author.
- Reformulation of some phrases for better readability, and correction of typographical errors.

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

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

- Removed outdated informative references to ETSI documents.
- Added citations to IEEE 1609.2, .3 and .4-2016.
- Minor textual issues.

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

- Keep the previous text on multiple addresses, so remove talk about MIP6, NEMOv6 and MCoA.
- Clarified that a 'Beacon' is an IEEE 802.11 frame Beacon.
- Clarified the figure showing Infrastructure mode and OCB mode side by side.
- Added a reference to the IP Security Architecture RFC.
- Detailed the IPv6-per-channel prohibition paragraph which reflects the discussion at the last IETF IPWAVE WG meeting.
- Added section "Address Mapping -- Unicast".
- Added the ".11 Trailer" to pictures of 802.11 frames.
- Added text about SNAP carrying the Ethertype.
- New RSU definition allowing for it be both a Router and not necessarily a Router some times.
- Minor textual issues.

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

- Replaced almost all occurences of 802.11p with 802.11-OCB, leaving only when explanation of evolution was necessary.
- Shortened by removing parameter details from a paragraph in the Introduction.
- Moved a reference from Normative to Informative.
- Added text in intro clarifying there is no handover spec at IEEE, and that 1609.2 does provide security services.

- Named the contents the fields of the EthernetII header (including the Ethertype bitstring).
- Improved relationship between two paragraphs describing the increase of the Sequence Number in 802.11 header upon IP fragmentation.
- Added brief clarification of "tracking".

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

- Introduced message exchange diagram illustrating differences between 802.11 and 802.11 in OCB mode.
- Introduced an appendix listing for information the set of 802.11 messages that may be transmitted in OCB mode.
- Removed appendix sections "Privacy Requirements", "Authentication Requirements" and "Security Certificate Generation".
- Removed appendix section "Non IP Communications".
- Introductory phrase in the Security Considerations section.
- Improved the definition of "OCB".
- Introduced theoretical stacked layers about IPv6 and IEEE layers including EPD.
- Removed the appendix describing the details of prohibiting IPv6 on certain channels relevant to 802.11-OCB.
- Added a brief reference in the privacy text about a precise clause in IEEE 1609.3 and .4.
- Clarified the definition of a Road Side Unit.
- Removed the discussion about security of WSA (because is non-IP).
- Removed mentioning of the GeoNetworking discussion.
- 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 IEEE Management Information Base (MIB) attribute "OCBActivated" [IEEE-802.11-2016]. Whenever OCBActivated is set to true the IEEE Std 802.11-OCB state is activated. For example, an 802.11 STAtion operating outside the context of a basic service set has the OCBActivated flag set. Such a station, when it has the flag set, uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

Appendix 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. 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:

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

All the nodes in the radio communication range (IP-OBU and IP-RSU) receive all the messages transmitted (IP-OBU and IP-RSU) within the

radio communications range. The eventual conflict(s) are resolved by the MAC CDMA function.

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

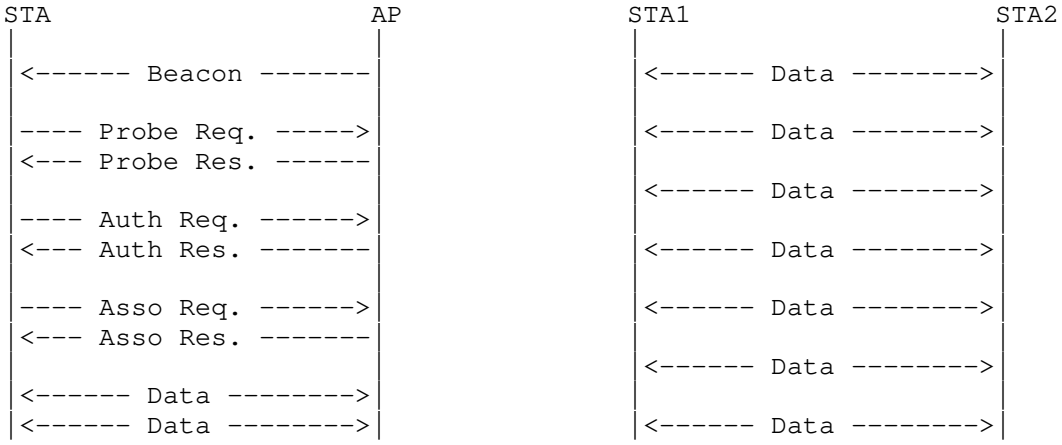


Figure 3: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

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

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

In order to delineate the aspects introduced by 802.11-OCB to 802.11, we refer to the earlier [IEEE-802.11p-2010]. The amendment is concerned with vehicular communications, where the wireless link is

similar to that of Wireless LAN (using a PHY layer specified by 802.11a/b/g/n), but which needs to cope with the high mobility factor inherent in scenarios of communications between moving vehicles, and between vehicles and fixed infrastructure deployed along roads. While 'p' is a letter identifying the Ammendment, just like 'a, b, g' and 'n' are, 'p' is concerned more with MAC modifications, and a little with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a 'p' MAC with an 'a' PHY by operating outside the context of a BSS with OFDM at 5.4GHz and 5.9GHz.

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

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

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

- Operation Outside the Context of a BSS (OCB): the (earlier 802.11p) 802.11-OCB links are operated without a Basic Service Set (BSS). This means that the frames IEEE 802.11 Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always 0xffffffffffff (48 '1' bits, represented as MAC address ff:ff:ff:ff:ff:ff, or otherwise the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by administrator (e.g. 'My-Home-AccessPoint'). The OCB operation -

namely the lack of beacon-based scanning and lack of authentication - should be taken into account when the Mobile IPv6 protocol [RFC6275] and the protocols for IP layer security [RFC4301] are used. The way these protocols adapt to OCB is not described in this document.

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

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

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

- In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong

need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in Section 5. A relevant function is described in documents IEEE 1609.3-2016 [IEEE-1609.3] and IEEE 1609.4-2016 [IEEE-1609.4].

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

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

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

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

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

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

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

Changes needed on the network stack in OCB mode:

- Physical layer:

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

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

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

restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

MAC layer:

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

* No encryption key or method must be used.

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

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

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

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

Appendix E. 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 4. The IP layer operates on top of the EtherType Protocol Discrimination (EPD); this Discrimination layer is described in IEEE Std 802.3-2012; the interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).

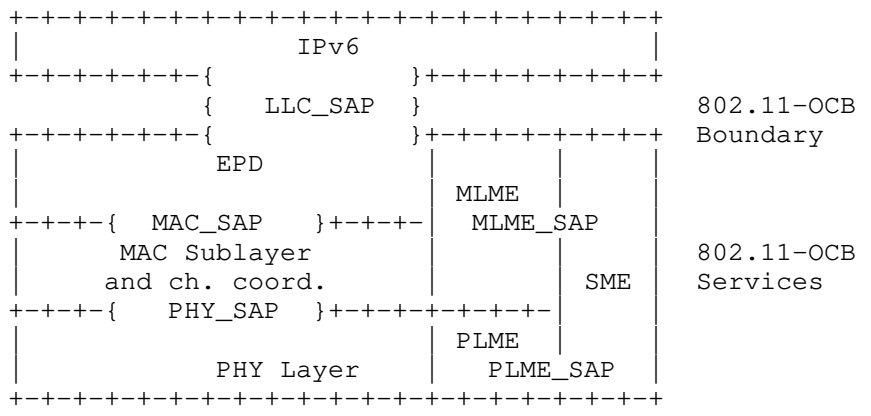


Figure 4: EtherType Protocol Discrimination

Appendix F. Design Considerations

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

Appendix G. IEEE 802.11 Messages Transmitted in OCB mode

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

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;
- The STA may send data frames of subtype Data, Null, QoS Data, and QoS Null.

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

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

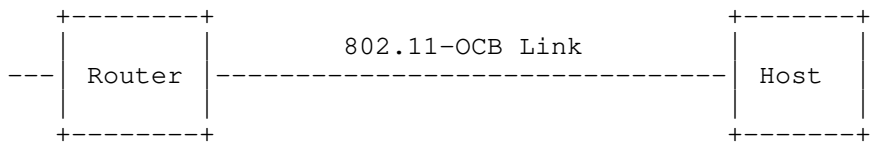


Figure 5: Topology for capturing IP packets on 802.11-OCB

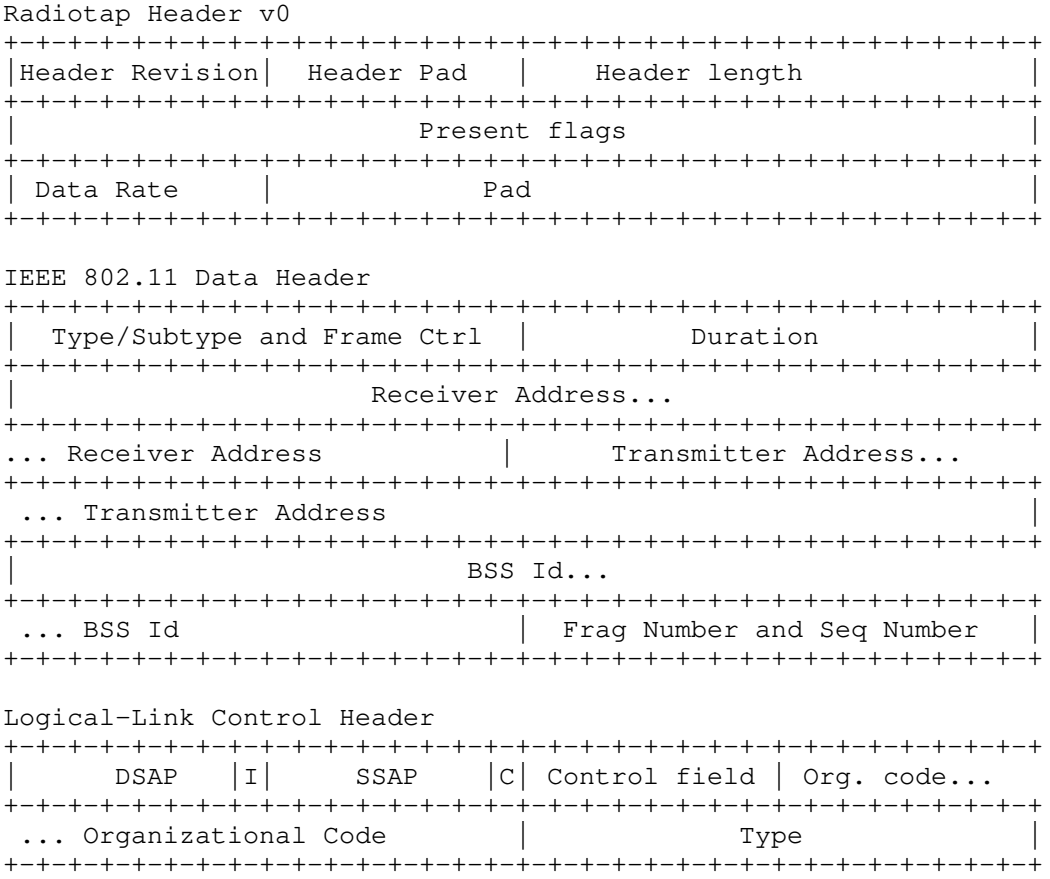
During several capture operations running from a few moments to several hours, no message relevant to the BSSID contexts were captured (no Association Request/Response, Authentication Req/Resp, Beacon). This shows that the operation of 802.11-OCB is outside the context of a BSSID.

