

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 26, 2018

A. Petrescu
CEA, LIST
N. Benamar
Moulay Ismail University
J. Haerri
Eurecom
J. Lee
Sangmyung University
T. Ernst
YoGoKo
February 22, 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-19.txt](#)

Abstract

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

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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

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

This Internet-Draft will expire on August 26, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	Communication Scenarios where IEEE 802.11-OCB Links are Used	4
4.	IPv6 over 802.11-OCB	5
4.1.	Maximum Transmission Unit (MTU)	5
4.2.	Frame Format	5
4.2.1.	Ethernet Adaptation Layer	5
4.3.	Link-Local Addresses	7
4.4.	Address Mapping	7
4.4.1.	Address Mapping -- Unicast	8
4.4.2.	Address Mapping -- Multicast	8
4.5.	Stateless Autoconfiguration	8
4.6.	Subnet Structure	9
5.	Security Considerations	9
6.	IANA Considerations	10
7.	Contributors	10
8.	Acknowledgements	11
9.	References	11
9.1.	Normative References	11
9.2.	Informative References	14
Appendix A.	ChangeLog	15
Appendix B.	802.11p	23
Appendix C.	Aspects introduced by the OCB mode to 802.11	23
Appendix D.	Changes Needed on a software driver 802.11a to become a 802.11-OCB driver	27
Appendix E.	EtherType Protocol Discrimination (EPD)	28
Appendix F.	Design Considerations	29
F.1.	Vehicle ID	29
F.2.	Reliability Requirements	30
F.3.	Multiple interfaces	30
F.4.	MAC Address Generation	31

Appendix G . IEEE 802.11 Messages Transmitted in OCB mode	31
Appendix H . Implementation Status	32
H.1 . Capture in Monitor Mode	33
H.2 . Capture in Normal Mode	35
Appendix I . Extra Terminology	37
Authors' Addresses	38

[1](#). Introduction

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

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

- o Exceptions due to different operation of IPv6 network layer on 802.11 than on Ethernet. To satisfy these exceptions, this document describes an Ethernet Adaptation Layer between Ethernet headers and 802.11 headers. The Ethernet Adaptation Layer is described [Section 4.2.1](#). The operation of IP on Ethernet is described in [[RFC1042](#)], [[RFC2464](#)] and [[I-D.hinden-6man-rfc2464bis](#)].
- o Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure and handover behaviour. For security and privacy recommendations see [Section 5](#) and [Section 4.5](#). The subnet structure is described in [Section 4.6](#). The handover behaviour on OCB links is not described in this document.

