Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: August 24, 2017

A. Petrescu
CEA, LIST
N. Benamar
Moulay Ismail University
J. Haerri
Eurecom
C. Huitema

J. Lee
Sangmyung University
T. Ernst
YoGoKo
T. Li
Peloton Technology
February 20, 2017

Transmission of IPv6 Packets over IEEE 802.11 Networks in mode Outside the Context of a Basic Service Set (IPv6-over-80211ocb)
draft-ietf-ipwave-ipv6-over-80211ocb-01.txt

Abstract

In order to transmit IPv6 packets on IEEE 802.11 networks run outside the context of a basic service set (OCB, earlier "802.11p") there is a need to define a few parameters such as the recommended Maximum Transmission Unit size, 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.

In addition, the document attempts to list what is different in 802.11 OCB (802.11p) compared to more 'traditional' 802.11a/b/g/n layers, layers over which IPv6 protocols operates without issues. Most notably, the operation outside the context of a BSS (OCB) has impact on IPv6 handover behaviour and on IPv6 security.

An example of an IPv6 packet captured while transmitted over an IEEE 802.11 OCB link (802.11p) is given.

Status of This Memo

This Internet-Draft will expire on August 24, 2017.

Copyright Notice

Table of Contents

1. Introduction

This document describes the transmission of IPv6 packets on IEEE Std 802.11 OCB networks (earlier known as 802.11p). 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 required to the standards: IPv6 works fine directly over 802.11 OCB too (with an LLC layer).

The term "802.11p" is an earlier definition. As of year 2012, the behaviour of "802.11p" networks has been rolled in the document IEEE Std 802.11-2012. In this document the term 802.11p disappears. Instead, each 802.11p feature is conditioned by a flag in the Management Information Base. That flag is named "OCBActivated". Whenever OCBActivated is set to true the feature it relates to represents an earlier 802.11p feature. 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, it uses a BSS identifier equal to ff:ff:ff:ff:ff:ff.

In the following text we use the term "802.11p" to mean 802.11-2012 OCB, and vice-versa.

The IPv6 network layer operates on 802.11 OCB in the same manner as it operates on 802.11 WiFi. The IPv6 network layer operates on WiFi by involving an Ethernet Adaptation Layer; this Ethernet Adaptation Layer converts between 802.11 Headers and Ethernet II headers. The operation of IP on Ethernet is described in [RFC1042] and [RFC2464]. The situation of IPv6 networking layer on Ethernet Adaptation Layer is illustrated below:

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

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11 OCB layers, is illustrated below. 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 Accesss Point).

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

However, there may be some deployment considerations helping optimize the performances of running IPv6 over 802.11-OCB (e.g. in the case of handovers between 802.11 OCB-enabled access routers, or the consideration of using the IP security layer).

We briefly introduce the vehicular communication scenarios where IEEE 802.11-OCB links are used. This is followed by a description of differences in specification terms, between 802.11 OCB and 802.11a/b/g/n (and the same differences expressed in terms of requirements to software implementation are listed in Appendix B.)

The document then concentrates on the parameters of layering IP over 802.11 OCB as over Ethernet: MTU, Frame Format, Interface Identifier,

Address Mapping, State-less Address Auto-configuration. The values of these parameters are precisely the same as IPv6 over Ethernet [RFC2464]: the recommended value of MTU to be 1500 octets, the Frame Format containing the Type 0x86DD, the rules for forming an Interface Identifier, the Address Mapping mechanism and the Stateless Address Auto-Configuration.

As an example, these characteristics of layering IPv6 straight over LLC over 802.11 OCB MAC are illustrated by dissecting an IPv6 packet captured over a 802.11 OCB link; this is described in the section Section 6.

A couple of points can be considered as different, although they are not required in order to have a working implementation of IPv6-over-802.11-OCB. These points are consequences of the OCB operation which is particular to 802.11 OCB (Outside the Context of a BSS). First, the handovers between OCB links need specific behaviour for IP Router Advertisements, or otherwise 802.11 OCB's Time Advertisement, or of higher layer messages such as the 'Basic Safety Message' (in the US) or the 'Cooperative Awareness Message' (in the EU) or the 'WAVE Routing Advertisement'; second, the IP security mechanisms are necessary, since OCB means that 802.11 is stripped of all 802.11 link-layer security; a small additional security aspect which is shared between 802.11 OCB and other 802.11 links is the privacy concerns related to the address formation mechanisms.

