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

Abstract

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

Status of This Memo

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

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

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

This Internet-Draft will expire on June 21, 2019.
1. Introduction

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

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

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

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

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

2. Terminology

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

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

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

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

802.11-OCB: mode specified in IEEE Std 802.11-2016 when the MIB attribute dot11OCBActivated is true. Note: compliance with standards and regulations set in different countries when using the 5.9GHz frequency band is required.

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

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

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

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

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

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

The IPv6 packet transmitted on 802.11-OCB MUST be immediately preceded by a Logical Link Control (LLC) header and an 802.11 header. In the LLC header, and in accordance with the EtherType Protocol Discrimination (EPD, see Appendix E), the value of the Type field MUST be set to 0x86DD (IPv6). In the 802.11 header, the value of the Subtype sub-field in the Frame Control field MUST be set to 8 (i.e. ‘QoS Data’); the value of the Traffic Identifier (TID) sub-field of the QoS Control field of the 802.11 header MUST be set to binary 001 (i.e. User Priority ‘Background’, QoS Access Category ‘AC_BK’).

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

4.2.1. Ethernet Adaptation Layer

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

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

The operation of the Ethernet Adaptation Layer is depicted by the double arrow in Figure 1.
The Receiver and Transmitter Address fields in the 802.11 header MUST contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header MUST be the same as the value of the Type field in the Ethernet II Header. That value MUST be set to 0x86DD (IPv6).

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

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

![Diagram](image-url)

**Figure 1: Operation of the Ethernet Adaptation Layer**

**Figure 2: Ethernet Adaptation Layer stacked with other layers**

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

There are several types of IPv6 addresses [RFC4291], [RFC4193], that MAY be assigned to an 802.11-OCB interface. Among these types of addresses only the IPv6 link-local addresses MAY be formed using an EUI-64 identifier.

If the IPv6 link-local address is formed using an EUI-64 identifier, then the mechanism of forming that address is the same mechanism as used to form an IPv6 link-local address on Ethernet links. This mechanism is described in section 5 of [RFC2464].

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

4.4. Address Mapping

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

4.4.1. Address Mapping -- Unicast

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

4.4.2. Address Mapping -- Multicast

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

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

4.5. Stateless Autoconfiguration

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

The Interface Identifier for an 802.11-OCB interface is formed using the same rules as the Interface Identifier for an Ethernet interface;
the RECOMMENDED method for forming stable Interface Identifiers (IID) is described in [RFC8064]. The method of forming IIDs described in section 4 of [RFC2464] MAY be used during transition time.

The bits in the Interface Identifier have no generic meaning and the identifier should be treated as an opaque value. The bits 'Universal' and 'Group' in the identifier of an 802.11-OCB interface are significant, as this is an IEEE link-layer address. The details of this significance are described in [RFC7136]. If semantically opaque Interface Identifiers are needed, a potential method for generating semantically opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration is given in [RFC7217].

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

The IPv6 packets can be captured easily in the Internet and on-link in public roads. For this reason, an attacker may realize many attacks on privacy. One such attack on 802.11-OCB is to capture, store and correlate Company ID information present in MAC addresses of many cars (e.g. listen for Router Advertisements, or other IPv6 application data packets, and record the value of the source address in these packets). Further correlation of this information with other data captured by other means, or other visual information (car color, others) MAY constitute privacy risks.

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

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose Interface Identifiers don’t change too often. It is RECOMMENDED to use the mechanisms described in RFC 7217 to permit the use of Stable Interface Identifiers that do not change within one subnet prefix. A possible source for the Net-Iface Parameter is a virtual interface name, or logical interface name, that is decided by a local administrator.

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

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

The structure of this subnet is ephemeral, in that it is strongly influenced by the mobility of vehicles: the 802.11 hidden node effects appear; the 802.11 networks in OCB mode may be considered as ‘ad-hoc’ networks with an addressing model as described in [RFC5889]. On another hand, the structure of the internal subnets in each car is relatively stable.