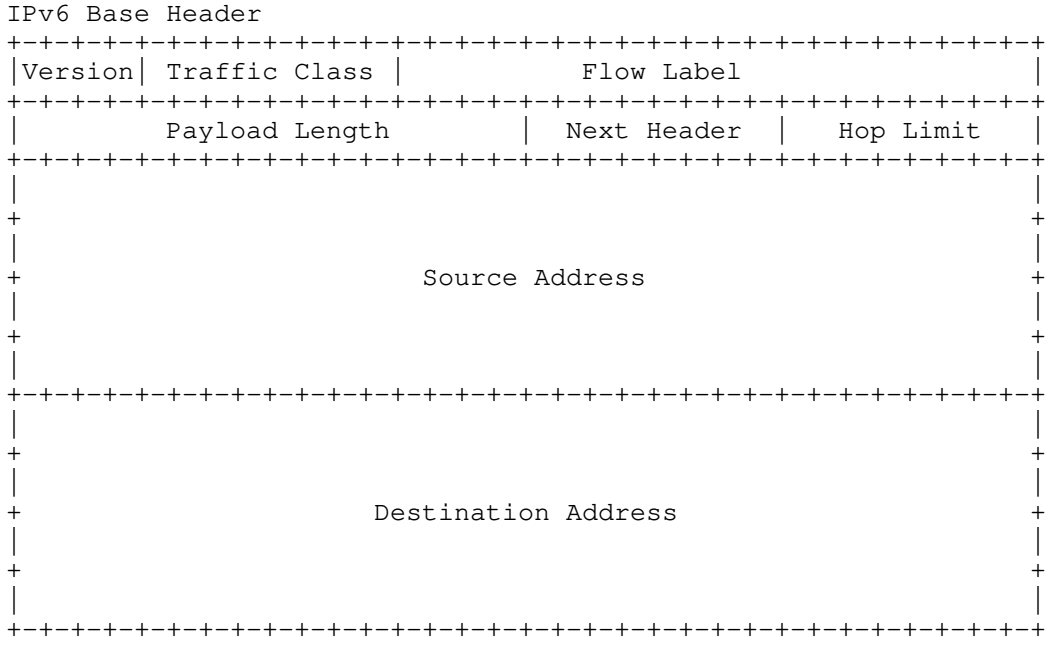
Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

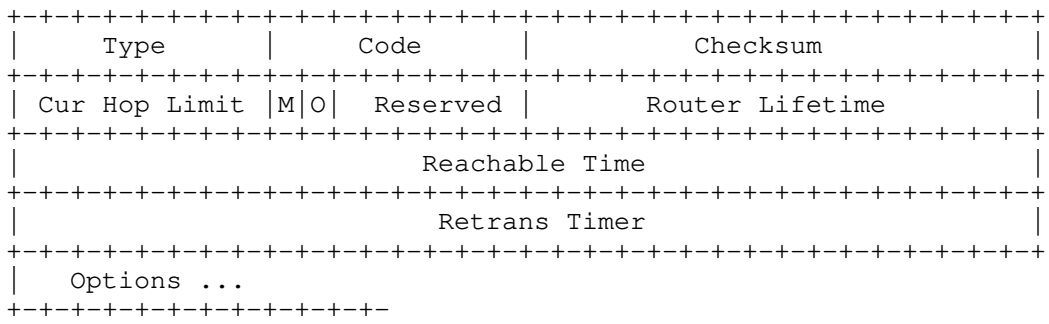
H.1. Capture in Monitor Mode

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

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







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].

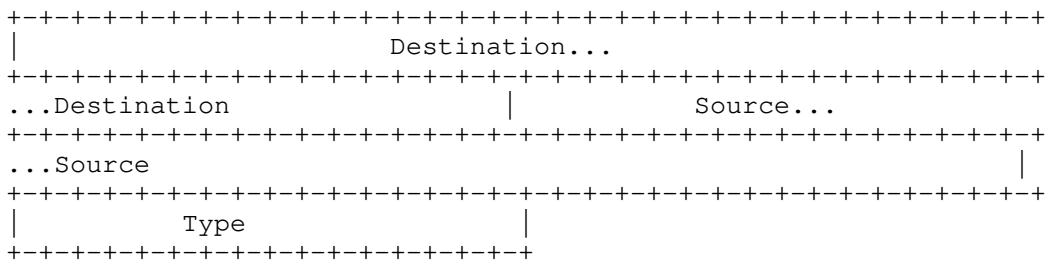
The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1.

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.

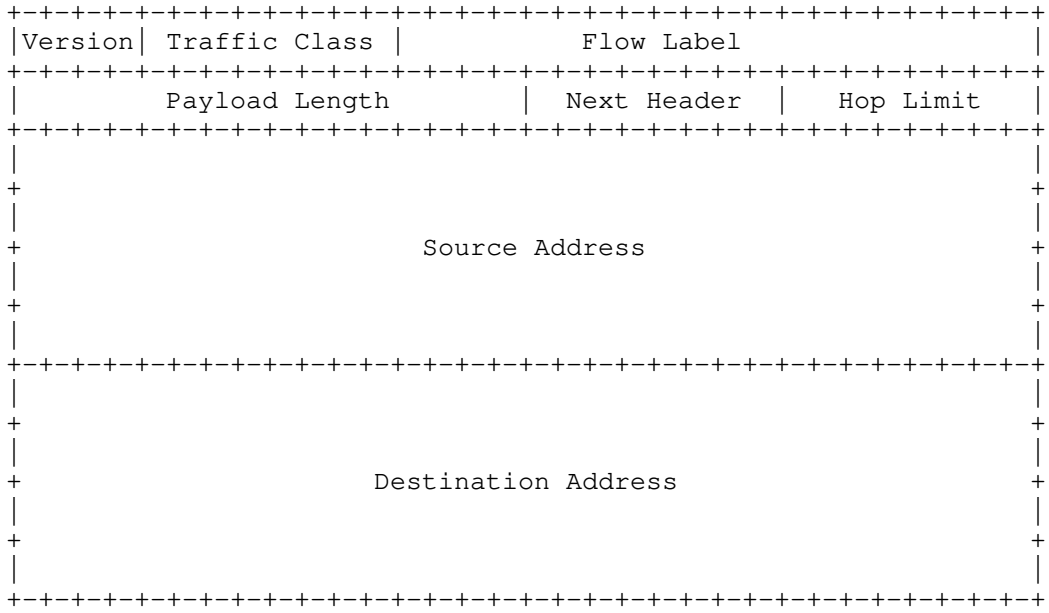
H.2. Capture in Normal Mode

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

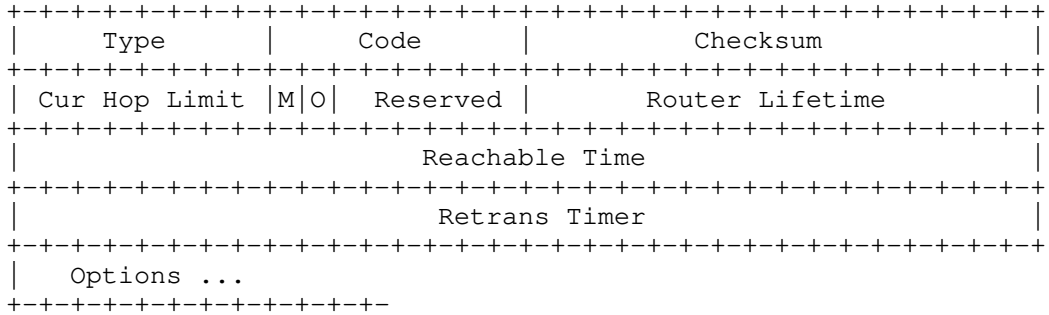
Ethernet II Header



IPv6 Base Header



Router Advertisement



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

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

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

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

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

Appendix I. Extra Terminology

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

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

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

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

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

Authors' Addresses

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

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

Nabil Benamar
Moulay Ismail University
Morocco

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

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

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

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

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr

IPWAVE Working Group
Internet-Draft
Intended status: Informational
Expires: January 3, 2019

J. Jeong, Ed.
Sungkyunkwan University

July 2, 2018

IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-03

Abstract

This document discusses problem statement and use cases 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 vehicle-to-everything (V2X) networking. First, this document surveys use cases using V2V, V2I, and V2X networking. Second, this document analyzes current protocols for vehicular networking and general problems on those current protocols. Third, this document does problem exploration for key aspects in IP-based vehicular networking, such as IPv6 over IEEE 802.11-OCB, IPv6 Neighbor Discovery, Mobility Management, Vehicle Identities Management, Multihop V2X Communications, Multicast, DNS Naming Services, Service Discovery, IPv6 over Cellular Networks, Security and Privacy. For each key aspect, this document discusses problem statement to analyze the gap between the state-of-the-art techniques and requirements in IP-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 January 3, 2019.

Table of Contents

1. Introduction

Vehicular networks have been focused on the driving safety, driving efficiency, and entertainment in road networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC], service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850 - 5.925 GHz band (5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking.

For driving safety services based on the DSRC, IEEE has standardized Wireless Access in Vehicular Environments (WAVE) standards, such as IEEE 802.11p [IEEE-802.11p], IEEE 1609.2 [WAVE-1609.2], IEEE 1609.3 [WAVE-1609.3], and IEEE 1609.4 [WAVE-1609.4]. Note that IEEE 802.11p has been published as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012. Along with these WAVE standards, IPv6 and Mobile IP protocols (e.g., MIPv4 and MIPv6) can be extended to vehicular networks [RFC2460][RFC5944][RFC6275]. Also, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. In addition, ISO has standardized a standard specifying the IPv6 network protocols and services for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].

This document discusses problem statements and use cases related to IP-based vehicular networking for Intelligent Transportation Systems (ITS). This document first surveys the use cases for using V2V and V2I networking in the ITS. Second, for problem statement, this document deals with critical aspects in vehicular networking, such as IPv6 over IEEE 802.11-OCB, IPv6 Neighbor Discovery, Mobility Management, Vehicle Identities Management, Multihop V2X Communications, Multicast, DNS Naming Services, Service Discovery, IPv6 over Cellular Networks, Security and Privacy. For each key 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, with the problem statement, this document suggests demanding key standardization items for the deployment of IPWAVE in road environments. As a consequence, this will make it possible to design a network architecture and protocols for vehicular networking.