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

[2](#). Terminology

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

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

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

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

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

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

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

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

4.2. Frame Format

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

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

4.2.1. Ethernet Adaptation Layer

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

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

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

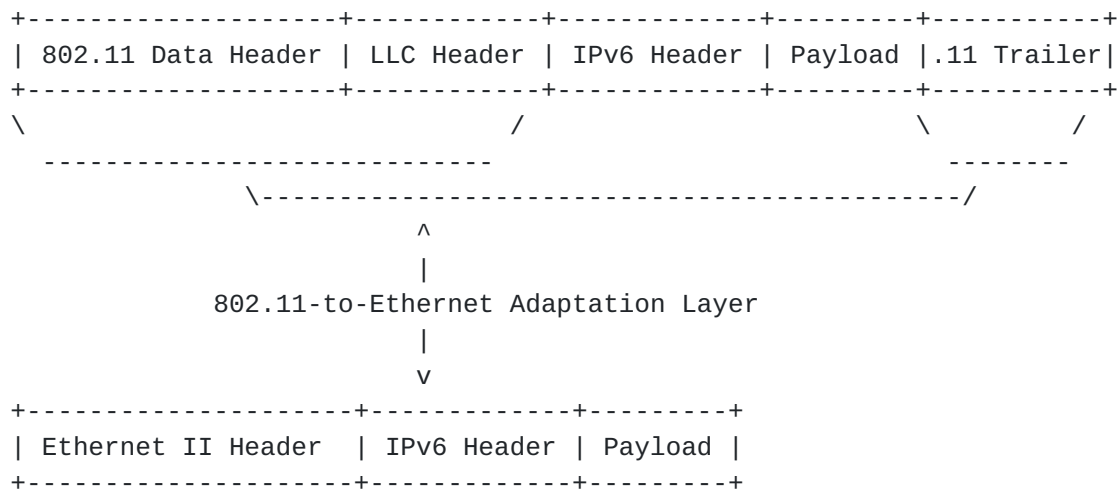


Figure 1: Operation of the Ethernet Adaptation Layer

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

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

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

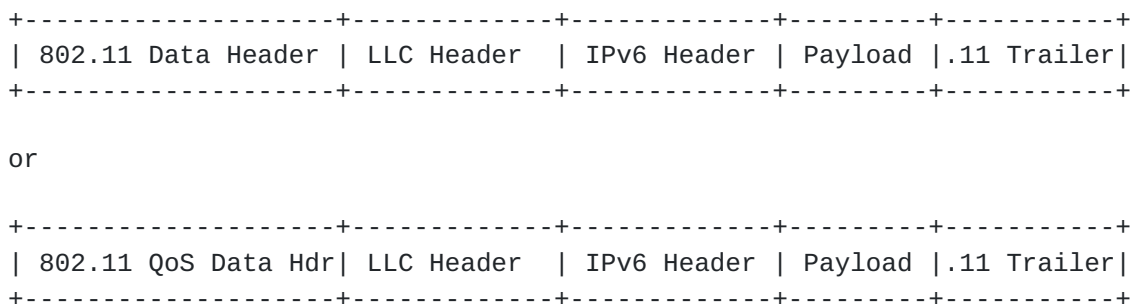


Figure 2: 802.11 Data Header or 802.11 QoS Data Header

The distinction between the two formats is given by the value of the field "Subtype" in the Frame Control Field. The value of the field "Subtype" in the 802.11 Data header is 0x0. The value of the field "Subtype" in the 802.11 QoS header is 8.

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

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

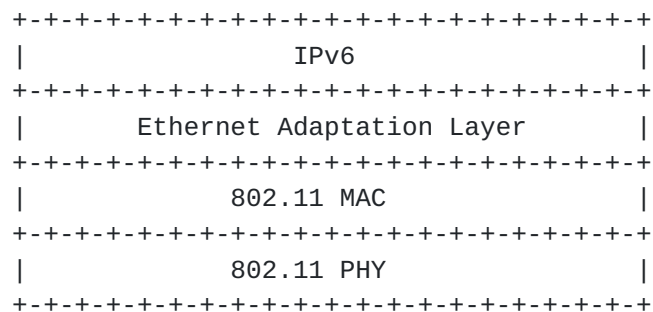


Figure 3: Ethernet Adaptation Layer stacked with other layers

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

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

[4.3.](#) Link-Local Addresses

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

[4.4.](#) Address Mapping

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

4.4.1. Address Mapping -- Unicast

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

4.4.2. Address Mapping -- Multicast

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

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

4.5. Stateless Autoconfiguration

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

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

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

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

4.6. Subnet Structure

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

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

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

The operation of the Mobile IPv6 protocol over 802.11 OCB links is different than on other links. The Movement Detection operation ([section 11.5.1 of \[RFC6275\]](#)) can not rely on Neighbor Unreachability Detection operation of the Neighbor Discovery protocol, for the reason mentioned in the previous paragraph. Also, the 802.11 OCB link layer is not a lower layer that can provide an indication that a link layer handover has occurred. 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 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.ietf-tsvwg-ieee-802-11]

Szigeti, T., Henry, J., and F. Baker, "Diffserv to IEEE 802.11 Mapping", [draft-ietf-tsvwg-ieee-802-11-11](#) (work in progress), December 2017.