As recommended in [RFC5889], when the timing requirements are very strict (e.g. fast drive through IP-RSU coverage), no on-link subnet prefix should be configured on an 802.11-OCB interface. In such cases, the exclusive use of IPv6 link-local addresses is RECOMMENDED.

Additionally, even if the timing requirements are not very strict (e.g. the moving subnet formed by two following vehicles is stable, a fixed IP-RSU is absent), the subnet is disconnected from the Internet (a default route is absent), and the addressing peers are equally qualified (impossible to determine that some vehicle owns and distributes addresses to others) the use of link-local addresses is RECOMMENDED.

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

Protocols like Mobile IPv6 [RFC6275] and DNAv6 [RFC6059], which depend on timely movement detection, might need additional tuning work to handle the lack of link-layer notifications during handover. This is for further study.

5. Security Considerations

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

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

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

The potential attack vectors are: MAC address spoofing, IP address and session hijacking, and privacy violation Section 5.1.

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

5.1. Privacy Considerations

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11-OCB interface may involve privacy, MAC address spoofing and IP address hijacking risks. A vehicle embarking an IP-OBU whose egress interface is 802.11-OCB may expose itself to eavesdropping and subsequent correlation of data; this may reveal data considered private by the vehicle owner; there is a risk of being tracked. In outdoors public environments, where vehicles typically circulate, the privacy risks are more important than in indoors settings. It is highly likely that attacker sniffers are deployed along routes which listen for IEEE frames, including IP packets, of vehicles passing by. For this reason, in the 802.11-OCB deployments, there is a strong necessity to use protection tools such as dynamically changing MAC addresses Section 5.2, semantically opaque Interface Identifiers and stable Interface Identifiers Section 4.5. This may help mitigate privacy risks to a certain level.

5.2. MAC Address and Interface ID Generation

In 802.11-OCB networks, the MAC addresses MAY change during well defined renumbering events. In the moment the MAC address is changed
on an 802.11-OCB interface all the Interface Identifiers of IPv6 addresses assigned to that interface MUST change.

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

A ‘randomized’ MAC address has the following characteristics:

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

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

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

5.3. Pseudonym Handling

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

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

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

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

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

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

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

8. Acknowledgements

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

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

For the multicast discussion, the authors would like to thank Owen DeLong, Joe Touch, Jen Linkova, Erik Kline, Brian Haberman and participants to discussions in network working groups.
The authors would like to thank participants to the Birds-of-a-Feather "Intelligent Transportation Systems" meetings held at IETF in 2016.

Human Rights Protocol Considerations review by Amelia Andersdotter.

9. References

9.1. Normative References


9.2. Informative References


[I-D.hinden-6man-rfc2464bis]

[I-D.ietf-ipwave-vehicular-networking-survey]

[I-D.ietf-mboned-ieee802-mcast-problems]

[IEEE-1609.2]

[IEEE-1609.3]

[IEEE-1609.4]

[IEEE-802.11-2016]
Appendix A. ChangeLog

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

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

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

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

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

-29:

-28:
o  Created a new section ‘Pseudonym Handling’.
o  removed the ‘Vehicle ID’ appendix.
o  improved the address generation from random MAC address.
o  shortened Term IP-RSU definition.
o  removed refs to two detail Clauses in IEEE documents, kept just these latter.


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

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

From draft-ietf-ipwave-ipv6-over-80211ocb-23 to draft-ietf-ipwave-ipv6-over-80211ocb-24
o  Nit: wrote "IPWAVE Working Group" on the front page, instead of "Network Working Group".

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

From draft-ietf-ipwave-ipv6-over-80211ocb-22 to draft-ietf-ipwave-ipv6-over-80211ocb-23
o  No content modifications, but check the entire draft chain on IPv6-only: xml2rfc, submission on tools.ietf.org and datatracker.
From draft-ietf-ipwave-ipv6-over-80211ocb-21 to draft-ietf-ipwave-ipv6-over-80211ocb-22

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

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

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

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

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

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

- Removed the text about fragmentation.
- Removed the mentioning of WSMP and GeoNetworking.
- Removed the explanation of the binary representation of the EtherType.
- Rendered normative the paragraph about unicast and multicast address mapping.
- Removed paragraph about addressing model, subnet structure and easiness of using LLs.
- Clarified the Type/Subtype field in the 802.11 Header.
- Used RECOMMENDED instead of recommended, for the stable interface identifiers.
From draft-ietf-ipwave-ipv6-over-80211ocb-17 to draft-ietf-ipwave-ipv6-over-80211ocb-18
- Improved the MTU and fragmentation paragraph.