In the published literature, many documents describe aspects related to running IPv6 over 802.11 OCB: [I-D.jeong-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].

RSU: Road Side Unit. An IP router equipped with, or connected to, at least one interface that is 802.11 and that is an interface that operates 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: text in document IEEE 802.11-2012 that is flagged by "dot11OCBActivated". This means: IEEE 802.11e for quality of

service; 802.11j-2004 for half-clocked operations; and 802.11p for operation in the 5.9 GHz band and in mode OCB.

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, among which we refer the reader to one recently updated [I-D.petrescu-its-scenarios-reqs], about scenarios and requirements for IP in Intelligent Transportation Systems.

4. 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 authentication/association procedures. 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 Beacons transmitted
- No authentication required
- No association needed
- No encryption provided
- Flag dot11OCBActivated set to true

The following message exchange diagram illustrates a comparison between traditional 802.11 and 802.11 in OCB mode. The 'Data' messages can be IP messages such as the messages used in Stateless or Stateful Address Auto-Configuration, or other IP messages. 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 D.

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

      (a) Traditional IEEE 802.11                (b) IEEE 802.11 OCB mode
```

The link 802.11 OCB was specified in IEEE Std 802.11p(TM)-2010 [ieee802.11p-2010] as an amendment to the 802.11 specifications, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, these 802.11p amendments have been included in IEEE 802.11(TM)-2012 [ieee802.11-2012], titled "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"; the modifications are diffused throughout various sections (e.g. 802.11p's Time Advertisement message is described in section 'Frame formats', and the operation outside the context of a BSS described in section 'MLME').

In document 802.11-2012, specifically anything referring "OCBActivated", or "outside the context of a basic service set" is actually referring to the 802.11p aspects introduced to 802.11. Note in earlier 802.11p documents the term "OCBEnabled" was used instead.

In order to delineate the aspects introduced by 802.11 OCB to 802.11, we refer to the earlier [ieee802.11p-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 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.

The 802.11 OCB links are specified to be compatible as much as possible with the behaviour of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11 OCB MAC layer offers practically the same interface to IP as the WiFi and Ethernet layers do (802.11a/b/g/n and 802.3).

To support this similarity statement (IPv6 is layered on top of LLC on top of 802.11 OCB similarly as on top of LLC on top of 802.11a/b/g/n, and as on top of LLC on top of 802.3) it is useful to analyze the differences between 802.11 OCB and 802.11 specifications. Whereas the 802.11p amendment specifies relatively complex and numerous changes to the MAC layer (and very little to the PHY layer), we note there are only a few characteristics which may be important for an implementation transmitting IPv6 packets on 802.11 OCB links.

In the list below, the only 802.11 OCB fundamental points which influence IPv6 are the OCB operation and the 12Mbit/s maximum which may be afforded by the IPv6 applications.

o Operation Outside the Context of a BSS (OCB): the 802.11p links are operated without a Basic Service Set (BSS). This means that the messages Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always ff:ff:ff:ff:ff:ff (48 '1' bits, or 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 - has a potentially strong impact on the use of the Mobile IPv6 protocol and on the protocols for IP layer security.

o Timing Advertisement: is a new message defined in 802.11p, 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. At the date of writing, an experienced reviewer considers that currently no field testing has used this message. Another implementor considers this feature implemented in an initial manner. In the future, it is speculated that this message may be useful for very simple devices which may not have their own hardware source of time (Galileo, GPS, cellular network), or by vehicular devices situated in areas not covered by such network (in tunnels, underground, outdoors but shaded by foliage or buildings, in remote areas, etc.)

- Frequency range: this is a characteristic of the PHY layer, with almost no impact to the interface between MAC and IP. However, it is worth considering that the frequency range is regulated by a regional authority (ARCEP, ETSI, FCC, etc.); as part of the regulation process, specific applications are associated with specific frequency ranges. In the case of 802.11p, 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". This band is "5.9GHz" which is different from the bands "2.4GHz" or "5GHz" used by Wireless LAN. However, as with Wireless LAN, the operation of 802.11p 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 the fixed infrastructure an explicit FCC autorization is required; for an onboard device a 'licensed-by-rule' concept applies: rule certification conformity is required); however technical conditions are different than those of the bands "2.4GHz" or "5GHz". On one hand, the allowed power levels, and implicitly the maximum allowed distance between vehicles, is of 33dBm for 802.11p (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. On the hand, 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).

- Prohibition of IPv6 on some channels relevant for the PHY of IEEE 802.11-OCB, as opposed to IPv6 not being prohibited on any channel on which 802.11a/b/g/n runs; at the time of writing, this prohibition is explicit in IEEE 1609 documents.

- '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 802.11p links, there are strong privacy concerns with respect to addressing. While the 802.11p 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 Section 7. A relevant function is described in IEEE 1609.3, clause 5.5.1 and IEEE 1609.4, clause 6.7.

Other aspects particular to 802.11p 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 802.11p networks. The

subnet structure which may be assumed in 802.11p networks is strongly influenced by the mobility of vehicles.

5. Layering of IPv6 over 802.11p as over Ethernet

5.1. Maximum Transmission Unit (MTU)

The default MTU for IP packets on 802.11p is 1500 octets. It is the same value as IPv6 packets on Ethernet links, as specified in [RFC2464]. This value of the MTU respects the recommendation that every link in the Internet must have a minimum MTU of 1280 octets (stated in [RFC2460], and the recommendations therein, especially with respect to fragmentation). If IPv6 packets of size larger than 1500 bytes are sent on an 802.11-OCB interface then the IP stack will fragment. In case there are IP fragments, the field "Sequence number" of the 802.11 Data header containing the IP fragment field is increased.

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

The Equivalent Transmit Time on Channel is a concept that may be used as an alternative to the MTU concept. A rate of transmission may be specified as well. The ETTC, rate and MTU may be in direct relationship.

5.2. Frame Format

IP packets are transmitted over 802.11p as standard Ethernet packets. As with all 802.11 frames, an Ethernet adaptation layer is used with 802.11p as well. This Ethernet Adaptation Layer 802.11-to-Ethernet is described in Section 5.2.1. The Ethernet Type code (EtherType) for IPv6 is 0x86DD (hexadecimal 86DD, or otherwise #86DD).

The Frame format for transmitting IPv6 on 802.11p networks is the same as transmitting IPv6 on Ethernet networks, and is described in section 3 of [RFC2464]. The frame format for transmitting IPv6 packets over Ethernet is illustrated below:

```
                               0                   1
                               0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                               |          Destination          |
                               +-                             -+
                               |            Ethernet           |
                               +-                             -+
                               |            Address            |
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                               |             Source            |
                               +-                             -+
                               |            Ethernet           |
                               +-                             -+
                               |            Address            |
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                               |1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 1|
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                               |             IPv6              |
                               +-                             -+
                               |            header             |
                               +-                             -+
                               |             and               |
                               +-                             -+
                               /            payload ...        /
                               +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                               (Each tic mark represents one bit.)
```

5.2.1. Ethernet Adaptation Layer

In general, 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. For example, an 802.15.4 adaptation layer may perform fragmentation and reassembly operations on a MAC whose maximum Packet Data Unit size is smaller than the minimum MTU recognized by the IPv6 Networking layer. Other examples involve link-layer address transformation, packet header insertion/removal, and so on.

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.

```
  +--------------------+-------------+-------------+---------+
  | 802.11 Data Header | LLC Header  | IPv6 Header | Payload |
  +--------------------+-------------+-------------+---------+
                   ^
                   |
                   802.11-to-Ethernet Adaptation Layer
                   |
                   v

  +---------------------+-------------+---------+
  | Ethernet II Header  | IPv6 Header | Payload |
  +---------------------+-------------+---------+
```

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

When the MTU value is smaller than the size of the IP packet to be sent, the IP layer fragments the packet into multiple IP fragments. During this operation, the "Sequence number" field of the 802.11 Data Header is increased.

In OCB mode, IPv6 packets can be transmitted either as "IEEE 802.11 Data" or alternatively as "IEEE 802.11 QoS Data", as illustrated in the following figure:

```
      +--------------------+-------------+-------------+---------+
      | 802.11 Data Header | LLC Header  | IPv6 Header | Payload |
      +--------------------+-------------+-------------+---------+

   or

      +--------------------+-------------+-------------+---------+
      | 802.11 QoS Data Hdr| LLC Header  | IPv6 Header | Payload |
      +--------------------+-------------+-------------+---------+
```

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

The mapping between qos-related fields in the IPv6 header (e.g. "Traffic Class", "Flow label") and fields in the "802.11 QoS Data

Header" (e.g. "QoS Control") are not specified in this document. Guidance for a potential mapping is provided in [I-D.ietf-tsvwg-ieee-802-11], although it is not specific to OCB mode.

5.3. Link-Local Addresses

The link-local address of an 802.11p interface is formed in the same manner as on an Ethernet interface. This manner is described in section 5 of [RFC2464].

5.4. Address Mapping

For unicast as for multicast, there is no change from the unicast and multicast address mapping format of Ethernet interfaces, as defined by sections 6 and 7 of [RFC2464].

5.4.1. Address Mapping -- Unicast

5.4.2. Address Mapping -- Multicast

IPv6 protocols often make use of IPv6 multicast addresses in the destination field of IPv6 headers. For example, an ICMPv6 link-scoped Neighbor Advertisement is sent to the IPv6 address ff02::1 denoted "all-nodes" address. When transmitting these packets on 802.11-OCB links it is necessary to map the IPv6 address to a MAC address.

The same mapping requirement applies to the link-scoped multicast addresses of other IPv6 protocols as well. In DHCPv6, the "All_DHCP_Servers" IPv6 multicast address ff02::1:2, and in OSPF the "All_SPF_Routers" IPv6 multicast address ff02::5, need to be mapped on a multicast MAC address.

An IPv6 packet with a multicast destination address DST, consisting of the sixteen octets DST[1] through DST[16], is transmitted to the IEEE 802.11-OCB MAC multicast address whose first two octets are the value 0x3333 and whose last four octets are the last four octets of DST.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 0 1 1 0 0 1 1|0 0 1 1 0 0 1 1|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   DST[13]     |   DST[14]     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   DST[15]     |   DST[16]     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

A Group ID TBD of length 112bits may be requested from IANA; this Group ID signifies "All 80211OCB Interfaces Address". Only the least 32 significant bits of this "All 80211OCB Interfaces Address" will be mapped to and from a MAC multicast address.

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.

5.5. Stateless Autoconfiguration

The Interface Identifier for an 802.11p 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 SLAAC procedure.

The bits in the 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 802.11p interface are significant, as this is a IEEE link-layer address. The details of this significance are described in [I-D.ietf-6man-ug].

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11p interface may involve privacy risks. A vehicle embarking an On-Board Unit whose egress interface is 802.11p may expose itself to eavesdropping and subsequent correlation of data; this may reveal data considered private by the vehicle owner.

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 [I-D.ietf-6man-default-iids].

5.6. Subnet Structure

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

6. Example IPv6 Packet captured over a IEEE 802.11p link

We remind that a main goal of this document is to make the case that IPv6 works fine over 802.11p networks. Consequently, this section is an illustration of this concept and thus can help the implementer when it comes to running IPv6 over IEEE 802.11p. By way of example we show that there is no modification in the headers when transmitted over 802.11p networks - they are transmitted like any other 802.11 and Ethernet packets.

We describe an experiment of capturing an IPv6 packet on an 802.11p link. In this experiment, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11p 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.

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

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 802.11p 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.

6.1. Capture in Monitor Mode

The IPv6 RA packet captured in monitor mode is illustrated below. The radio tap header provides more flexibility for reporting the characteristics of frames. The Radiotap Header is prepended by this particular stack and operating system on the Host machine to the RA

packet received from the network (the Radiotap Header is not present on the air). The implementation-dependent Radiotap Header is useful for piggybacking PHY information from the chip's registers as data in a packet understandable by userland applications using Socket interfaces (the PHY interface can be, for example: power levels, data rate, ratio of signal to noise).

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

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

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

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

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

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

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

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