2. Terminology

This document uses the following definitions:

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

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

- Road-Side Unit (RSU): A node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, LTE-V2X, etc.) 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.

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

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

- Traffic Control Center (TCC): A node that maintains road infrastructure information (e.g., RSUs, traffic signals, and loop detectors), vehicular traffic statistics (e.g., average vehicle speed and vehicle inter-arrival time per road segment), and vehicle information (e.g., a vehicle’s identifier, position, direction, speed, and trajectory as a navigation path). TCC is included in a vehicular cloud for vehicular networks.

3. Use Cases

This section provides 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).

3.1. V2V

The use cases of V2V networking discussed in this section include

- Context-aware navigation for driving safety and collision avoidance;
- Cooperative adaptive cruise control in an urban roadway;
- Platooning in a highway;
- Cooperative environment sensing.

These four techniques will be important elements for self-driving vehicles.

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

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

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

Cooperative-environment-sensing use cases suggest that vehicles can share environment information from various sensors, such as radars, LiDARs and cameras, mounted on them with other vehicles and pedestrians. [Automotive-Sensing] introduces a millimeter-wave vehicular communication for massive automotive sensing. Data generated by those sensors can be substantially large, and these data shall be routed to different destinations. In addition, from the perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver vehicles. Through cooperative enivronment sensing, driver vehicles can use enivronment information sensed by driverless vehicles for better interaction with environments.

3.2. V2I

The use cases of V2I networking discussed in this section include

- Navigation service;
- Energy-efficient speed recommendation service;
- Accident notification service.

A navigation service, such as the Self-Adaptive Interactive Navigation Tool (called SAINT) [SAINT], using V2I networking interacts with TCC for the global road traffic optimization and can guide individual vehicles for appropriate navigation paths in real time. The enhanced SAINT (called SAINT+) [SAINTplus] can give the fast moving paths for emergency vehicles (e.g., ambulance and fire engine) toward accident spots while providing other vehicles with efficient detour paths.

A TCC can recommend an energy-efficient speed to a vehicle driving in different traffic environments. [Fuel-Efficient] studys fuel-efficient route and speed plans for platooned trucks.

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

3.3. V2X

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

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I2P 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.

4. Analysis for Current Protocols

4.1. Current Protocols for Vehicular Networking

We analyze the current protocols from the follow aspects:

- IP address autoconfiguration;
- Routing;
- Mobility management;
- DNS naming service;
- Service discovery;
- Security and privacy.

4.1.1. IP Address Autoconfiguration

For IP address autoconfiguration, Fazio et al. proposed a vehicular address configuration (VAC) scheme using DHCP where elected leader-vehicles provide unique identifiers for IP address configurations [Address-Autoconf]. Kato et al. proposed an IPv6 address assignment scheme using lane and position information [Address-Assignment]. Baldessari et al. proposed an IPv6 scalable address autoconfiguration scheme called GeoSAC for vehicular networks [GeoSAC]. Wetterwald et al. conducted a comprehensive study of the cross-layer identities management in vehicular networks using multiple access network technologies, which constitutes a fundamental element of the ITS architecture [Identity-Management].

4.1.2. Routing

For 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]. Abrougui et al. presented a gateway discovery scheme for VANET, called Location-Aided Gateway Advertisement and Discovery (LAGAD) mechanism [LAGAD].

4.1.3. Mobility Management

For mobility management, Chen et al. tackled the issue of network fragmentation in VANET environments [IP-Passing-Protocol] by proposing 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. Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support highly mobile vehicles [H-DMM]. [NEMO-LMS] proposed an architecture to enable IP mobility for moving networks using a network-based mobility scheme based on PMIPv6. Chen et al. proposed a network mobility protocol to reduce handoff delay and maintain Internet connectivity to moving vehicles in a highway [NEMO-VANET]. Lee et al. proposed P-NEMO, which is a PMIPv6-based IP mobility management scheme to maintain the Internet connectivity at the vehicle as a mobile network, and provides a make-before-break mechanism when vehicles switch to a new access network [PMIP-NEMO-Analysis]. Peng et al. proposed a novel mobility management scheme for integration of VANET and fixed IP networks [VNET-MM]. Nguyen et al. extended their previous works on a vehicular adapted DMM considering a Software-Defined Networking (SDN) architecture [SDN-DMM].

4.1.4. DNS Naming Service

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

4.1.5. Service Discovery

For service discovery, as a popular existing service discovery protocol, DNS-based Service Discovery (DNS-SD) [RFC6763] with mDNS [RFC6762] provides service discovery. Vehicular ND [ID-Vehicular-ND] proposes an extension of IPv6 ND for the prefix and service discovery.

4.1.6. Security and Privacy

For security and privacy, Fernandez et al. proposed a secure vehicular IPv6 communication scheme using Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [Securing-VCOMM]. Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks [VNET-AAA].

4.2. General Problems

This section describes a vehicular network architecture for V2V and V2I communications. Then it analyzes the limitations of the current protocols for vehicular networking.

4.2.1. Vehicular Network Architecture

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

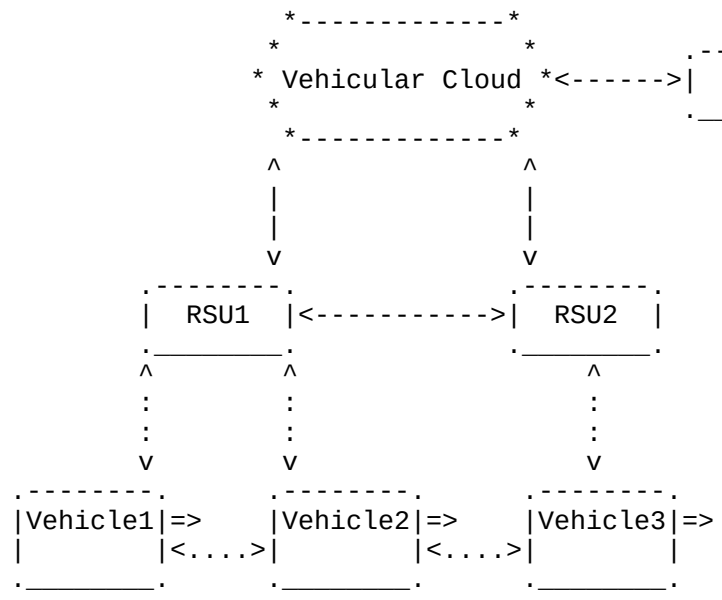


Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

In vehicular networks, unidirectional links exist and must be considered for wireless communications. Also, in the vehicular networks, control plane must be separated from data plane for efficient mobility management and data forwarding. ID/Pseudonym change for privacy requires a lightweight DAD. IP tunneling should be avoided for performance efficiency. The mobility information of a mobile device (e.g., vehicle), such as trajectory, position, speed, and direction, can be used by the mobile device and infrastructure nodes (e.g., TCC and RSU) for the accommodation of proactive protocols because it is usually equipped with a GPS receiver. Vehicles can use the TCC as its Home Network, so the TCC maintains the mobility information of vehicles for location management.

Cespedes et al. proposed a vehicular IP in WAVE called VIP-WAVE for I2V and V2I networking [VIP-WAVE]. The standard WAVE does not support both seamless communications for Internet services and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU), either. To overcome these limitations of the standard WAVE, 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.

Baccelli et al. provided an analysis of the operation of IPv6 as it has been described by the IEEE WAVE standards 1609 [IPv6-WAVE]. This analysis confirms that the use of the standard IPv6 protocol stack in WAVE is not sufficient. It recommebs that the IPv6 addressing assignment should follow considerations for ad-hoc link models, defined in [RFC5889] for nodes' mobility and link variability.

Petrescu et al. proposed the joint IP networking and radio architecture for V2V and V2I communication in [Joint-IP-Networking]. The proposed architecture considers 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. This architecture defines three types of vehicles: Leaf Vehicle, Range Extending Vehicle, and Internet Vehicle.

4.2.1.1. V2I-based Internetworking

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

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

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

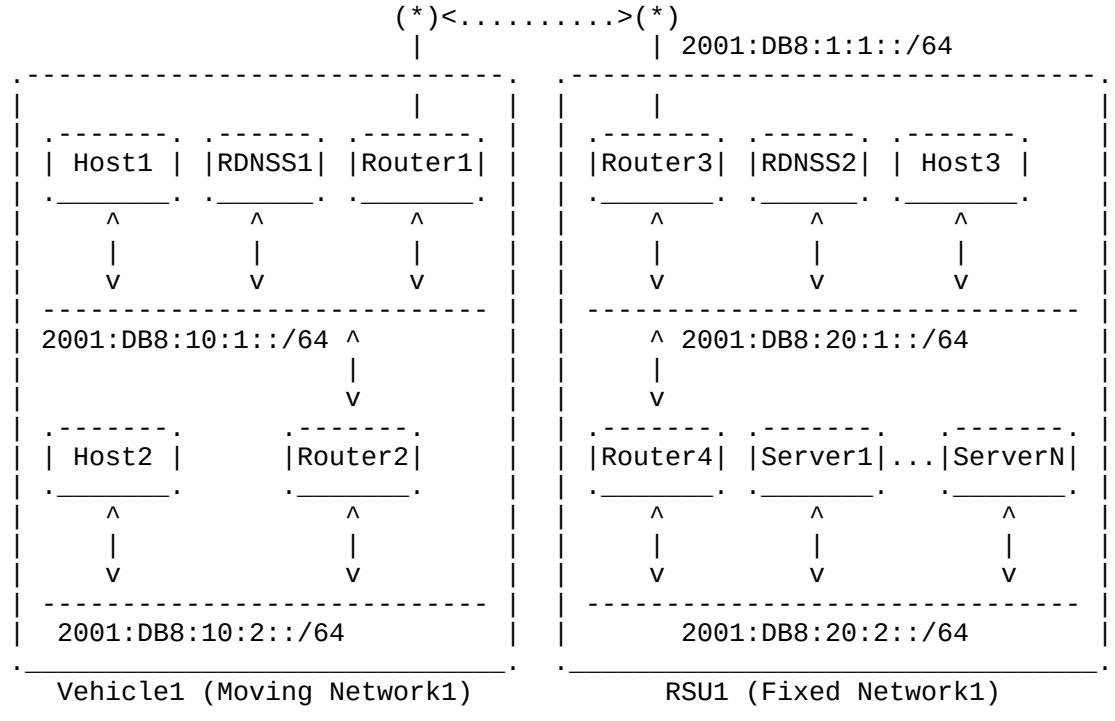


Figure 2: Internetworking between Vehicle Network and RSU Network

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

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

4.2.1.2. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles in Figure 3.