From draft-ietf-ipwave-ipv6-over-80211ocb-16 to draft-ietf-ipwave-ipv6-over-80211ocb-17
- Substituted "MUST be increased" to "is increased" in the MTU section, about fragmentation.

From draft-ietf-ipwave-ipv6-over-80211ocb-15 to draft-ietf-ipwave-ipv6-over-80211ocb-16
- Removed the definition of the 'WiFi' term and its occurrences. Clarified a phrase that used it in Appendix C "Aspects introduced by the OCB mode to 802.11".
- Added more normative words: MUST be 0x86DD, MUST fragment if size larger than MTU, Sequence number in 802.11 Data header MUST be increased.

From draft-ietf-ipwave-ipv6-over-80211ocb-14 to draft-ietf-ipwave-ipv6-over-80211ocb-15
- Added normative term MUST in two places in section "Ethernet Adaptation Layer".

From draft-ietf-ipwave-ipv6-over-80211ocb-13 to draft-ietf-ipwave-ipv6-over-80211ocb-14
- Created a new Appendix titled "Extra Terminology" that contains terms DSRC, DSRCS, OBU, RSU as defined outside IETF. Some of them are used in the main Terminology section.
- Added two paragraphs explaining that ND and Mobile IPv6 have problems working over 802.11-OCB, yet their adaptations is not specified in this document.

From draft-ietf-ipwave-ipv6-over-80211ocb-12 to draft-ietf-ipwave-ipv6-over-80211ocb-13
- Substituted "IP-OBU" for "OBRU", and "IP-RSU" for "RSRU" throughout and improved OBU-related definitions in the Terminology section.

From draft-ietf-ipwave-ipv6-over-80211ocb-11 to draft-ietf-ipwave-ipv6-over-80211ocb-12
Improved the appendix about "MAC Address Generation" by expressing the technique to be an optional suggestion, not a mandatory mechanism.

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

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

From draft-ietf-ipwave-ipv6-over-80211ocb-09 to draft-ietf-ipwave-ipv6-over-80211ocb-10

- Removed text requesting a new Group ID for multicast for OCB.
- Added a clarification of the meaning of value "3333" in the section Address Mapping -- Multicast.
- Added note clarifying that in Europe the regional authority is not ETSI, but "ECC/CEPT based on ENs from ETSI".
- Added note stating that the manner in which two STAtions set their communication channel is not described in this document.
- Added a time qualifier to state that the "each node is represented uniquely at a certain point in time."
- Removed text "This section may need to be moved" (the "Reliability Requirements" section). This section stays there at this time.
- In the term definition "802.11-OCB" added a note stating that "any implementation should comply with standards and regulations set in the different countries for using that frequency band."
- In the RSU term definition, added a sentence explaining the difference between RSU and RSRU: in terms of number of interfaces and IP forwarding.
- Replaced "with at least two IP interfaces" with "with at least two real or virtual IP interfaces".
- Added a term in the Terminology for "OBU". However the definition is left empty, as this term is defined outside IETF.
- Added a clarification that it is an OBU or an OBRU in this phrase "A vehicle embarking an OBU or an OBRU".
Checked the entire document for a consistent use of terms OBU and OBRU.

Added note saying that "'p' is a letter identifying the Amendment".

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


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

Minor typographical errors.

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

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

Moved the EPD description to an Appendix on its own.

Shortened the Introduction and the Abstract.

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

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

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

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

Added term definition for WiFi.

Updated the authorship and expanded the Contributors section.

