Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 4, 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
October 31, 2016

Transmission of IP Packets over IEEE 802.11 in mode Outside the Context of a Basic Service Set
draft-petrescu-ipv6-over-80211p-05.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

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.

As an overview, we illustrate how an IPv6 stack runs over 802.11p by layering different protocols on top of each other. The IPv6 Networking is layered on top of the IEEE 802.2 Logical-Link Control (LLC) layer; this is itself layered on top of the 802.11p MAC; this layering illustration is similar to that of running IPv6 over 802.2 LLC over the 802.11 MAC, or over Ethernet MAC.

```
+-----------------+       +-----------------+
|       ...       |       |       ...       |
+-----------------+       +-----------------+
| IPv6 Networking |       | IPv6 Networking |
+-----------------+       +-----------------+
|    802.2 LLC    |  vs.  |    802.2 LLC    |
+-----------------+       +-----------------+
|   802.11p MAC   |       |   802.11b MAC   |
+-----------------+       +-----------------+
|   802.11p PHY   |       |   802.11b PHY   |
+-----------------+       +-----------------+
```

However, there are several deployment considerations to optimize the performances of running IPv6 over 802.11p (e.g. in the case of handovers between 802.11p Access Points, 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 802.11p and 802.11a/b/g/n (and the same differences expressed in terms of requirements to software implementation are listed in Appendix C.)

The document then concentrates on the parameters of layering IP over 802.11p 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.

Similarly, for IPv4, the values of these parameters are precisely the same as IPv4 over Ethernet [RFC0894]: the recommended value of MTU to be 1500 octets, and the Frame Format containing the Type 0x0800. For IPv4, Address Resolution Protocol (ARP) [RFC0826] is used to determine the MAC address used for an IPv4 address, exactly as is done for Ethernet.

As an example, these characteristics of layering IPv6 straight over LLC over 802.11p MAC are illustrated by dissecting an IPv6 packet captured over a 802.11p link; this is described in the section titled "Example of IPv6 Packet captured over an IEEE 802.11p link".

A couple of points can be considered as different, although they are not required in order to have a working implementation of IPv6-over-802.11p. These points are consequences of the OCB operation which is particular to 802.11p (Outside the Context of a BSS). First, the handovers between OCB links need specific behaviour for IP Router Advertisements, or otherwise 802.11p'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 802.11p is stripped of all 802.11 link-layer security; a small additional security aspect which is shared between 802.11p and other 802.11 links is the privacy concerns related to the address formation mechanisms. The OCB handovers and security are described each in section Section 7 and Section 9 respectively.

In standards, the operation of IPv6 as a 'data plane' over 802.11p is specified at IEEE P1609 in [ieeep1609.3-D9-2010]. For example, it mentions that "Networking services also specifies the use of the Internet protocol IPv6, and supports transport protocols such as UDP and TCP. [...] A Networking Services implementation shall support either IPv6 or WSMP or both." and "IP traffic is sent and received through the LLC sublayer as specified in [...]". The layered stacks depicted in the "Architecture" document P1609.0 [ieeep1609.0-D2] suggest that WSMP messages may not be transmitted as payload of IPv6 datagrams; WSMP and IPv6 are parallel (not stacked) layers.

Also, the operation of IPv6 over a GeoNetworking layer and over G5 is described in [etsi-302663-v1.2.1p-2013].

In the published literature, three documents describe aspects related to running IPv6 over 802.11p: [vip-wave], [ipv6-80211p-its] and [ipv6-wave].

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.

OCB: Outside the Context of a Basic Service Set identifier.

OCB - Outside the Context of a Basic-Service Set ID (BSSID).

802.11-OCB - IEEE 802.11-2012 text 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 802.11p Links are Used

The IEEE 802.11p 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 802.11p 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:

- o Wildcard BSSID (i.e., all bits are set to 1) used by each node
- o No beacons transmitted
- o No authentication required
- o No association needed
- o No encryption provided
- o dot11OCBActivated OID set to true

The link 802.11p is 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 802.11p 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 802.11p 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 802.11p 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 802.11p 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 802.11p and non-p 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 802.11p links.