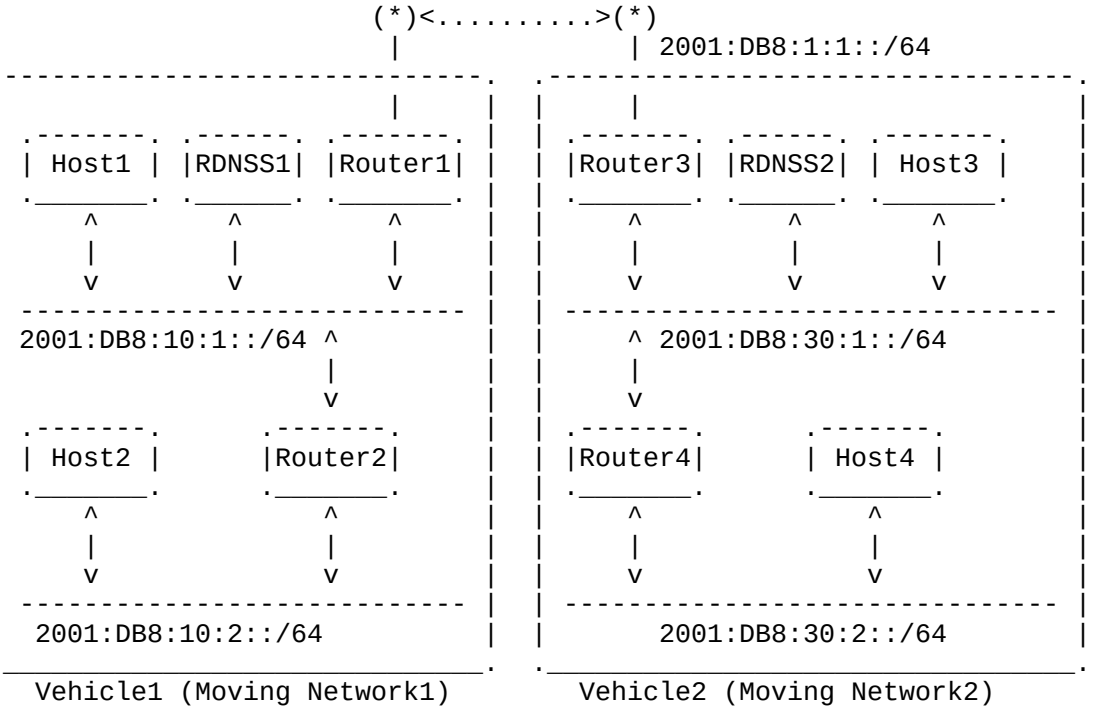


Figure 3: Internetworking between Two Vehicle Networks

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.

The differences between IPWAVE (including Vehicular Ad Hoc Networks (VANET)) and Mobile Ad Hoc Networks (MANET) are as follows:

- IPWAVE is not power-constrained operation;
- Traffic can be sourced or sinked outside of IPWAVE;
- IPWAVE shall support both distributed and centralized operations;
- No "sleep" period operation is required for energy saving.

4.2.2. Latency

The communication delay (i.e., latency) between two vehicular nodes (vehicle and RSU) should be bounded to a certain threshold. For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. The real implementations for such applications are not available, so the feasibility of IP-based safety applications is not tested yet.

4.2.3. Security

Security protects vehicles roaming in road networks from the attacks of malicious vehicular nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious vehicular nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe. Sybil attack, which tries to illude a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. Applications on IP-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.

4.2.4. Pseudonym Handling

For the protection of privacy, pseudonym for a vehicle’s network interface is used, which the interface’s identifier is changed periodically. Such a pseudonym affects an IPv6 address based on the network interface’s identifier, and a transport-layer session with an IPv6 address pair. The pseudonym handling is not implemented and test yet for applications on IP-based vehicular networking.

5. Problem Exploration

5.1. IPv6 over IEEE 802.11-OCB

IPv6 over IEEE 802.11-OCB generally follows the standard IPv6 procedure. [IPv6-over-80211-OCB] specifies several details for IPv6 packets transporting over IEEE 802.11-OCB. Especially, an Ethernet Adaptation (EA) layer is suggested to be inserted between Logical Link Control layer and Network layer. The EA layer is mainly in charge of transforming some parameters between 802.11 MAC layer and IPv6 layer.

5.2. Neighbor Discovery

Neighbor Discovery (ND) [RFC4861] is a core part of the IPv6 protocol suite. This section discusses the need for modifying ND for use with vehicular networking (e.g., V2V and V2I). The vehicles are moving fast within the communication coverage of a vehicular node (e.g., vehicle and RSU). The external link between two vehicular nodes can be used for vehicular networking, as shown in Figure 2 and Figure 3.

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.

5.2.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in WAVE [IPv6-WAVE]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces. However, interference and different levels of transmission power may cause unidirectional links to appear in a WAVE link model.

Also, in an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix are on the same IP link. Hence, there is a relationship between link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. Such a relationship does not hold in a WAVE link model due to node mobility and highly dynamic topology.

Thus, IPv6 ND should be extended to support the concept of a link for an IPv6 prefix in terms of multicast in VANET.

5.2.2. MAC Address Pseudonym

As the ETSI GeoNetworking, 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 should be updated. For the continuity of an end-to-end transport-layer (e.g., TCP, UDP, and SCTP) session, the IP addresses of the transport-layer session should be notified to both the end points and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address.

5.2.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes in within the internal networks of two vehicular nodes (e.g., vehicle and RSU) want to communicate with each other. For this communication, the network prefix dissemination or exchange is required. It is assumed that a vehicular node has an external network interface and its internal network. The standard IPv6 ND needs to be extended for the communication between the internal-network vehicular nodes by letting each of them know the other side’s prefix with a new ND option [ID-Vehicular-ND].

5.2.4. Routing

For Neighbor Discovery in vehicular networks (called vehicular ND), Ad Hoc routing is required for either unicast or multicast in the links in a connected VANET with the same IPv6 prefix [GeoSAC]. Also, a rapid DAD should be supported to prevent or reduce IPv6 address conflicts in such links.

5.3. Mobility Management

The seamless connectivity and timely data exchange between two end points requires an efficient mobility management including location management and handover. 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 DAD, data packet routing, and handover in a proactive manner.

5.4. Vehicle Identity Management

A vehicle can have multiple network interfaces using different access network technologies [Identity-Management]. These multiple network interfaces mean multiple identities. To identify a vehicle with multiple indenties, a Vehicle Identification Number (VIN) can be used as a globally unique vehicle identifier.

To support the seamless connectivity over the multiple identities, a cross-layer network architecture is required with vertical handover functionality [Identity-Management].

5.5. Multihop V2X

Multihop packet forwarding among vehicles in 802.11-OCB mode shows an unfavorable performance due to the common known broadcast-storm problem [Broadcast-Storm]. This broadcast-storm problem can be mitigated by the coordination (or scheduling) of a cluster head in a connected VANET or an RSU in an intersection area, which is a coordinator for the access to wireless channels.

5.6. Multicast

IP multicast in vehicular network environments is especially useful for various services. For instance, an automobile manufacturer can multicast a particular group/class/type of vehicles for service notification. As another example, a vehicle or an RSU can disseminate alert messages in a particular area [Multicast-Alert].

In general IEEE 802 wireless media, some performance issues about multicast are found in [Multicast-Considerations-802]. Since serveral procedures and functions based on IPv6 use multicast for control-plane messages, such as Neighbor Discovery (called ND) and Service Discovery, [Multicast-Considerations-802] describes that the ND process may fail due to unreliable wireless link, causing failure of the DAD process. Also, the Router Advertisement messages can be lost in multicasting.

5.7. DNS Naming Services and Service Discovery

When two vehicular nodes communicate with each other with the DNS name of the partner node, DNS naming service (i.e., DNS name resolution) is required. As shown in Figure 2 and Figure 3, a recursive DNS server (RDNSS) within an internal network can perform such DNS name resolution for the sake of other vehicular nodes.

A service discovery service is required for an application in a vehicular node to search for another application or server in another

vehicular node, which resides in either the same internal network or the other internal network. In V2I or V2V networking, as shown in Figure 2 and Figure 3, such a service discovery service can be provided by either DNS-based Service Discovery (DNS-SD) [RFC6763] with mDNS [RFC6762] or the vehicular ND with a new option for service discovery [ID-Vehicular-ND].

5.8. IPv6 over Cellular Networks

IP has been supported in celluar networks since the time of General Packet Radio Service (GPRS) in the 2nd generation cellular networks of Global System for Mobile communications (2G-GSM) developed and maintained by the 3rd Generation Partnership Project (3GPP). The 2G and 3G-based radio accesses separate end-user data traffic (User Plane) from network transport traffic among network elements (Transport Plane). The two planes run independently in terms of addressing and the IP version. The Transport Plane forms tunnels to transport user data traffic [IPv6-3GPP-Survey].

The 4G-Long-Term-Evolution (4G-LTE) radio access simplifies the complex architecture of GPRS core network by introduing the Evolved Packet Core (EPC). Both 2G/3G and 4G-LTE system use Access Point Name (APN) to bridge user data and outside network. User traffic is transported via Packet Data Protocol (PDP) Contexts in GPRS, and Packet Data Network (PDN) Connections in EPC. Different traffics at a user equipment (UE) side need to connect to different APNs through multiple PDP Contexts or PDN Connections. Each of the context or the connection needs to have its own IP address.

IPv6 is partially supported in 2G/3G and 4G-LTE. In 2G/3G, a UE can be allocated an IPv6 address via two different ways, IPv6 and IPv4v6 PDP Contexts. By IPv4v6 PDP Context, both an IPv4 address and an /64 IPv6 prefix are allocated. In 4G-LTE, the IPv6 address allocation has a different process compared with that in 2G/3G networks. The major difference is that 4G-LTE builds the IP connectivity at the beginning of a UE attachment, whereas the IP connectivity of 2G/3G networks is created on demand. All 3GPP networks (i.e., 2G/3G and 4G-LTE) only support SLAAC address allocation, and do not suggest performing DAD. In addition, 3GPP networks remove link-layer address resolution, e.g., ND Protocol for IPv6, due to the assumption that the GGSN (Gateway GPRS Support Node) in 2G/3G networks or the P-GW (Packet Data Network Gateway) in 4G-LTE network is always the first-hop router for a UE.

Recently, 3GPP has announced a new technical specification, Release 14 (3GPP-R14), which proposes an architecture enhancements for vehicle-to-everything (V2X) services using the modified sidelink interface that originally is designed for the LTE Device-to-Device

(LTE-D2D) communications. 3GPP-R14 regulates that the V2X services only support IPv6 implementation. 3GPP is also investigating and discussing the evolved V2X services in the next generation cellular networks, i.e., 5G new radio (5G-NR), for advanced V2X communications and automated vehicles' applications.