[I-D.perkins-intarea-multicast-ieee802]

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

[IEEE-1609.2]

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

[IEEE-1609.3]

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

[IEEE-1609.4]

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

[IEEE-802.11-2016]

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

[IEEE-802.11p-2010]

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

Appendix A. ChangeLog

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-18](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-19](#)

- o Removed the text about fragmentation.
- o Removed the mentioning of WSMP and GeoNetworking.
- o Removed the explanation of the binary representation of the EtherType.
- o Rendered normative the paragraph about unicast and multicast address mapping.

- o Removed paragraph about addressing model, subnet structure and easiness of using LLs.
- o Clarified the Type/Subtype field in the 802.11 Header.
- o Used RECOMMENDED instead of recommended, for the stable interface identifiers.

From [draft-ietf-ipwave-ipv6-over-80211ocb-17](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-18](#)

- o Improved the MTU and fragmentation paragraph.

From [draft-ietf-ipwave-ipv6-over-80211ocb-16](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-17](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-15](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-16](#)

- o Removed the definition of the 'WiFi' term and its occurences. Clarified a phrase that used it in [Appendix C](#) "Aspects introduced by the OCB mode to 802.11".
- o Added more normative words: MUST be 0x86DD, MUST fragment if size larger than MTU, Sequence number in 802.11 Data header MUST be increased.

From [draft-ietf-ipwave-ipv6-over-80211ocb-14](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-15](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-13](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-14](#)

- o Created a new Appendix titled "Extra Terminology" that contains terms DSRC, DSRCs, OBU, RSU as defined outside IETF. Some of them are used in the main Terminology section.
- o Added two paragraphs explaining that ND and Mobile IPv6 have problems working over 802.11 OCB, yet their adaptations is not specified in this document.

From [draft-ietf-ipwave-ipv6-over-80211ocb-12](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-13](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-11](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-12](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-10](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-11](#)

- o Shortened the paragraph on forming/terminating 802.11-OCB links.
- o Moved the draft tsvwg-ieee-802-11 to Informative References.

From [draft-ietf-ipwave-ipv6-over-80211ocb-09](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-10](#)

- o Removed text requesting a new Group ID for multicast for OCB.
- o Added a clarification of the meaning of value "3333" in the section Address Mapping -- Multicast.
- o Added note clarifying that in Europe the regional authority is not ETSI, but "ECC/CEPT based on ENs from ETSI".
- o Added note stating that the manner in which two STations set their communication channel is not described in this document.
- o Added a time qualifier to state that the "each node is represented uniquely at a certain point in time."
- o Removed text "This section may need to be moved" (the "Reliability Requirements" section). This section stays there at this time.
- o In the term definition "802.11-OCB" added a note stating that "any implementation should comply with standards and regulations set in the different countries for using that frequency band."
- o In the RSU term definition, added a sentence explaining the difference between RSU and RSRU: in terms of number of interfaces and IP forwarding.

- o Replaced "with at least two IP interfaces" with "with at least two real or virtual IP interfaces".
- o Added a term in the Terminology for "OBU". However the definition is left empty, as this term is defined outside IETF.
- o Added a clarification that it is an OBU or an OBRU in this phrase "A vehicle embarking an OBU or an OBRU".
- o Checked the entire document for a consistent use of terms OBU and OBRU.
- o Added note saying that "'p' is a letter identifying the Amendment".
- o Substituted lower case for capitals SHALL or MUST in the Appendices.
- o Added reference to [RFC7042](#), helpful in the 3333 explanation. Removed reference to individual submission [draft-petrescu-its-scenario-reqs](#) and added reference to [draft-ietf-ipwave-vehicular-networking-survey](#).
- o Added figure captions, figure numbers, and references to figure numbers instead of 'below'. Replaced "section Section" with "section" throughout.
- o Minor typographical errors.