In the list below, the only 802.11p 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.)

- o 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).

- o Explicit prohibition of IPv6 on some channels relevant for the PHY of IEEE 802.11p, as opposed to IPv6 not being prohibited on any channel on which 802.11a/b/g/n runs; for example, IPv6 is prohibited on the 'Control Channel' (number 178 at FCC/IEEE, and 180 at ETSI); for a detailed analysis of IEEE and ETSI prohibition of IP in particular channels see Appendix B.

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. The standard IEEE 802.11p uses OFDM encoding at PHY, as other non-b 802.11 variants do. This considers 20MHz encoding to be 'full-rate' encoding, as the earlier 20MHz encoding which is used extensively by 802.11b. In addition to the full-rate encoding, the OFDM rates also involve 5MHz and 10MHz. The 10MHz encoding is named 'half-rate'. The encoding dictates the bandwidth and latency characteristics that can be afforded by the higher-layer applications of IP communications. The half-rate means that each symbol takes twice the time to be transmitted; for this to work, all 802.11 software timer values are doubled. With this, in certain channels of the "5.9GHz" band, a maximum bandwidth of 12Mbit/s is possible, whereas in other "5.9GHz" channels a minimal bandwidth of 1Mbit/s may be used. It is worth mentioning the half-rate encoding is an optional feature characteristic of OFDM PHY (compared to 802.11b's full-rate 20MHz), used by 802.11a before 802.11p used it. In addition to the half-rate (10MHz) used by 802.11p in some channels, some other 802.11p channels may use full-rate (20MHz) or quarter-rate(?) (5MHz) encoding instead.

o It is worth mentioning that more precise interpretations of the 'half-rate' term suggest that a maximum throughput be 27Mbit/s (which is half of 802.11g's 54Mbit/s), whereas 6Mbit/s or 12Mbit/s throughputs represent effects of further 802.11p-specific PHY reductions in the throughput necessary to better accommodate vehicle-class speeds and distance ranges.

o 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 9.

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. 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.

This section does not address safety-related applications, which are done on non-IP communications. However, this section will consider the transmission of such non IP communication in the design specification of IPv6 over IEEE 802.11-OCB.

5.1. 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.

5.2. Non IP Communications

In IEEE 1609 and ETSI ITS, safety-related communications CANNOT be used with IP datagrams. For example, Basic Safety Message (BSM, an IEEE 1609 datagram) and Cooperative Awareness Message (CAM, an ETSI ITS-G5 datagram), are each transmitted as a payload that is preceded by link-layer headers, without an IP header.

Each vehicle taking part of traffic (i.e. having its engine turned on and being located on a road) MUST use Non IP communication to periodically broadcast its status information (ID, GPS position, speed,..) in its immediate neighborhood. Using these mechanisms, vehicles become 'aware' of the presence of other vehicles in their immediate vicinity. Therefore, IP communication being transmitted by vehicles taking part of traffic MUST co-exist with Non IP communication and SHOULD NOT break any Non IP mechanism, including 'harmful' interference on the channel.

The ID of the vehicle transmitting Non IP communication is transmitted in the src MAC address of the IEEE 1609 / ETSI-ITS-G5 datagrams. Accordingly, non-IP communications expose the ID of each vehicle, which may be considered as a privacy breach.

IEEE 802.11-OCB bypasses the authentication mechanisms of IEEE 802.11 networks, in order to transmit non IP communications to without any delay. This may be considered as a security breach.

IEEE 1609 and ETSI ITS provided strong security and privacy mechanisms for Non IP Communications. Security (authentication, encryption) is done by asymetric cryptography, where each vehicle attaches its public key and its certificate to all of its non IP messages. Privacy is enforced through the use of Pseudonymes. Each vehicle will be pre-loaded with a large number (>1000s) of pseudonymes generated by a PKI, which will uniquely assign a pseudonyme to a certificate (and thus to a public/private key pair).