5.8.1. Cellular V2X (C-V2X) Using 4G-LTE

Before 3GPP-R14, some researchers have studied the potential usage of C-V2X communications. For example, [VMaSC-LTE] explores a multihop cluster-based hybrid architecture using both DSRC and LTE for safety message dissemination. Most of the research consider a short message service for safety instead of IP datagram forwarding. In other C-V2X research, the standard IPv6 is assumed.

The 3GPP technical specification [TS-23285-3GPP] states that both IP based and non-IP based V2X messages are supported, and only IPv6 is supported for IP based messages. Moreover, [TS-23285-3GPP] instructes that a UE autoconfigures a link- local IPv6 address by following [RFC4862], but without sending Neighbor Solicitation and Neighbor Advertisement messages for DAD.

5.8.2. Cellular V2X (C-V2X) Using 5G

The emerging services, functions and applications in automotive industry spurs ehhanced V2X (eV2X)-based services in the future 5G era. The 3GPP Technical Report [TS-22886-3GPP] is studying new use cases for V2X using 5G in the future.

5.9. Security and Privacy

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 two vehicular nodes (e.g., vehicle and RSU).

6. Security Considerations

This document discussed security and privacy for IP-based vehicular networking.

The security and privacy 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.

7. Informative References

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

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

[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.

[Broadcast-Storm]
Wisitpongphan, N., K. Tonguz, O., S. Parikh, J., Mudalige, P., Bai, F., and V. Sadekar, "Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks", IEEE Wireless Communications, December 2007.

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

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

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

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

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

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

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

[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.

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

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

[ID-DNSNA]
Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-03 (work in progress), July 2018.

[ID-Vehicular-ND]
Jeong, J., Ed., Shen, Y., Jo, Y., Jeong, J., and J. Lee, "IPv6 Neighbor Discovery for Prefix and Service Discovery in Vehicular Networks", draft-jeong-ipwave-vehicular-neighbor-discovery-03 (work in progress), July 2018.

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

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

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

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

[IPv6-3GPP-Survey]
Soininen, J. and J. Korhonen, "Survey of IPv6 Support in 3GPP Specifications and Implementations", IEEE Communications Surveys & Tutorials, January 2015.

[IPv6-over-80211-OCB]
Petrescu, A., Benamar, N., Haerri, J., Lee, J., and T. Ernst, "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-25 (work in progress), June 2018.

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

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

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

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

[Multicast-Alert]
Camara, D., Bonnet, C., Nikaein, N., and M. Wetterwald, "Multicast and Virtual Road Side Units for Multi Technology Alert Messages Dissemination", IEEE 8th International Conference on Mobile Ad-Hoc and Sensor Systems, October 2011.

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

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

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

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

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

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

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

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

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

[RFC5944] Perkins, C., Ed., "IP Mobility Support in IPv4, Revised", RFC 5944, November 2010.

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

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

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

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

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

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

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

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

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

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

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

[TS-22886-3GPP]
3GPP, "Study on Enhancement of 3GPP Support for 5G V2X Services", 3GPP TS 22.886, June 2018.

[TS-23285-3GPP]
3GPP, "Architecture Enhancements for V2X Services", 3GPP TS 23.285, June 2018.

[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.

[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.

[VMaSC-LTE]
Ucar, S., Ergen, S., and O. Ozkasap, "Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination", IEEE Transactions on Vehicular Technology, April 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.

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

[WAVE-1609.0]
IEEE 1609 Working Group, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture", IEEE Std 1609.0-2013, March 2014.

[WAVE-1609.2]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", IEEE Std 1609.2-2016, March 2016.

[WAVE-1609.3]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services", IEEE Std 1609.3-2016, April 2016.

[WAVE-1609.4]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation", IEEE Std 1609.4-2016, March 2016.

Appendix A. Acknowledgments

This work was supported by 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 Global Research Laboratory Program through the NRF funded by the Ministry of Science and ICT (MSIT) (NRF-2013K1A1A2A02078326) and by the DGIST R&D Program of the MSIT (18-EE-01).

This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

Appendix B. Contributors

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

The following are co-authors of this document:

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

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

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

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

Jerome Haerri
Communication Systems Department
EURECOM
Sophia-Antipolis
France

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

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

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

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

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

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

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

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

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

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

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

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

EMail: Michelle.Wetterwald@gmail.com

Appendix C. Changes from draft-ietf-ipwave-vehicular-networking-02

The following changes are made from draft-ietf-ipwave-vehicular-networking-02:

- The overall structure of the document is reorganized for the problem statement for IPWAVE.

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: May 8, 2019

J. Jeong, Ed.
Sungkyunkwan University

November 4, 2018

IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-07

Abstract

This document discusses the problem statement and use cases on IP-based vehicular networks, which are considered a key component of 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 surveys use cases using V2V, V2I, and V2X networking. Second, it analyzes proposed protocols for IP-based vehicular networking and highlights the limitations and difficulties found on those protocols. Third, it presents a problem exploration for key aspects in IP-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document discusses a problem statement to evaluate the gap between the state-of-the-art techniques and requirements in IP-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 May 8, 2019.

Table of Contents

1. Introduction

Vehicular networking studies have mainly focused on driving safety, driving efficiency, and entertainment in road networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC], service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850 - 5.925 GHz band (5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) networking. Also, the European Union (EU) passed a decision to allocate radio spectrum for safety-related and non-safety-related applications of ITS with the frequency band of 5.875 - 5.905 GHz, which is called Commission Decision 2008/671/EC [EU-2008-671-EC].

For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety services based on the DSRC in terms of standards for the Wireless Access in Vehicular Environments (WAVE) system. L1 and 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. Note that IEEE 802.11p has been published as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) called IEEE 802.11-OCB [IEEE-802.11-OCB] in 2012.

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC5944] and MIPv6 [RFC6275]) can be applied (or easily modified) to vehicular networks. In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. Note that a GN protocol is useful to route an event or notification message to vehicles around a geographic position, such as an acciendent area in a roadway. 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].

This document discusses problem statements and use cases related to IP-based vehicular networking for Intelligent Transportation Systems (ITS), which is denoted as IP Wireless Access in Vehicular Environments (IPWAVE). First, it surveys the use cases for using V2V, V2I, and V2X networking in the ITS. Second, for literature review, it analyzes proposed protocols for IP-based vehicular networking and highlights the limitations and difficulties found on those protocols. Third, for problem statement, it presents a problem exploration with key aspects in IPWAVE, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect of the problem statement, it analyzes the gap between the state-of-the-art techniques and the requirements in IP-based vehicular networking. It also discusses potential topics relevant to IPWAVE Working Group (WG), such as Vehicle Identities Management, Multihop V2X Communications, Multicast, DNS Naming Services, Service Discovery, and IPv6 over Cellular Networks. Therefore, with the problem statement, this document will open a door to develop key protocols for IPWAVE that will be essential to IP-based vehicular networks.

2. Terminology

This document uses the following definitions:

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

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

- Road-Side Unit (RSU): A node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, LTE-V2X, etc.) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in car parking area.

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

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

- Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support the address autoconfiguration and mobility management of them. It has end-to-end connections with RSUs under its control. It maintains a DAD table having the IP addresses of the vehicles moving within the communication coverage of its RSUs.

- Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network nodes.

- 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.

3. Use Cases

This section provides 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).

3.1. V2V

The use cases of V2V networking discussed in this section include

- Context-aware navigation for driving safety and collision avoidance;

- Cooperative adaptive cruise control in an urban roadway;

- Platooning in a highway;

- Cooperative environment sensing.

These four techniques will be important elements for self-driving vehicles.

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

Cooperative Adaptive Cruise Control (CACC) [CA-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.

Cooperative-environment-sensing use cases suggest that vehicles can share environmental information from various vehicle-mounted sensors, such as radars, LiDARs and cameras with other vehicles and pedestrians. [Automotive-Sensing] introduces a millimeter-wave vehicular communication for massive automotive sensing. Data generated by those sensors can be substantially large, and these data shall 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 context.

3.2. V2I

The use cases of V2I networking discussed in this section include

- Navigation service;
- Energy-efficient speed recommendation service;
- Accident notification service.

A navigation service, such as the Self-Adaptive Interactive Navigation Tool (called SAINT) [SAINT], using V2I networking interacts with TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles for appropriate navigation paths in real time. The enhanced SAINT (called SAINT+) [SAINTplus] can give the fast moving paths for emergency vehicles (e.g., ambulance and fire engine) toward accident spots while providing other vehicles with efficient detour paths.

A TCC can recommend an energy-efficient speed to a vehicle driving in different traffic environments. [Fuel-Efficient] studies fuel-efficient route and speed plans for platooned trucks.

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

3.3. V2X

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

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with the access technology with an RSU (e.g., WiFi). Vehicles and pedestrians can also communicate with each other via an RSU that delivers scheduling information for wireless communication in order to save the smartphones' battery through sleeping mode.

For Vehicle-to-Pedestrian (V2P), a vehicle and a pedestrian's smartphone can directly communicate with each other via V2X without the relaying of an RSU as in a V2V scenario such that the pedestrian's smartphone is regarded as a vehicle with a wireless media interface to be able to communicate with another vehicle. In Vehicle-to-Device (V2D), a device can be a mobile node such as bicycle and motorcycle, and can communicate directly with a vehicle for collision avoidance.

4. Analysis for Existing Protocols

4.1. Existing Protocols for Vehicular Networking

We describe some currently existing protocols and proposed solutions with respect to the following aspects that are relevant and essential for vehicular networking:

- IPv6 over 802.11-OCB;
- IP address autoconfiguration;
- Routing;
- Mobility management;
- DNS naming service;
- Service discovery;
- Security and privacy.

4.1.1. IPv6 over 802.11-OCB

For IPv6 packets transporting over IEEE 802.11-OCB, [IPv6-over-802.11-OCB] specifies several details, such as Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. Especially, an Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC layer and IPv6 network layer, which is located between IEEE 802.11-OCB's logical link control layer and IPv6 network layer.

4.1.2. IP Address Autoconfiguration

For IP address autoconfiguration, Fazio et al. proposed a vehicular address configuration (VAC) scheme using DHCP where elected leader-vehicles provide unique identifiers for IP address configurations in vehicles [Address-Autoconf]. Kato et al. proposed an IPv6 address assignment scheme using lane and position information [Address-Assignment]. Baldessari et al. proposed an IPv6 scalable address autoconfiguration scheme called GeoSAC for vehicular networks [GeoSAC]. Wetterwald et al. conducted for heterogeneous vehicular networks (i.e., employing multiple access technologies) a comprehensive study of the cross-layer identities management, which constitutes a fundamental element of the ITS architecture [Identity-Management].

4.1.3. Routing

For 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]. Abrougui et al. presented a gateway discovery scheme for VANET, called Location-Aided Gateway Advertisement and Discovery (LAGAD) mechanism [LAGAD].