From [draft-ietf-ipwave-ipv6-over-80211ocb-08](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-09](#)

- o Significantly shortened the Address Mapping sections, by text copied from [RFC2464](#), and rather referring to it.
- o Moved the EPD description to an Appendix on its own.
- o Shortened the Introduction and the Abstract.
- o Moved the tutorial section of OCB mode introduced to .11, into an appendix.
- o Removed the statement that suggests that for routing purposes a prefix exchange mechanism could be needed.
- o Removed refs to [RFC3963](#), [RFC4429](#) and [RFC6775](#); these are about ND, MIP/NEMO and oDAD; they were referred in the handover discussion section, which is out.

- o Updated a reference from individual submission to now a WG item in IPWAVE: the survey document.
- o Added term definition for WiFi.
- o Updated the authorship and expanded the Contributors section.
- o Corrected typographical errors.

From [draft-ietf-ipwave-ipv6-over-80211ocb-07](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-08](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-06](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-07](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-05](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-06](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-04](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-05](#)

- o Lengthened the title and cleaned the abstract.

- o Added text suggesting LLs may be easy to use on OCB, rather than GUAs based on received prefix.
- o Added the risks of spoofing and hijacking.
- o Removed the text speculation on adoption of the TSA message.
- o Clarified that the ND protocol is used.
- o Clarified what it means "No association needed".
- o Added some text about how two STAs discover each other.
- o Added mention of external (OCB) and internal network (stable), in the subnet structure section.
- o Added phrase explaining that both .11 Data and .11 QoS Data headers are currently being used, and may be used in the future.
- o Moved the packet capture example into an [Appendix I](#) Implementation Status.
- o Suggested moving the reliability requirements appendix out into another document.
- o Added a IANA Consiserations section, with content, requesting for a new multicast group "all OCB interfaces".
- o Added new OBU term, improved the RSU term definition, removed the ETTC term, replaced more occurences of 802.11p, 802.11 OCB with 802.11-OCB.
- o References:
 - * Added an informational reference to ETSI's IPv6-over-GeoNetworking.
 - * Added more references to IETF and ETSI security protocols.
 - * Updated some references from I-D to RFC, and from old RFC to new RFC numbers.
 - * Added reference to multicast extensions to IPsec architecture RFC.
 - * Added a reference to 2464-bis.
 - * Removed FCC informative references, because not used.

- o Updated the affiliation of one author.
- o Reformulation of some phrases for better readability, and correction of typographical errors.

From [draft-ietf-ipwave-ipv6-over-80211ocb-03](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-04](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-02](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-03](#)

- o Keep the previous text on multiple addresses, so remove talk about MIP6, NEMOV6 and MCoA.
- o Clarified that a 'Beacon' is an IEEE 802.11 frame Beacon.
- o Clarified the figure showing Infrastructure mode and OCB mode side by side.
- o Added a reference to the IP Security Architecture RFC.
- o Detailed the IPv6-per-channel prohibition paragraph which reflects the discussion at the last IETF IPWAVE WG meeting.
- o Added section "Address Mapping -- Unicast".
- o Added the ".11 Trailer" to pictures of 802.11 frames.
- o Added text about SNAP carrying the Ethertype.
- o New RSU definition allowing for it be both a Router and not necessarily a Router some times.
- o Minor textual issues.

From [draft-ietf-ipwave-ipv6-over-80211ocb-01](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-02](#)

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

From [draft-ietf-ipwave-ipv6-over-80211ocb-00](#) to [draft-ietf-ipwave-ipv6-over-80211ocb-01](#)

- o Introduced message exchange diagram illustrating differences between 802.11 and 802.11 in OCB mode.
- o Introduced an appendix listing for information the set of 802.11 messages that may be transmitted in OCB mode.
- o Removed appendix sections "Privacy Requirements", "Authentication Requirements" and "Security Certificate Generation".
- o Removed appendix section "Non IP Communications".
- o Introductory phrase in the Security Considerations section.
- o Improved the definition of "OCB".
- o Introduced theoretical stacked layers about IPv6 and IEEE layers including EPD.
- o Removed the appendix describing the details of prohibiting IPv6 on certain channels relevant to 802.11-OCB.
- o Added a brief reference in the privacy text about a precise clause in IEEE 1609.3 and .4.
- o Clarified the definition of a Road Side Unit.