Non IP Communication being developped for safety-critical applications, complex mechanisms have been provided for their support. These mechanisms are OPTIONAL for IP Communication, but SHOULD be used whenever possible.

5.3. 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.

5.4. Privacy requirements

Vehicles will move. As each vehicle moves, it needs to regularly announce its network interface and reconfigure its local and global view of its network. L2 mechanisms of IEEE 802.11-OCB MAY be employed to assist IPv6 in discovering new network interfaces. L3 mechanisms over IEEE 802.11-OCB SHOULD be used to assist IPv6 in discovering new network interfaces.

The headers of the L2 mechanisms of IEEE 802.11-OCB and L3 management mechanisms of IPv6 are not encrypted, and as such expose at least the src MAC address of the sender. In the absence of mitigations, adversaries could monitor the L2 or L3 management headers, track the MAC Addresses, and through that track the position of vehicles over time; in some cases, it is possible to deduce the vehicle manufacturer name from the OUI of the MAC address of the interface (with help of additional databases). It is important that sniffers along roads not be able to easily identify private information of automobiles passing by.

Similary to Non IP safety-critical communications, the obvious mitigation is to use some form of MAC Address Randomization. We can assume that there will be "renumbering events" causing the MAC Addresses to change. Clearly, a change of MAC Address should induce a simultaneous change of IPv6 Addresses, to prevent linkage of the old and new MAC Addresses through continuous use of the same IP Addresses.

The change of an IPv6 address also implies the change of the network prefix. Prefix delegation mechanisms should be available to vehicles to obtain new prefixes during "renumbering events".

Changing MAC and IPv6 addresses will disrupt communications, which goes against the reliability requirements expressed in [TS103097]. We will assume that the renumbering events happen only during "safe" periods, e.g. when the vehicle has come to a full stop. The determination of such safe periods is the responsibility of implementors. In automobile settings it is common to decide that certain operations (e.g. software update, or map update) must happen only during safe periods.

MAC Address randomization will not prevent tracking if the addresses stay constant for long intervals. Suppose for example that a vehicle only renumbers the addresses of its interface when leaving the vehicle owner's garage in the morning. It would be trivial to observe the "number of the day" at the known garage location, and to associate that with the vehicle's identity. There is clearly a tension there. If renumbering events are too infrequent, they will not protect privacy, but if their are too frequent they will affect reliability. We expect that implementors will eventually find the right balance.

5.5. Authentication requirements

IEEE 802.11-OCB does not have L2 authentication mechanisms. Accordingly, a vehicle receiving a IPv6 over IEEE 802.11-OCB packet cannot check or be sure the legitimacy of the src MAC (and associated ID). This is a significant breach of security.

Similarly to Non IP safety-critical communications, IPv6 over 802.11-OCB packets must contain a certificate, including at least the public key of the sender, that will allow the receiver to authenticate the packet, and guarantee its legitimacy.

To satisfy the privacy requiremrents of Section 5.4, the certificate SHALL be changed at each 'renumbering event'.

5.6. 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.

The privacy requirements of Section 5.4 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.

5.7. 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.

5.8. Security Certificate 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". So MUST also the Security Certificates. Unless unavailable, the Security Certificate Generation mechanisms SHOULD follow the specification in IEEE 1609.2 [ieee16094] or ETSI TS 103 097 [TS103097]. These security mechanisms have the following characteristics:

- Authentication - Elliptic Curve Digital Signature Algorithm (ECDSA) - A Secured Hash Function (SHA-256) will sign the message with the public key of the sender.

- Encryption - Elliptic Curve Integrated Encryption Scheme (ECIES) - A Key Derivation Function (KDF) between the sender's public key and the receiver's private key will generate a symetric key used to encrypt a packet.

If the mechanisms described in IEEE 1609.2 [ieee16094] or ETSI TS 103 097 [TS103097] are either not supported or not capable of running on the hardware, an alternative approach based on Pretty-Good-Privacy (PGP) MAY be used as an alternative.