4.1.4. Mobility Management

For mobility management, Chen et al. tackled the issue of network fragmentation in VANET environments [IP-Passing-Protocol] by proposing 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 highly variable. Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support highly mobile vehicles [H-DMM]. [NEMO-LMS] proposed an architecture to enable IP mobility for moving networks using a network-based mobility scheme based on PMIPv6. Chen et al. proposed a network mobility protocol to reduce handoff delay and maintain Internet connectivity to moving vehicles in a highway [NEMO-VANET]. Lee et al. proposed P-NEMO, which is a PMIPv6-based IP mobility management scheme to maintain the Internet connectivity at the vehicle as a mobile network, and provides a make-before-break mechanism when vehicles switch to a new access network [PMIP-NEMO-Analysis]. Peng et al. proposed a novel mobility management scheme for integration of VANET and fixed IP networks [VNET-MM]. Nguyen et al. extended their previous works on a vehicular adapted DMM considering a Software-Defined Networking (SDN) architecture [SDN-DMM].

4.1.5. DNS Naming Service

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

4.1.6. Service Discovery

To discover instances of a demanded service in vehicular networks, DNS-based Service Discovery (DNS-SD) [RFC6763] with either DNSNA [ID-DNSNA] or mDNS [RFC6762] provides vehicles with service discovery by using standard DNS queries. Vehicular ND [ID-Vehicular-ND]

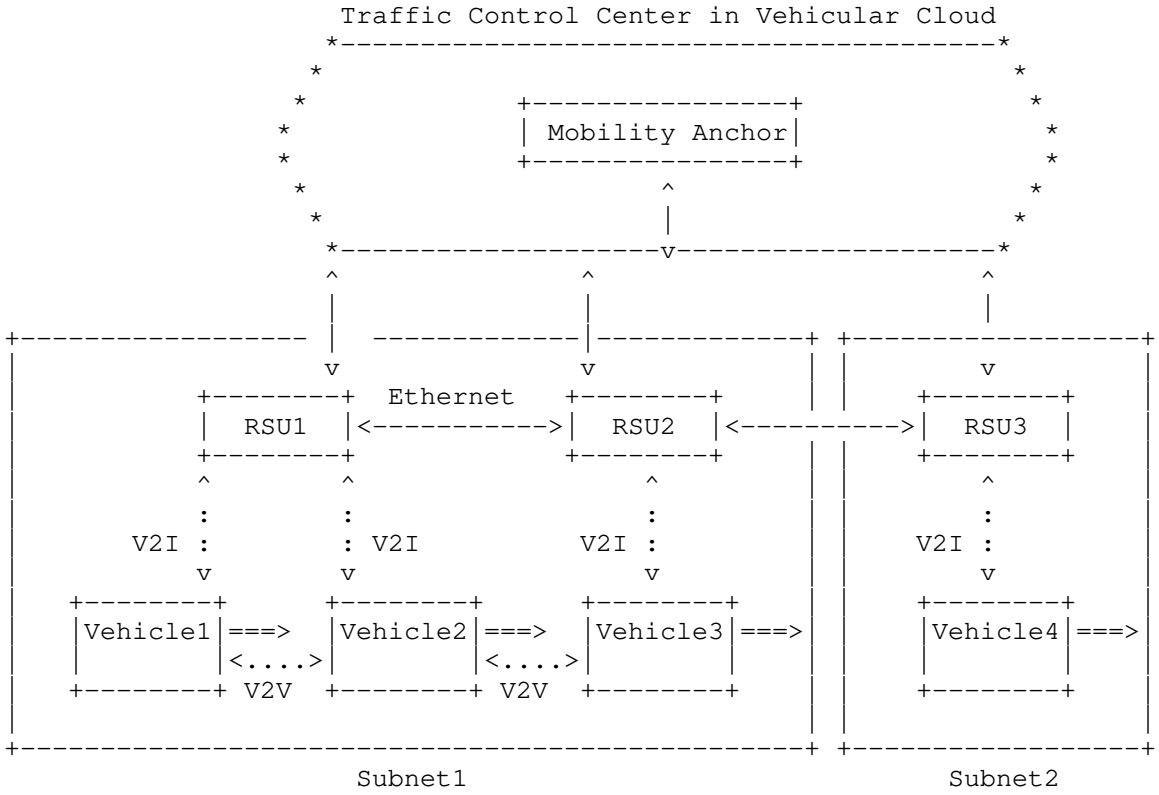
proposes an extension of IPv6 ND for the prefix and service discovery with new ND options [ID-VND-Discovery]. Note that a DNS query for service discovery is unicasted in DNSNA, but it is multicasted in both mDNS and Vehicular ND.

4.1.7. Security and Privacy

For security and privacy, Fernandez et al. proposed a secure vehicular IPv6 communication scheme using Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [Securing-VCOMM]. Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks [VNET-AAA].

4.2. General Problems

This section describes a possible vehicular network architecture for V2V, V2I, and V2X communications. Then it analyzes the limitations of the current protocols for vehicular networking.



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

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

4.2.1. Vehicular Network Architecture

Figure 1 shows a possible architecture for V2I and V2V networking in a road network. It is assumed that RSUs as routers and vehicles with OBU have wireless media interfaces (e.g., IEEE 802.11-OCB, LTE Uu and Device-to-Device (D2D) (also known as PC5 [TS-23.285-3GPP]), Bluetooth, and Light Fidelity (Li-Fi)) for V2I and V2V communication. Also, it is assumed that such 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. Three RSUs (RSU1, RSU2, and RSU3) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of RSUs and vehicles in the road network. A Mobility Anchor (MA) is located in the TCC as its key component for the mobility management of vehicles. Two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to

RSU1, and one vehicle (Vehicle3) is wirelessly connected to RSU2. The wireless networks of RSU1 and RSU2 belong to a multi-link subnet (denoted as Subnet1) with the same network prefix. Thus, these three vehicles are within the same subnet. On the other hand, another vehicle (Vehicle4) is wireless connected to RSU4, belonging to another subnet (denoted as Subnet2). That is, the first three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle3) and the last vehicle (i.e., Vehicle4) are located in the two different subnets. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the same subnet along their IPv6 addresses, which are based on the same prefix. On the other hand, Vehicle3 can communicate with Vehicle4 via RSU2 and RSU3 employing V2I (i.e., V2I2V) communication because they are within the two different subnets along with their IPv6 addresses, which are based on the two different prefixes.

In vehicular networks, unidirectional links exist and must be considered for wireless communications. Also, in the vehicular networks, control plane must be separated from data plane for efficient mobility management and data forwarding using Software-Defined Networking (SDN) [SDN-DMM]. ID/Pseudonym change for privacy requires a lightweight DAD. IP tunneling over the wireless link should be avoided for performance efficiency. The mobility information of a mobile (e.g., vehicle-mounted) device through a GPS receiver in its vehicle, such as trajectory, position, speed, and direction, can be used by the mobile device and infrastructure nodes (e.g., TCC and RSU) for the accommodation of mobility-aware proactive protocols. Vehicles can use the TCC as their Home Network having a home agent for mobility management as in MIPv6 [RFC6275] and Proxy Mobile IPv6 (PMIPv6) [RFC5213], so the TCC maintains the mobility information of vehicles for location management.

Cespedes et al. proposed a vehicular IP in WAVE called VIP-WAVE for I2V and V2I networking [VIP-WAVE]. The standard WAVE does not support both seamless communications for Internet services and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU), either. To overcome these limitations of the standard WAVE, 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 PMIPv6 [RFC5213], and (iii) one-hop and two-hop communications for I2V and V2I networking.

Baccelli et al. provided an analysis of the operation of IPv6 as it has been described by the IEEE WAVE standards 1609 [IPv6-WAVE]. This analysis confirms that the use of the standard IPv6 protocol stack in WAVE is not sufficient. It recommends that the IPv6 addressing

assignment should follow considerations for ad-hoc link models, defined in [RFC5889] for nodes' mobility and link variability.

Petrescu et al. proposed the joint IP networking and radio architecture for V2V and V2I communication in [Joint-IP-Networking]. The proposed architecture considers 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. This architecture defines three types of vehicles: Leaf Vehicle, Range Extending Vehicle, and Internet Vehicle.

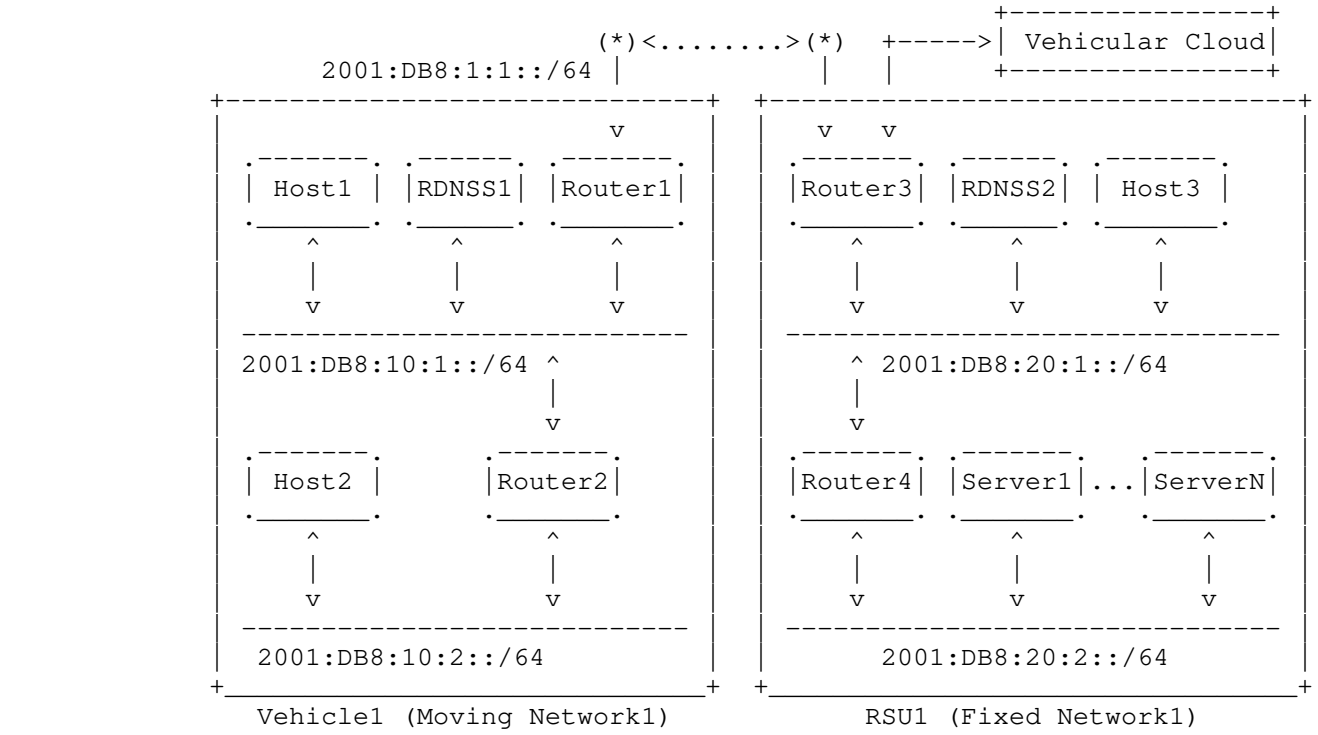


Figure 2: Internetworking between Vehicle Network and RSU Network

4.2.1.1. V2I-based Internetworking

This section discusses the internetworking between a vehicle's moving network and an RSU's fixed network via V2I communication.