- o Removed the discussion about security of WSA (because is non-IP).
- o Removed mentioning of the GeoNetworking discussion.
- o Moved references to scientific articles to a separate 'overview' draft, and referred to it.

Appendix B. 802.11p

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

Appendix C. Aspects introduced by the OCB mode to 802.11

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

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

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

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

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

The message exchange diagram in Figure 4 illustrates a comparison between traditional 802.11 and 802.11 in 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](#).

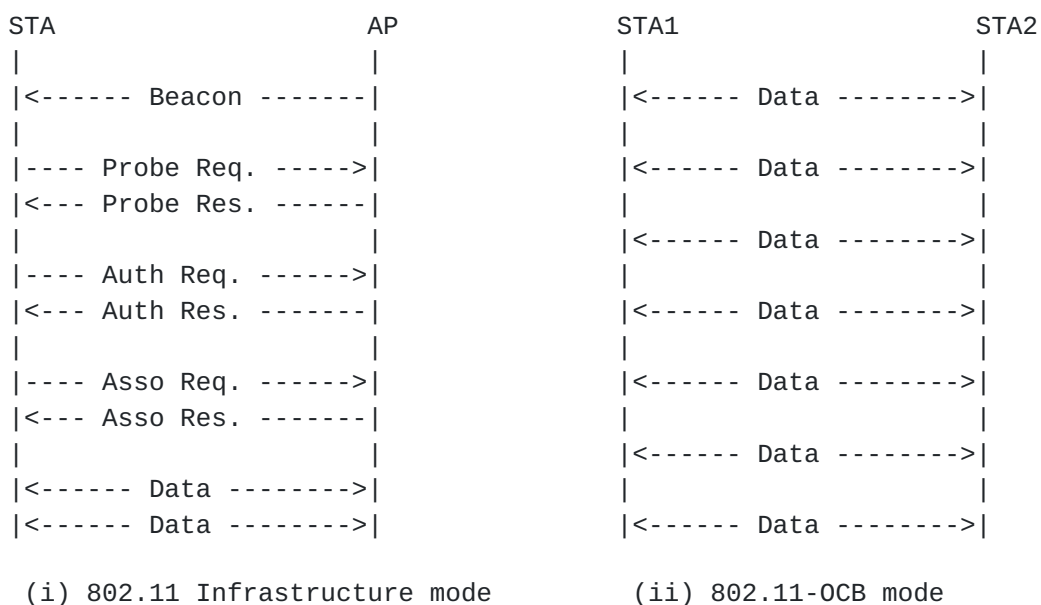


Figure 4: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)