6. Layering of IPv4 and IPv6 over 802.11p as over Ethernet

6.1. 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 into more IP packets, depending on the initial size. In case there are IP fragments, the field "Sequence number" of the 802.11 Data header containing the IP fragment field is increased.

It is possible to send IP packets of size bigger than the MTU of 1500 bytes without the IP fragmentation mechanism to be involved. However, in such cases it is not safe to assume that the on-link receiver understands it and does not send a "Packet too Big" ICMPv6 message back - it likely will.

It is possible to set the MTU value on an interface to a value smaller than 1500 bytes, and thus trigger IP fragmentation for packets larger than that value. For example, set the MTU to 500 bytes and the IP fragmentation will generate IP fragments as soon as IP packets to be sent are larger than 500 bytes. However, the lowest such limit is 255 bytes. It is not possible to set an MTU of 254 bytes or lower on an interface.

It is possible that the MAC layer fragments as well (in addition to the IP layer performing fragmentation). The 802.11 Data Header includes a "Fragment number" field and a "More Fragments" field. This former is set to 0 usually.

It is possible that the application layer fragments.

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.

6.2. 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 6.2.1. The Ethernet Type code (EtherType) for IPv6 is 0x86DD (hexadecimal 86DD, or otherwise #86DD). The EtherType code for IPv4 is 0x0800.

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 IPv4 on 802.11p networks is the same as transmitting IPv4 on Ethernet networks and is described in [RFC0894]. For sake of completeness, the frame format for transmitting IPv6 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.)
```

6.2.1. 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. The other fields in the Data and LLC Headers are not used by the IPv6 stack.

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.

IPv6 packets can be transmitted as "IEEE 802.11 Data" or alternatively as "IEEE 802.11 QoS Data".