As shown in Figure 2, the vehicle's moving network and the RSU's fixed network are self-contained networks having multiple subnets and

having an edge router for the communication with another vehicle or RSU. The method of prefix assignment for each subnet inside the vehicle's mobile network and the RSU's fixed network is out of scope for this document. Internetworking between two internal networks via V2I communication requires an exchange of network prefix and other parameters through a prefix discovery mechanism, such as ND-based prefix discovery [ID-VND-Discovery]. For the ND-based prefix discovery, network prefixs and parameters should be registered into a vehicle's router and an RSU router with an external network interface in advance.

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 Uu and D2D, Bluetooth, and LiFi) and a transmission power level. Note that LiFi is a technology for light-based wireless communication between devices in order to transmit both data and position. 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 have been performed, packets can be transmitted between the vehicle's moving network and the RSU's fixed network. DNS services should be supported to enable name resolution for hosts or servers residing either in the vehicle's moving network or the RSU's fixed network. It is assumed that the DNS names of in-vehicle devices and their service names are registered into a DNS server (i.e., recursive DNS server called RDNSS) in a vehicle or an RSU, as shown in Figure 2. For service discovery, those DNS names and service names can be advertised to neighboring vehicles through either DNS-based service discovery mechanisms [RFC6762][RFC6763][ID-DNSNA] and ND-based service discovery [ID-Vehicular-ND][ID-VND-Discovery]. For the ND-based service discovery, service names should be registered into a vehicle's router and an RSU router with an external network interface in advance. Refer to Section 4.1.5 and Section 4.1.6 for detailed information. For these DNS services, an RDNSS within each internal network of a vehicle or RSU can be used for the hosts or servers.

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.

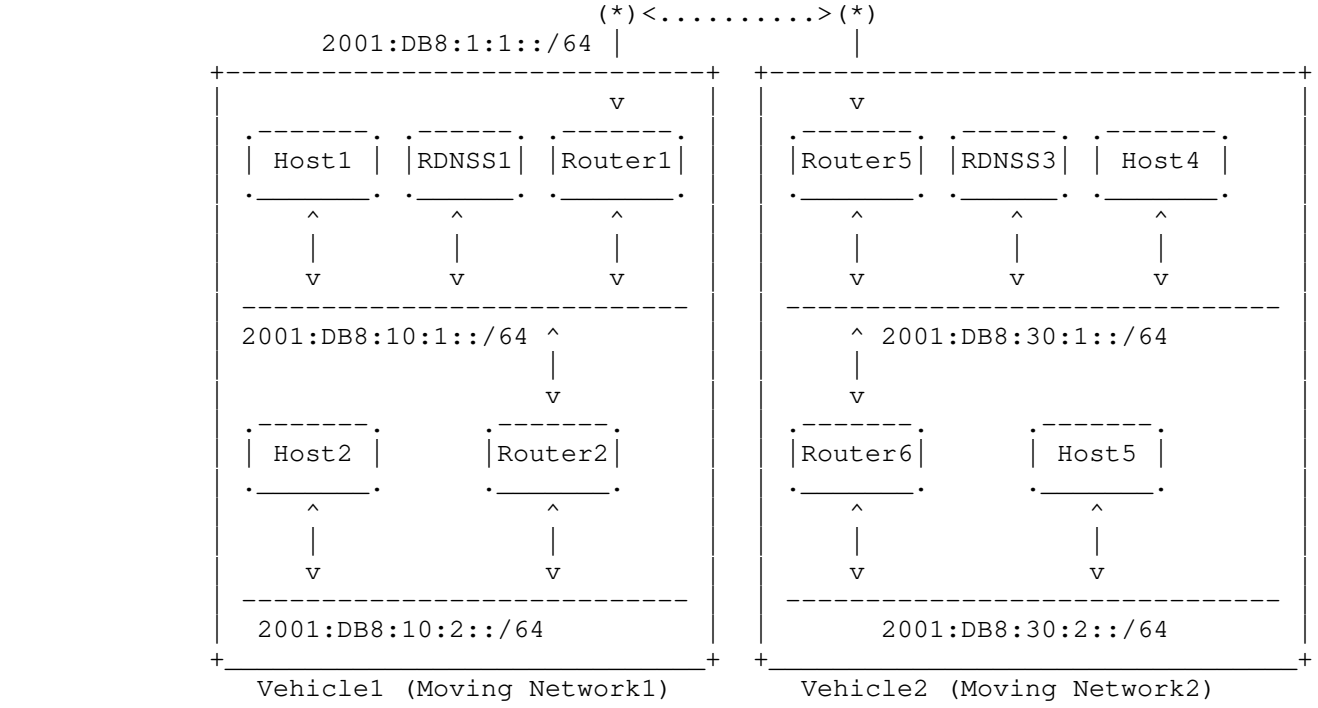


Figure 3: Internetworking between Two Vehicle Networks

4.2.1.2. V2V-based Internetworking

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

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 (RDNSS3), the two hosts (Host4 and Host5), and the two routers (Router5 and Router6).

Vehicle1's Router1 (called mobile router) and Vehicle2's Router5 (called mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking.

The differences between IPWAVE (including Vehicular Ad Hoc Networks (VANET)) and Mobile Ad Hoc Networks (MANET) are as follows:

- IPWAVE is not power-constrained operation;
- Traffic can be sourced or sinked outside of IPWAVE;
- IPWAVE shall support both distributed and centralized operations;
- No "sleep" period operation is required for energy saving.

4.2.2. Latency

The communication delay (i.e., latency) between two vehicular nodes (vehicle and RSU) should be bounded to a certain threshold. For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. The real implementations for such applications are not available, so the feasibility of IP-based safety applications is not tested yet.

4.2.3. Security

Strong security measures shall protect vehicles roaming in road networks from the attacks of malicious nodes, which are controlled by hackers. For safety applications, the cooperation among vehicles is assumed. Malicious nodes may disseminate wrong driving information (e.g., location, speed, and direction) to make driving be unsafe. Sybil attack, which tries to illude a vehicle with multiple false identities, disturbs a vehicle in taking a safe maneuver. Applications on IP-based vehicular networking, which are resilient to such a sybil attack, are not developed and tested yet.

4.2.4. Pseudonym Handling

For the protection of drivers' privacy, pseudonym for a vehicle's network interface should be used, with the help of which the interface's identifier can be changed periodically. Such a pseudonym affects an IPv6 address based on the network interface's identifier, and a transport-layer (e.g., TCP) session with an IPv6 address pair. The pseudonym handling is not implemented and tested yet for applications on IP-based vehicular networking.

5. Problem Exploration

This section discusses key topics for IPWAVE WG, such as neighbor discovery, mobility management, and security & privacy.

5.1. Neighbor Discovery

Neighbor Discovery (ND) [RFC4861] is a core part of the IPv6 protocol suite. This section discusses the need for modifying ND for use with vehicular networking (e.g., V2V, V2I, and V2X). The vehicles are moving fast within the communication coverage of a vehicular node (e.g., vehicle and RSU). The external wireless link between two vehicular nodes can be used for vehicular networking, as shown in Figure 2 and Figure 3.

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 reduce collision probability with other NA messages.

5.1.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in a vehicular wireless link [VIP-WAVE]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces. However, interference and different levels of transmission power may cause unidirectional links to appear in vehicular wireless links. As a result, a new vehicular link model is required for the vehicular wireless link.

There is a relationship between a link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IP link or extended IP links via ND proxy. Note that a subnet prefix can be used by spanning multiple links as a multi-link subnet [RFC6775]. Also, note that IPv6 Stateless Address Autoconfiguration can be performed in the multiple links where each of them is not assigned with a unique subnet prefix, that is, all of them are configured with the same subnet prefix [RFC4861][RFC4862]. A vehicular link model needs to consider a multi-hop VANET over a multi-link subnet. Such a VANET is usually a multi-link subnet consisting of multiple vehicles interconnected by wireless communication range. Such a subnet has a highly dynamic topology over time due to node mobility.

Thus, IPv6 ND should be extended into a Vehicular Neighbor Discovey (VND) [ID-Vehicular-ND] to support the concept of an IPv6 link corresponding to an IPv6 prefix even in a multi-link subnet consisting of multiple vehicles and RSUs that are interconnected with wireless communication range in IP-based vehicular networks.

5.1.2. MAC Address Pseudonym

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 should be updated. For the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, with a mobility management scheme (e.g., MIPv6 and PMIPv6), the new IP address for the transport-layer session should be notified to an appropriate end point, and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address.

5.1.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes in within the internal networks of two vehicular nodes (e.g., vehicle and RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is required. It is assumed that a vehicular node has an external network interface and its internal network. The legacy IPv6 ND [RFC4861] needs to be extended to a vehicular ND (VND) [ID-Vehicular-ND] for the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) of vehicular nodes by letting each of them know the other side's prefix with a new ND option [ID-VND-Discovery]. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without an additional vehicular ad hoc routing protocol [VANET-Geo-Routing].

5.1.4. Routing

For multihop V2V communications in a multi-link subnet (as a connected VANET), a vehicular ad hoc routing protocol (e.g., geographic routing) may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix [VANET-Geo-Routing]. Instead of the vehicular ad hoc routing protocol, Vehicular ND along with a prefix discovery option can be used to let vehicles exchange their prefixes in a multihop fashion

[ID-Vehicular-ND][ID-VND-Discovery]. With the exchanged prefixes, they can compute their routing table (or IPv6 ND's neighbor cache) for the multi-link subnet with a distance-vector algorithm [Intro-to-Algorithms]. Also, an efficient, rapid DAD should be supported to prevent or reduce IPv6 address conflicts in the multi-link subnet by using a DAD optimization [ID-Vehicular-ND][RFC6775] or an IPv6 geographic-routing-based address autoconfiguration [GeoSAC].

