Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 9, 2017

J. Haerri
EURECOM
A. Petrescu
CEA, LIST
C. Huitema
Microsoft

July 8, 2016

Transmission of IPv6 Packets over IEEE 802.11-OCB Networks
draft-haerri-ipv6-over-80211ocb-00.txt

Abstract

This document describes the mechanisms required by IPv6 to be transmitted on IEEE 802.11 OCB networks.

Status of This Memo

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

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

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

This Internet-Draft will expire on January 9, 2017.

Table of Contents

1. Introduction

This document describes the transmission of IPv6 packets on IEEE 802.11 OCB networks.

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].

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

802.11-OCB - IEEE 802.11-2012 [ieee802.11-2012] text flagged by "dot11OCBActivated". This means: IEEE 802.11e for quality of service; and 802.11p [ieee802.11p-2010] for operation in the 5.9 GHz band and in mode OCB.

3. 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 that of 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.

3.1. 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 irrespectivey to the different NICs and/or technologies is required.

3.2. 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 payload of 802.11 messages, 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. According to this mechanisms, vehicles become 'aware' of the presence of other vehicles in their immediate vincinity. Accordingly, 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 Geonet 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 for non IP communications to be transmitted 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 (>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.

3.3. 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 to 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 being not 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 being not available, IPv6 over IEEE 802.11-OCB MUST implement a higher layer mechanism for time synchroniation 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.

3.4. Privacy requirements

Vehicles will move. As they move, each vehicle 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 prefices 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.

3.5. 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 3.4, the certificate SHALL be changed at each 'renumbering event'.

3.6. Multiple interfaces

There are considerations of 2 or more IEEE 802.11-OCB interface cards per vehicle. For each vehicle taking part of 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 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 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 3.4 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.

3.7. 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].

One possible 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.

3.8. 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.

4. Mapping IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit

MTU is determined by the IEEE 802.11-2012 specification [ieee802.11-2012].

4.2. Frame Format

4.3. Stateless Autoconfiguration

4.4. Link-Local Addresses

4.5. Address Mapping -- Unicast

4.6. Address Mapping -- Multicast

5. Security Considerations

The source MAC address can be generated by the following random-number generation algorithm:

```
f = ... 48bits.
The output must not collide with existing allocations.
```

For one 802.11-OCB interface multiple random MAC addresses MAY be generated.

For each MAC address there is an associated certificate.

6. IANA Considerations

7. Acknowledgements

The authors would like to acknowledge...

8. References

8.1. Normative References

[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>.

8.2. Informative References

[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]
"IEEE Std 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; document freely available at URL http://standards.ieee.org/getieee802/download/802.11-2012.pdf retrieved on July 08th, 2016.".

[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.".

[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 -00.txt to -00.txt:

o first version.

Authors' Addresses

Jerome Haerri
EURECOM
Sophia-Antipolis 06904
France

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

Alexandre Petrescu
CEA, LIST
Communicating Systems Laboratory
Gif-sur-Yvette , Ile-de-France 91190
France

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

Christian Huitema
Microsoft
Redmond, WA 98052
U.S.A.

Email: huitema@microsoft.com