```
IEEE 802.11 Data                  IEEE 802.11 QoS Data
Logical-Link Control              Logical-Link Control
IPv6 Header                       IPv6 Header
```

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.

6.2.2. MAC Address Resolution

For IPv4, Address Resolution Protocol (ARP) [RFC0826] is used to determine the MAC address used for an IPv4 address, exactly as is done for Ethernet.

6.3. Link-Local Addresses

For IPv6, 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].

For IPv4, link-local addressing is described in [RFC3927].

6.4. 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].

(however, there is discussion about geography, networking and IPv6 multicast addresses: geographical dissemination of IPv6 data over 802.11p may be useful in traffic jams, for example).

6.4.1. Address Mapping -- Unicast

6.4.2. 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]     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Other than link-scope addressing, it may be possible to conceive other IPv6 multicast addresses for specific use in vehicular communication scenarios. For example, certain vehicle types (or road infrastructure equipment) in a zone can be denoted by an IPv6 multicast address: "all-yellow-taxis-in-street", or "all-uber-cars". This helps sending a message to these particular types of vehicles, instead of sending to all vehicles in that same street. The protocols SDP and LLDP could further be used in managing this as a service.

It may be possible to map parts of other-than-link-scope IPv6 multicast address (e.g. parts of a global-scope IPv6 multicast address) into parts of a 802.11-OCB MAC address. This may help certain IPv6 operations.

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.

Alternatively, instead of 0x3333 address other addresses reserved at IEEE can be considered. The Group MAC addresses reserved at IEEE are listed at https://standards.ieee.org/develop/regauth/grpmac/public.html (address browsed in July 2016).

6.5. 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.

For example, the Interface Identifier for an 802.11p interface whose built-in address is, in hexadecimal:

30-14-4A-D9-F9-6C

would be

32-14-4A-FF-FE-D9-F9-6C.

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, 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. The address generation mechanism should consider these aspects, as described in [I-D.ietf-6man-ipv6-address-generation-privacy].

6.6. Subnet Structure

In this section the subnet structure may be described: the addressing model (are multi-link subnets considered?), address resolution, multicast handling, packet forwarding between IP subnets. Alternatively, this section may be spinned off into a separate document.

The 802.11p networks, much like other 802.11 networks, may be considered as 'ad-hoc' networks. The addressing model for such networks is described in [RFC5889].

The SLAAC procedure makes the assumption that if a packet is retransmitted a fixed number of times (typically 3, but it is link dependent), any connected host receives the packet with high probability. On ad-hoc links (when 802.11p is operated in OCB mode, the link can be considered as 'ad-hoc'), both the hidden terminal problem and mobility-range considerations make this assumption incorrect. Therefore, SLAAC should not be used when address collisions can induce critical errors in upper layers.

Some aspects of multi-hop ad-hoc wireless communications which are relevant to the use of 802.11p (e.g. the 'hidden' node) are described in [I-D.baccelli-multi-hop-wireless-communication].

When operating in OCB mode, it may be appropriate to use a 6LoWPAN adaptation layer [RFC6775]. However, it should be noted that the use

6lowpan adaptation layer is comparable with the use of Ethernet to 802.11 adaptation layer.

7. Handovers between OCB links

A station operating IEEE 802.11p in the 5.9 GHz band in US or EU is required to send data frames outside the context of a BSS. In this case, the station does not utilize the IEEE 802.11 authentication, association, or data confidentiality services. This avoids the latency associated with establishing a BSS and is particularly suited to communications between mobile stations or between a mobile station and a fixed one playing the role of the default router (e.g. a fixed Road-Side Unit a.k.a RSU acting as an infrastructure router).

The process of movement detection is described in section 11.5.1 of [RFC6275]. In the context of 802.11p deployments, detecting movements between two adjacent RSUs becomes harder for the moving stations: they cannot rely on Layer-2 triggers (such as L2 association/de-association phases) to detect when they leave the vicinity of an RSU and move within coverage of another RSU. In such case, the movement detection algorithms require other triggers. We detail below the potential other indications that can be used by a moving station in order to detect handovers between OCB ("Outside the Context of a BSS") links.

A movement detection mechanism may take advantage of positioning data (latitude and longitude).