5.2. Mobility Management

The seamless connectivity and timely data exchange between two end points requires an efficient mobility management including location management and handover. Most of vehicles are equipped with a GPS receiver as part of a dedicated navigation system or a corresponding smartphone App. In the case where the provided location information is precise enough, well-known temporary degradations in precision may occur due to system configuration or the adverse local environment. This precision is improved thanks to assistance by the RSUs or a cellular system with this navigation system. With this GPS navigator, an efficient mobility management is possible by vehicles periodically reporting their current position and trajectory (i.e., navigation path) to RSUs and a Mobility Anchor (MA) in TCC. The RSUs and MA can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the 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 RSUs along with mobility information [ID-Vehicular-ND].

With the prediction of the vehicle mobility, MA can support RSUs to perform DAD, data packet routing, 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 a proactive manner. Even though a vehicle moves into the wireless link under another RSU belonging to a different subnet, the RSU can proactively perform the DAD for the sake of the vehicle, reducing IPv6 control traffic overhead in the wireless link [ID-Vehicular-ND].

Therefore, with a proactive handover and a multihop DAD in vehicular networks [ID-Vehicular-ND], RSUs can efficiently forward data packets from the wired network (or the wireless network) to a moving destination vehicle along its trajectory along with the MA. Thus, a moving vehicle can communicate with its corresponding vehicle in the vehicular network or a host/server in the Internet along its trajectory.

5.3. Security and Privacy

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular 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 efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., RSU) connected to an authentication server in TCC. Also, Transport Layer Security (TLS) certificates can be used for secure E2E vehicle communications.

For secure V2I communication, a 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, a secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym should be provided to the vehicle; that is, 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 E2E communications between two vehicular nodes (e.g., vehicle and RSU) in terms of transport layer for a long-living higher-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IP addresses, because an adversary can see the change of the MAC and IP addresses and track the vehicle with those addresses.

6. Security Considerations

This document discussed security and privacy for IP-based vehicular networking.

The security and privacy for key components in IP-based vehicular networking, such as neighbor discovery and mobility management, need to be analyzed in depth.

7. Informative References

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

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

[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.

[Broadcast-Storm]
Wisitpongphan, N., K. Tonguz, O., S. Parikh, J., Mudalige, P., Bai, F., and V. Sadekar, "Broadcast Storm Mitigation Techniques in Vehicular Ad Hoc Networks", IEEE Wireless Communications, December 2007.

[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.

[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.

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

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

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

[EU-2008-671-EC]
European Union, "Commission Decision of 5 August 2008 on the Harmonised Use of Radio Spectrum in the 5875 - 5905 MHz Frequency Band for Safety-related Applications of Intelligent Transport Systems (ITS)", EU 2008/671/EC, August 2008.

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

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

[Fuel-Efficient]
van de Hoef, S., H. Johansson, K., and D. V. Dimarogonas, "Fuel-Efficient En Route Formation of Truck Platoons", IEEE Transactions on Intelligent Transportation Systems, January 2018.

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

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

[ID-DNSNA] Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-04 (work in progress), October 2018.

[ID-Vehicular-ND] Xiang, Zhong., Jeong, J., Ed., and Y. Shen, "IPv6 Neighbor Discovery for IP-Based Vehicular Networks", draft-xiang-ipwave-vehicular-neighbor-discovery-00 (work in progress), November 2018.

[ID-VND-Discovery] 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-04 (work in progress), October 2018.

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

[IEEE-802.11-OCB] IEEE 802.11 Working Group, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2016, December 2016.

[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.

[Intro-to-Algorithms] H. Cormen, T., E. Leiserson, C., L. Rivest, R., and C. Stein, "Introduction to Algorithms, 3rd ed.", The MIT Press, 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.

[IPv6-over-802.11-OCB]
Petrescu, A., Benamar, N., Haerri, J., Lee, J., and T. Ernst, "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-30 (work in progress), September 2018.

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

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

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

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

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

[Multicast-Alert]
Camara, D., Bonnet, C., Nikaein, N., and M. Wetterwald, "Multicast and Virtual Road Side Units for Multi Technology Alert Messages Dissemination", IEEE 8th International Conference on Mobile Ad-Hoc and Sensor Systems, October 2011.

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

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

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

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

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

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

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

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

[RFC5944] Perkins, C., Ed., "IP Mobility Support in IPv4, Revised", RFC 5944, November 2010.

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

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

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

[RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

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

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

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 8200, July 2017.

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

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

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

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

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

[TR-22.886-3GPP]
3GPP, "Study on Enhancement of 3GPP Support for 5G V2X Services", 3GPP TS 22.886, June 2018.

[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.

[TS-23.285-3GPP]
3GPP, "Architecture Enhancements for V2X Services", 3GPP TS 23.285, June 2018.

[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.

[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.

[VMaSC-LTE]
Ucar, S., Ergen, S., and O. Ozkasap, "Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination", IEEE Transactions on Vehicular Technology, April 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.

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

[WAVE-1609.0]
IEEE 1609 Working Group, "IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture", IEEE Std 1609.0-2013, March 2014.

[WAVE-1609.2]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", IEEE Std 1609.2-2016, March 2016.

[WAVE-1609.3]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services", IEEE Std 1609.3-2016, April 2016.

[WAVE-1609.4]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation", IEEE Std 1609.4-2016, March 2016.

Appendix A. Relevant Topics to IPWAVE Working Group

This section discusses topics relevant to IPWAVE WG: (i) vehicle identity management; (ii) multihop V2X; (iii) multicast; (iv) DNS naming services and service discovery; (v) IPv6 over cellular networks.

A.1. Vehicle Identity Management

A vehicle can have multiple network interfaces using different access network technologies [Identity-Management]. These multiple network interfaces mean multiple identities. To identify a vehicle with multiple indenties, a Vehicle Identification Number (VIN) can be used as a globally unique vehicle identifier.

To support the seamless connectivity over the multiple identities, a cross-layer network architecture is required with vertical handover functionality [Identity-Management]. Also, an AAA service for multiple identities should be provided to vehicles in an efficient way to allow horizontal handover as well as vertical handover; note that AAA stands for Authentication, Authorization, and Accounting.

A.2. Multihop V2X

Multihop packet forwarding among vehicles in 802.11-OCB mode shows an unfavorable performance due to the common known broadcast-storm problem [Broadcast-Storm]. This broadcast-storm problem can be mitigated by the coordination (or scheduling) of a cluster head in a connected VANET or an RSU in an intersection area, where the cluster head can work as a coodinator for the access to wireless channels.

A.3. Multicast

IP multicast in vehicular network environments is especially useful for various services. For instance, an automobile manufacturer can multicast a particular group/class/type of vehicles for service notification. As another example, a vehicle or an RSU can disseminate alert messages in a particular area [Multicast-Alert].

In general IEEE 802 wireless media, some performance issues about multicast are found in [Multicast-802]. Since several procedures and functions based on IPv6 use multicast for control-plane messages, such as Neighbor Discovery (ND) and Service Discovery, [Multicast-802] describes that the ND process may fail due to unreliable wireless link, causing failure of the DAD process. Also, the Router Advertisement messages can be lost in multicasting.

A.4. DNS Naming Services and Service Discovery

When two vehicular nodes communicate with each other using the DNS name of the partner node, DNS naming service (i.e., DNS name resolution) is required. As shown in Figure 2 and Figure 3, a recursive DNS server (RDNSS) within an internal network can perform such DNS name resolution for the sake of other vehicular nodes.

A service discovery service is required for an application in a vehicular node to search for another application or server in another vehicular node, which resides in either the same internal network or the other internal network. In V2I or V2V networking, as shown in Figure 2 and Figure 3, such a service discovery service can be provided by either DNS-based Service Discovery (DNS-SD) [RFC6763] with mDNS [RFC6762] or the vehicular ND with a new option for service discovery [ID-Vehicular-ND][ID-VND-Discovery].

A.5. IPv6 over Cellular Networks

Recently, 3GPP has announced a set of new technical specifications, such as Release 14 (3GPP-R14), which proposes an architecture enhancements for V2X services using the modified sidelink interface that originally is designed for the LTE-D2D communications. 3GPP-R14 specifies that the V2X services only support IPv6 implementation. 3GPP is also investigating and discussing the evolved V2X services in the next generation cellular networks, i.e., 5G new radio (5G-NR), for advanced V2X communications and automated vehicles' applications.

A.5.1. Cellular V2X (C-V2X) Using 4G-LTE

Before 3GPP-R14, some researchers have studied the potential usage of C-V2X communications. For example, [VMaSC-LTE] explores a multihop cluster-based hybrid architecture using both DSRC and LTE for safety message dissemination. Most of the research considers a short message service for safety instead of IP datagram forwarding. In other C-V2X research, the standard IPv6 is assumed.

The 3GPP technical specification [TS-23.285-3GPP] states that both IP based and non-IP based V2X messages are supported, and only IPv6 is supported for IP based messages. Moreover, [TS-23.285-3GPP] instructs that a UE autoconfigures a link-local IPv6 address by following [RFC4862], but without sending Neighbor Solicitation and Neighbor Advertisement messages for DAD. This is because a unique prefix is allocated to each node by the 3GPP network, so the IPv6 addresses cannot be duplicate.

A.5.2. Cellular V2X (C-V2X) Using 5G

The emerging services, functions, and applications, which are developped in automotive industry, demand reliable and efficient communication infrastructure for road networks. Correspondingly, the support of enhanced V2X (eV2X)-based services by future converged and interoperable 5G systems is required. The 3GPP Technical Report [TR-22.886-3GPP] is studying new use cases and the corresponding service requirements for V2X (including V2V and V2I) using 5G in both infrastructure mode and the sidelink variations in the future.

Appendix B. Changes from draft-ietf-ipwave-vehicular-networking-06

The following changes are made from draft-ietf-ipwave-vehicular-networking-06:

- In Figure 1, a vehicular network architecture is modified to show a vehicular link model in a multi-link subnet with vehicular wireless links.
- In Section 5.1, a Vehicular Neighbor Discovery (VND) [ID-Vehicular-ND] is introduced along with a vehicular link model in a multi-link subnet. In such a subnet, the description of MAC Address Pseudonym, Prefix Dissemination/Exchange, and Routing is clarified.
- In Section 5.2, a proactive handover is introduced for an efficient mobility management with the cooperation among vehicles, RSUs, and MA along with link-layer parameters, such as Received Channel Power Indicator (RCPI).

Appendix C. 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 Global Research Laboratory Program through the NRF funded by the Ministry of Science and ICT (MSIT) (NRF-2013K1A1A2A02078326) and by the DGIST R&D Program of the MSIT (18-EE-01).

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 D. Contributors

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

The following are co-authors of this document:

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

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

Sandra Cespedes
NIC Chile Research Labs
Universidad de Chile
Av. Blanco Encalada 1975
Santiago
Chile

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

Jerome Haerri
Communication Systems Department
EURECOM
Sophia-Antipolis
France

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

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

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

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

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

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

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

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

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

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

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

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

EMail: Michelle.Wetterwald@gmail.com

Author's Address

Jaehoon Paul Jeong (editor)
Department of 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