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

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

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

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

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

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

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

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

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

- o Timing Advertisement: is a new message defined in 802.11-OCB, which does not exist in 802.11a/b/g/n. This message is used by stations to inform other stations about the value of time. It is similar to the time as delivered by a GNSS system (Galileo, GPS, ...) or by a cellular system. This message is optional for implementation.
- o Frequency range: this is a characteristic of the PHY layer, with almost no impact on the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, ECC/CEPT based on ENs from ETSI, FCC, etc.); as part of the regulation process, specific applications are associated with specific frequency ranges. In the case of 802.11-OCB, the regulator associates a set of frequency ranges, or slots within a band, to the use of applications of vehicular communications, in a band known as "5.9GHz". The 5.9GHz band is different from the 2.4GHz and 5GHz bands used by Wireless LAN. However, as with Wireless LAN, the operation of 802.11-OCB in "5.9GHz" bands is exempt from owning a license in EU (in US the 5.9GHz is a licensed band of spectrum; for the fixed infrastructure an explicit FCC authorization is required; for an on-board device a 'licensed-by-rule' concept applies: rule certification conformity is required.) Technical conditions are different than those of the bands "2.4GHz" or "5GHz". The allowed power levels, and implicitly the maximum allowed distance between vehicles, is of 33dBm for 802.11-OCB (in Europe), compared to 20 dBm for Wireless LAN 802.11a/b/g/n; this leads to a maximum distance of approximately 1km, compared to approximately 50m. Additionally, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in US) and on the use of frequencies for Intelligent Transportation Systems (in EU), compared to Wireless LAN (802.11a/b/g/n).
- o 'Half-rate' encoding: as the frequency range, this parameter is related to PHY, and thus has not much impact on the interface between the IP layer and the MAC layer.
- o In vehicular communications using 802.11-OCB links, there are strong privacy requirements with respect to addressing. While the 802.11-OCB standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong

need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in [Section 5](#). A relevant function is described in IEEE 1609.3-2016 [[IEEE-1609.3](#)], clause 5.5.1 and IEEE 1609.4-2016 [[IEEE-1609.4](#)], clause 6.7.

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

[Appendix D](#). Changes Needed on a software driver 802.11a to become a 802.11-OCB driver

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

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

- o The PHY entity shall be an orthogonal frequency division multiplexing (OFDM) system. It must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11-OCB layer, in France: 5875MHz to 5925MHz.
- o The OFDM system must provide a "half-clocked" operation using 10 MHz channel spacings.
- o The chip transmit spectrum mask must be compliant to the "Transmit spectrum mask" from the IEEE 802.11p amendment (but experimental environments tolerate otherwise).
- o The chip should be able to transmit up to 44.8 dBm when used by the US government in the United States, and up to 33 dBm in Europe; other regional conditions apply.

Changes needed on the network stack in OCB mode:

- o Physical layer:
 - * The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.
 - * The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).

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

MAC layer:

- * All management frames (beacons, join, leave, and others) emission and reception must be disabled except for frames of subtype Action and Timing Advertisement (defined below).
- * No encryption key or method must be used.
- * Packet emission and reception must be performed as in ad-hoc mode, using the wildcard BSSID (ff:ff:ff:ff:ff:ff).
- * The functions related to joining a BSS (Association Request/Response) and for authentication (Authentication Request/Reply, Challenge) are not called.
- * The beacon interval is always set to 0 (zero).
- * Timing Advertisement frames, defined in the amendment, should be supported. The upper layer should be able to trigger such frames emission and to retrieve information contained in received Timing Advertisements.

Appendix E. EtherType Protocol Discrimination (EPD)

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated in Figure 5. The IP layer operates on top of the EtherType Protocol Discrimination (EPD); this Discrimination layer is described in IEEE Std 802.3-2012; the interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).