Mobile IPv6 [RFC6275] specifies a new Router Advertisement option called the "Advertisement Interval Option". It can be used by an RSU to indicate the maximum interval between two consecutive unsolicited Router Advertisement messages sent by this RSU. With this option, a moving station can learn when it is supposed to receive the next RA from the same RSU. This can help movement detection: if the specified amount of time elapses without the moving station receiving any RA from that RSU, this means that the RA has been lost. It is up to the moving node to determine how many lost RAs from that RSU constitutes a handover trigger.

In addition to the Mobile IPv6 "Advertisement Interval Option", the Neighbor Unreachability Detection (NUD) [RFC4861] can be used to determine whether the RSU is still reachable or not. In this context, reachability confirmation would basically consist in receiving a Neighbor Advertisement message from a RSU, in response to a Neighbor Solicitation message sent by the moving station. The RSU should also configure a low Reachable Time value in its RA in order to ensure that a moving station does not assume an RSU to be reachable for too long.

The Mobile IPv6 "Advertisement Interval Option" as well as the NUD procedure only help knowing if the RSU is still reachable by the moving station. It does not provide the moving station with information about other potential RSUs that might be in range. For this purpose, increasing the RA frequency could reduce the delay to discover the next RSU. The Neighbor Discovery protocol [RFC4861] limits the unsolicited multicast RA interval to a minimum of 3 seconds (the MinRtrAdvInterval variable). This value is too high for dense deployments of Access Routers deployed along fast roads. The protocol Mobile IPv6 [RFC6275] allows routers to send such RA more frequently, with a minimum possible of 0.03 seconds (the same MinRtrAdvInterval variable): this should be preferred to ensure a faster detection of the potential RSUs in range.

If multiple RSUs are in the vicinity of a moving station at the same time, the station may not be able to choose the "best" one (i.e. the one that would afford the moving station spending the longest time in its vicinity, in order to avoid too frequent handovers). In this case, it would be helpful to base the decision on the signal quality (e.g. the RSSI of the received RA provided by the radio driver). A better signal would probably offer a longer coverage. If, in terms of RA frequency, it is not possible to adopt the recommendations of protocol Mobile IPv6 (but only the Neighbor Discovery specification ones, for whatever reason), then another message than the RA could be emitted periodically by the Access Router (provided its specification allows to send it very often), in order to help the Host determine the signal quality. One such message may be the 802.11p’s Time Advertisement, or higher layer messages such as the "Basic Safety Message" (in the US) or the "Cooperative Awareness Message " (in the EU), that are usually sent several times per second. Another alternative replacement for the IPv6 Router Advertisement may be the message ’WAVE Routing Advertisement’ (WRA), which is part of the WAVE Service Advertisement and which may contain optionally the transmitter location; this message is described in section 8.2.5 of [ieeep1609.3-D9-2010].

Once the choice of the default router has been performed by the moving node, it can be interesting to use Optimistic DAD [RFC4429] in order to speed-up the address auto-configuration and ensure the fastest possible Layer-3 handover.

To summarize, efficient handovers between OCB links can be performed by using a combination of existing mechanisms. In order to improve the default router unreachability detection, the RSU and moving stations should use the Mobile IPv6 "Advertisement Interval Option" as well as rely on the NUD mechanism. In order to allow the moving station to detect potential default router faster, the RSU should also be able to be configured with a smaller minimum RA interval such as the one recommended by Mobile IPv6. When multiple RSUs are available at the same time, the moving station should perform the handover decision based on the signal quality. Finally, optimistic DAD can be used to reduce the handover delay.

The Received Frame Power Level (RCPI) defined in IEEE Std 802.11-2012, conditioned by the dotOCBActived flag, is an information element which contains a value expressing the power level at which that frame was received. This value may be used in comparing power levels when triggering IP handovers.

8. 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 captured 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.

The popular wireshark network protocol analyzer is a free software tool for Windows and Unix. It includes a dissector for 802.11p features along with all other 802.11 features (i.e. it displays these features in a human-readable format).

8.1. 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.

8.2. 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).

9. Security Considerations

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.

The WAVE protocol stack provides for strong security when using the WAVE Short Message Protocol and the WAVE Service Advertisement [ieeep1609.2-D17].

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.

10. IANA Considerations

11. Contributors