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

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

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

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

The Ethernet Type field in the logical-link control header is set to 0x86dd which indicates that the frame transports an IPv6 packet. In the IEEE 802.11 data, the destination address is 33:33:00:00:00:01 which is he 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 802.11p to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11p enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.

6.2. Capture in Normal Mode

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

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

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

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

One notices that the Radiotap Header is not prepended, and that the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On another 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.

It may be interpreted that an Adaptation layer is inserted in a pure IEEE 802.11 MAC packets in the air, before delivering to the applications. In detail, this adaptation layer may consist in elimination of the Radiotap, 802.11 and LLC headers and insertion of the Ethernet II header. In this way, it can be stated that IPv6 runs naturally straight over LLC over the 802.11p MAC layer, as shown by the use of the Type 0x86DD, and assuming an adaptation layer (adapting 802.11 LLC/MAC to Ethernet II header).

7. 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.

802.11p 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 way less protected than commonly used links (wired link or protected 802.11).

At the IP layer, IPsec can be used to protect unicast communications, and SeND can be used for multicast communications. If no protection is used by the IP layer, upper layers should be protected. Otherwise, the end-user or system should be warned about the risks they run.

As with all Ethernet and 802.11 interface identifiers, there may exist privacy risks in the use of 802.11p interface identifiers. However, 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 802.11p 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 amd would hence dynamically change the affected IP address), in the way the IPv6 Privacy addresses were used, and other effects.

8. IANA Considerations

9. Contributors

Romain Kuntz contributed extensively about IPv6 handovers between links running outside the context of a BSS (802.11p 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 offering the ETSI ITS perspective, as well as other parts of the document.

10. 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, and William Whyte. Their valuable comments clarified certain 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 authours would like to thank participants to the Birds-of-a-Feather "Intelligent Transportation Systems" meetings held at IETF in 2016.

11. References

11.1. Normative References

[I-D.ietf-6man-default-iids]
Gont, F., Cooper, A., Thaler, D., and S. LIU, "Recommendation on Stable IPv6 Interface Identifiers", draft-ietf-6man-default-iids-16 (work in progress), September 2016.

[I-D.ietf-6man-ug]
Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", draft-ietf-6man-ug-06 (work in progress), December 2013.

[I-D.ietf-tsvwg-ieee-802-11]
Szigeti, T. and F. Baker, "DiffServ to IEEE 802.11 Mapping", draft-ietf-tsvwg-ieee-802-11-01 (work in progress), November 2016.

[I-D.jeong-ipwave-vehicular-networking-survey]
Jeong, J., Cespedes, S., Benamar, N., and J. Haerri, "Survey on IP-based Vehicular Networking for Intelligent Transportation Systems", draft-jeong-ipwave-vehicular-networking-survey-00 (work in progress), October 2016.

[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, <http://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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, DOI 10.17487/RFC2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

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

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

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <http://www.rfc-editor.org/info/rfc4429>.

[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, <http://www.rfc-editor.org/info/rfc4861>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <http://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, <http://www.rfc-editor.org/info/rfc6275>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <http://www.rfc-editor.org/info/rfc6775>.

[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, <http://www.rfc-editor.org/info/rfc7721>.

11.2. Informative References

[etsi-302663-v1.2.1p-2013]
"Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band, 2013-07, document en_302663v010201p.pdf, document freely available at URL http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.02.01_60/en_302663v010201p.pdf downloaded on October 17th, 2013.".

[etsi-draft-102492-2-v1.1.1-2006]
"Electromagnetic compatibility and Radio spectrum Matters (ERM); Intelligent Transport Systems (ITS); Part 2: Technical characteristics for pan European harmonized communications equipment operating in the 5 GHz frequency range intended for road safety and traffic management, and for non-safety related ITS applications; System Reference Document, Draft ETSI TR 102 492-2 V1.1.1, 2006-07, document tr_10249202v010101p.pdf freely available at URL http://www.etsi.org/deliver/etsi_tr/102400_102499/10249202/01.01.01_60/tr_10249202v010101p.pdf downloaded on October 18th, 2013.".