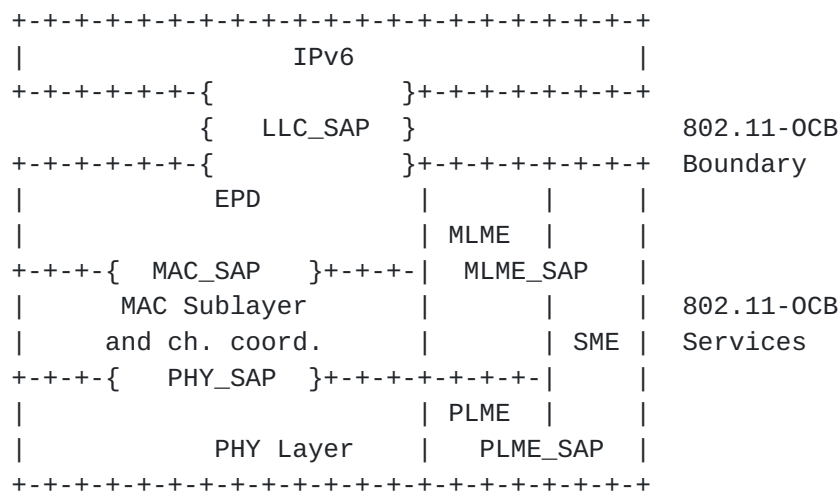


Figure 5: EtherType Protocol Discrimination

Appendix F. Design Considerations

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

F.1. Vehicle ID

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

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

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

F.2. Reliability Requirements

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

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

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

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

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

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

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

F.3. Multiple interfaces

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

The mode of operation of these other wireless interfaces is not clearly defined yet. One possibility is to consider each card as an independent network interface, with a specific MAC Address and a set of IPv6 addresses. Another possibility is to consider the set of

these wireless interfaces as a single network interface (not including the IEEE 802.11-OCB interface used by Non IP safety critical communications). This will require specific logic to ensure, for example, that packets meant for a vehicle in front are actually sent by the radio in the front, or that multiple copies of the same packet received by multiple interfaces are treated as a single packet. Treating each wireless interface as a separate network interface pushes such issues to the application layer.

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

The privacy requirements of Non IP safety-critical communications imply that if a change of pseudonym 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:

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

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

Appendix G. IEEE 802.11 Messages Transmitted in OCB mode

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

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

- o The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFack;
- o The STA may send data frames of subtype Data, Null, QoS Data, and QoS Null.

[Appendix H](#). Implementation Status

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

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

We describe an experiment of capturing an IPv6 packet on an 802.11-OCB link. In topology depicted in Figure 6, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11-OCB interface. The packet is captured on the Host, using a network protocol analyzer (e.g. Wireshark); the capture is performed in two different modes: direct mode and 'monitor' mode. The topology used during the capture is depicted below.

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).

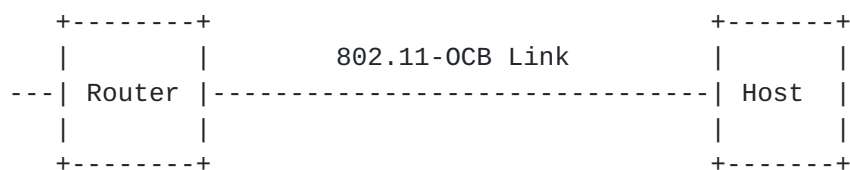


Figure 6: Topology for capturing IP packets on 802.11-OCB

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

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

H.1. Capture in Monitor Mode

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

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

Radiotap Header v0

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Header Revision| Header Pad | Header length |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
| Present flags |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Data Rate | Pad |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

IEEE 802.11 Data Header

```

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

```

Logical-Link Control Header

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```


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

IPv6 Base Header

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Router Advertisement

[illegible]

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

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

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

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

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

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

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

[H.2.](#) Capture in Normal Mode

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

Ethernet II Header

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Destination...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
...Destination                       |           Source...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
...Source                           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Type                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

IPv6 Base Header

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|Version| Traffic Class |           Flow Label           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|           Payload Length           | Next Header | Hop Limit |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     |
+                                     +
|                                     |
+                                     +
|                                     |
+                                     +
|                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     |
+                                     +
|                                     |
+                                     +
|                                     |
+                                     +
|                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     |
+                                     +
|                                     |
+                                     +
|                                     |
+                                     +
|                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

Router Advertisement

```

+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Type   |   Code   |           Checksum           |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Cur Hop Limit | M|O| Reserved | Router Lifetime |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   Options ...
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```


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

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

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

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

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

Appendix I. Extra Terminology

The following terms are defined outside the IETF. They are used to define the main terms in the main terminology section [Section 2](#).

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

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

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

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

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