Romain Kuntz contributed extensively the concepts described in Section 7 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 IPv4 and IPv6 messages over 802.11-OCB in initial trials.

12. 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 Roy, Ray Hunter, Tom Kurihara, Michelle Wetterwald, Michal Sojka, Jan de Jongh, Suresh Krishnan, Dino Farinacci, Vincent Park and Gloria Gwynne. 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.

13. References

13.1. Normative References

[I-D.ietf-6man-ipv6-address-generation-privacy]
Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-08 (work in progress), September 2015.

[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.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware", STD 37, RFC 826, DOI 10.17487/RFC0826, November 1982, <http://www.rfc-editor.org/info/rfc826>.

[RFC0894] Hornig, C., "A Standard for the Transmission of IP Datagrams over Ethernet Networks", STD 41, RFC 894, DOI 10.17487/RFC0894, April 1984, <http://www.rfc-editor.org/info/rfc894>.

[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>.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, DOI 10.17487/RFC3927, May 2005, <http://www.rfc-editor.org/info/rfc3927>.

[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>.

13.2. 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.baccelli-multi-hop-wireless-communication]
Baccelli, E. and C. Perkins, "Multi-hop Ad Hoc Wireless Communication", draft-baccelli-multi-hop-wireless-communication-06 (work in progress), July 2011.

[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".

[ipv6-80211p-its]
Shagdar, O., Tsukada, M., Kakiuchi, M., Toukabri, T., and T. Ernst, "Experimentation Towards IPv6 over IEEE 802.11p with ITS Station Architecture", International Workshop on IPv6-based Vehicular Networks, (colocated with IEEE Intelligent Vehicles Symposium), URL: http://hal.inria.fr/hal-00702923/en, Downloaded on: 24 October 2013, Availability: free at some sites, paying at others, May 2012.

[ipv6-wave]
Clausen, T., Baccelli, E., and R. Wakikawa, "IPv6 Operation for WAVE - Wireless Access in Vehicular Environments", Rapport de Recherche INRIA, number 7383, URL: http://hal.inria.fr/inria-00517909/, Downloaded on: 24 October 2013, Availability: free at some sites, September 2010.

[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.".

[vip-wave]
Cespedes, S., Lu, N., and X. Shen, "VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks", IEEE Transactions on Intelligent Transportation Systems, Volume 14, Issue 1, URL and Digital Object Identifier: http://dx.doi.org/10.1109/TITS.2012.2206387, Downloaded on: 24 October 2013, Availability: free at some sites, paying at others, March 2013.

Appendix A. ChangeLog

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

From draft-petrescu-ipv6-over-80211p-02.txt to draft-petrescu-ipv6-over-80211p-03.txt:

o Added clarification about the "OCBActivated" qualifier in the the new IEEE 802.11-2012 document; this IEEE document integrates now all earlier 802.11p features; this also signifies the dissapearance of an IEEE IEEE 802.11p document altogether.

o Added explanation about FCC not prohibiting IP on channels, and comments about engineering advice and reliability of IP messages.

o Added possibility to use 6lowpan adaptation layer when in OCB mode.

o Added appendix about the distribution of certificates to vehicles by using IPv6-over-802.11p single-hop communications.

o Refined the explanation of 'half-rate' mode.

o Added the privacy concerns and necessity of and potential effects of dynamically changing MAC addresses.

From draft-petrescu-ipv6-over-80211p-01.txt to draft-petrescu-ipv6-over-80211p-02.txt:

o updated authorship.

o added explanation about FCC not prohibiting IP on channels, and comments about engineering advice and reliability of IP messages.

o added possibility to use 6lowpan adaptation layer when in OCB mode.

o added appendix about the distribution of certificates to vehicles by using IPv6-over-802.11p single-hop communications.

o refined the explanation of 'half-rate' mode.

o added the privacy concerns and necessity of and potential effects of dynamically changing MAC addresses.

From draft-petrescu-ipv6-over-80211p-00.txt to draft-petrescu-ipv6-over-80211p-01.txt:

o updated one author's affiliation detail.

o added 2 more references to published literature about IPv6 over 802.11p.

From draft-petrescu-ipv6-over-80211p-00.txt to draft-petrescu-ipv6-over-80211p-00.txt:

- first version.

Appendix B. Explicit Prohibition of IPv6 on Channels Related to ITS Scenarios using 802.11p Networks - an Analysis

B.1. Interpretation of FCC and ETSI documents with respect to running IP on particular channels

- The FCC created the term "Control Channel" [fcc-cc]. For it, it defines the channel number to be 178 decimal, and positions it with a 10MHz width from 5885MHz to 5895MHz. The FCC rules point to standards document ASTM-E2213 (not freely available at the time of writing of this draft); in an interpretation of a reviewer of this document, this means not making any restrictions to the use of IP on the control channel.