[fcc-cc] "'Report and Order, Before the Federal Communications Commission Washington, D.C. 20554', FCC 03-324, Released on February 10, 2004, document FCC-03-324A1.pdf, document freely available at URL http://www.its.dot.gov/exit/fcc_edocs.htm downloaded on October 17th, 2013.".

[fcc-cc-172-184]
"'Memorandum Opinion and Order, Before the Federal Communications Commission Washington, D.C. 20554', FCC 06-10, Released on July 26, 2006, document FCC-06-110A1.pdf, document freely available at URL http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-110A1.pdf downloaded on June 5th, 2014.".

[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-ieee802-01 (work in progress), September 2016.

[I-D.petrescu-its-scenarios-reqs]
Petrescu, A., Janneteau, C., Boc, M., and W. Klaudel, "Scenarios and Requirements for IP in Intelligent Transportation Systems", draft-petrescu-its-scenarios-reqs-03 (work in progress), October 2013.

[ieee16094]
"1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages; document freely available at URL https://standards.ieee.org/findstds/standard/1609.2-2016.html retrieved on July 08th, 2016.".

[ieee802.11-2012]
"802.11-2012 - 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. Downloaded on October 17th, 2013, from IEEE Standards, document freely available at URL http://standards.ieee.org/findstds/standard/802.11-2012.html retrieved on October 17th, 2013.".

[ieee802.11p-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.".

[ieeep1609.0-D2]
"IEEE P1609.0/D2 Draft Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. pdf, length 879 Kb. Restrictions apply.".

[ieeep1609.2-D17]
"IEEE P1609.2(tm)/D17 Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages. pdf, length 2558 Kb. Restrictions apply.".

[ieeep1609.3-D9-2010]
"IEEE P1609.3(tm)/D9, Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, August 2010. Authorized licensed use limited to: CEA. Downloaded on June 19, 2013 at 07:32:34 UTC from IEEE Xplore. Restrictions apply, document at persistent link http://ieeexplore.ieee.org/servlet/opac?punumber=5562705".

[ieeep1609.4-D9-2010]
"IEEE P1609.4(tm)/D9 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-channel Operation. Authorized licensed use limited to: CEA. Downloaded on June 19, 2013 at 07:34:48 UTC from IEEE Xplore. Restrictions apply. Document at persistent link http://ieeexplore.ieee.org/servlet/opac?punumber=5551097".

[TS103097]
"Intelligent Transport Systems (ITS); Security; Security header and certificate formats; document freely available at URL http://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.01.01_60/ts_103097v010101p.pdf retrieved on July 08th, 2016.".

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-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. 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 802.11p compliant:

- The chip must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11p layer, in France: 5875MHz to 5925MHz.
- The chip must support the half-rate mode (the internal clock should be able to be divided by two).
- 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 regulatory domains rules, if used by the kernel to enforce local specific restrictions. Such modifications must respect the location-specific laws.

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 C. 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 asymetry 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.

C.1. Vehicle ID

Automotive networks require the unique representation of each of their node. Accordingly, a vehicle must be identified by at least one unique ID. The current specification at ETSI and at IEEE 1609 identifies a vehicle by its MAC address uniquely obtained from the 802.11-OCB NIC.

A MAC address uniquely obtained from a IEEE 802.11-OCB NIC implicitely generates multiple vehicle IDs in case of multiple 802.11-OCB NICs. A mechanims to uniquely identify a vehicle irrespectively to the different NICs and/or technologies is required.

C.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 asymetry, 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 asymetic, 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 MUST implement fast IPv6 mobility management mechanisms.

C.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 MUST 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.

If Mobile IPv6 with NEMO extensions is used, then the MCoA RFC5648 technology is relevant for Mobile Routers with multiple interfaces, deployed in vehicles.

The privacy requirements of [] 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.

C.4. MAC Address Generation

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

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

The way to meet the randomization requirements is to retain 46 bits from the output of a strong hash function, such as SHA256, taking as input a 256 bit local secret, the "nominal" MAC Address of the interface, and a representation of the date and time of the renumbering event.

Appendix D. 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.

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: benamar73@gmail.com

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

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

Christian Huitema
Friday Harbor, WA 98250
U.S.A.

Email: huitema@huitema.net

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

Tony Li
Peloton Technology
1060 La Avenida St.
Mountain View, California   94043
United States

Phone: +16503957356
Email: tony.li@tony.li