- The FCC created two more terms for particular channels [fcc-cc-172-184], among others. The channel 172 (5855MHz to 5865MHz)) is designated "exclusively for [V2V] safety communications for accident avoidance and mitigation, and safety of life and property applications", and the channel 184 (5915MHz to 5925MHz) is designated "exclusively for high-power, longer-distance communications to be used for public-safety applications involving safety of life and property, including road-intersection collision mitigation". However, they are not named "control" channels, and the document does not mention any particular restriction on the use of IP on either of these channels.

- On another hand, at IEEE, IPv6 is explicitely prohibited on channel number 178 decimal - the FCC's 'Control Channel'. The document [ieeep1609.4-D9-2010] prohibits upfront the use of IPv6 traffic on the Control Channel: 'data frames containing IP datagrams are only allowed on service channels'. Other 'Service Channels' are allowed to use IP, but the Control Channel is not.

- In Europe, basically ETSI considers FCC's "Control Channel" to be a "Service Channel", and defines a "Control Channel" to be in a slot considered by FCC as a "Service Channel". In detail, FCC's "Control Channel" number 178 decimal with 10MHz width (5885MHz to 5895MHz) is defined by ETSI to be a "Service Channel", and is named 'G5-SCH2' [etsi-302663-v1.2.1p-2013]. This channel is dedicated to 'ITS Road Safety' by ETSI. Other channels are dedicated to 'ITS road traffic efficiency' by ETSI. The ETSI's "Control Channel" - the "G5-CCH" - number 180 decimal (not 178) is reserved as a 10MHz-width centered on 5900MHz (5895MHz to 5905MHz) (the 5895MHz-5905MHz channel is a Service Channel for FCC). Compared to IEEE, ETSI makes no upfront statement with respect to IP and particular channels; yet it relates the 'In car Internet' applications ('When nearby a stationary public internet access point (hotspot), application can use standard IP services for applications.') to the 'Non-safety-related ITS application' [etsi-draft-102492-2-v1.1.1-2006]. Under an interpretation of an author of this Internet Draft, this may mean ETSI may forbid IP on the 'ITS Road Safety' channels, but may allow IP on 'ITS road traffic efficiency' channels, or on other 5GHz channels re-used from BRAN (also dedicated to Broadband Radio Access Networks).

o At EU level in ETSI (but not some countries in EU with varying adoption levels) the highest power of transmission of 33 dBm is allowed, but only on two separate 10Mhz-width channels centered on 5900MHz and 5880MHz respectively. It may be that IPv6 is not allowed on these channels (in the other 'ITS' channels where IP may be allowed, the levels vary between 20dBm, 23 dBm and 30 dBm; in some of these channels IP is allowed). A high-power of transmission means that vehicles may be distanced more (intuitively, for 33 dBm approximately 2km is possible, and for 20 dBm approximately 50meter).

B.2. Interpretations of Latencies of IP datagrams

IPv6 may be "allowed" on any channel. Certain interpretations consider that communicating IP datagrams may involve longer latencies than non-IP datagrams; this may make them little adapted for safety applications which require fast reaction. Certain other views disagree with this, arguing that IP datagrams are transmitted at the same speed as any other non-IP datagram and may thus offer same level of reactivity for safety applications.

Appendix C. Changes Needed on a software driver 802.11a to become a 802.11p 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:

o 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.

o The chip must support the half-rate mode (the internal clock should be able to be divided by two).

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 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 D. Use of IPv6 over 802.11p for distribution of certificates

Security of vehicular communications is one of the challenging tasks in the Intelligent Transport Systems. The adoption of security procedures becomes an indispensable feature that cannot be neglected when designing new protocols. One of the interesting use cases of transmitting IPv6 packets over IEEE 802.11p links is the distribution of certificates between road side infrastructure and the vehicule (Figure below).

```
###########
#         #
# Server  #
#(backend)#
#         #
###########
     |
     |
     |  <-- link  (depending on the infrastructure)
     |
     |
     |
     |
 ##########                    #############
 #        #                    #           #
 #  RSU   # - - - - - - - - - -#   Router  #
 #        #    802.11p Link    # in-vehicle#
 ##########                    #############
                                    o  o
```

Many security mechanisms have been proposed for the vehicular environment, mechanisms often relying on public key algorithms. Public key algorithms necessitate a public key infrastructure (PKI) to distribute and revoke certificates. The server backend in the figure can play the role of a Certification Authority which will send certificates and revocation lists to the RSU which in turn retransmits certificates in messages directed to passing-by vehicles. The initiation distribution of certificates as IPv6 messages over 802.11p links may be realized by WSA messages (WAVE Service Announcement, a non-IP message). The certificate is sent as an IPv6 messages over a single-hop 802.11p link.

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