Corrected typographical errors.
From draft-ietf-ipwave-ipv6-over-80211ocb-07 to draft-ietf-ipwave-ipv6-over-80211ocb-08

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

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

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

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

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

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

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

Added mention of external (OCB) and internal network (stable), in the subnet structure section.

Added phrase explaining that both .11 Data and .11 QoS Data headers are currently being used, and may be used in the future.

Moved the packet capture example into an Appendix Implementation Status.

Suggested moving the reliability requirements appendix out into another document.

Added a IANA Considerations section, with content, requesting for a new multicast group "all OCB interfaces".

Added new OBU term, improved the RSU term definition, removed the ETTC term, replaced more occurrences of 802.11p, 802.11-OCB with 802.11-OCB.

References:
* Added an informational reference to ETSI’s IPv6-over-GeoNetworking.
* Added more references to IETF and ETSI security protocols.
* Updated some references from I-D to RFC, and from old RFC to new RFC numbers.
* Added reference to multicast extensions to IPsec architecture RFC.
* Added a reference to 2464-bis.
* Removed FCC informative references, because not used.

Updated the affiliation of one author.

Reformulation of some phrases for better readability, and correction of typographical errors.

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

Removed a few informative references pointing to Dx draft IEEE 1609 documents.
o Removed outdated informative references to ETSI documents.

o Added citations to IEEE 1609.2, .3 and .4-2016.

o Minor textual issues.

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

o Keep the previous text on multiple addresses, so remove talk about MIPv6, NEMOv6 and MCoA.

o Clarified that a 'Beacon' is an IEEE 802.11 frame Beacon.

o Clarified the figure showing Infrastructure mode and OCB mode side by side.

o Added a reference to the IP Security Architecture RFC.

o Detailed the IPv6-per-channel prohibition paragraph which reflects the discussion at the last IETF IPWAVE WG meeting.

o Added section "Address Mapping -- Unicast".

o Added the "8.11 Trailer" to pictures of 802.11 frames.

o Added text about SNAP carrying the Ethertype.

o New RSU definition allowing for it be both a Router and not necessarily a Router some times.

o Minor textual issues.

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

o Replaced almost all occurrences of 802.11p with 802.11-OCB, leaving only when explanation of evolution was necessary.

o Shortened by removing parameter details from a paragraph in the Introduction.

o Moved a reference from Normative to Informative.

o Added text in intro clarifying there is no handover spec at IEEE, and that 1609.2 does provide security services.
o Named the contents the fields of the EthernetII header (including the Ethertype bitstring).

o Improved relationship between two paragraphs describing the increase of the Sequence Number in 802.11 header upon IP fragmentation.

o Added brief clarification of "tracking".

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

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

o Introduced an appendix listing for information the set of 802.11 messages that may be transmitted in OCB mode.

o Removed appendix sections "Privacy Requirements", "Authentication Requirements" and "Security Certificate Generation".

o Removed appendix section "Non IP Communications".

o Introductory phrase in the Security Considerations section.

o Improved the definition of "OCB".

o Introduced theoretical stacked layers about IPv6 and IEEE layers including EPD.

o Removed the appendix describing the details of prohibiting IPv6 on certain channels relevant to 802.11-OCB.

o Added a brief reference in the privacy text about a precise clause in IEEE 1609.3 and .4.

o Clarified the definition of a Road Side Unit.

o Removed the discussion about security of WSA (because is non-IP).

o Removed mentioning of the GeoNetworking discussion.

o Moved references to scientific articles to a separate 'overview' draft, and referred to it.
Appendix B. 802.11p

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

Appendix C. Aspects introduced by the OCB mode to 802.11

In the IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. In OCB mode, the manner in which channels are selected and used is simplified compared to when in BSS mode. Contrary to BSS mode, at link layer, it is necessary to set statically the same channel number (or frequency) on two stations that need to communicate with each other (in BSS mode this channel set operation is performed automatically during 'scanning'). The manner in which stations set their channel number in OCB mode is not specified in this document. Stations STA1 and STA2 can exchange IP packets only if they are set on the same channel. At IP layer, they then discover each other by using the IPv6 Neighbor Discovery protocol. The allocation of a particular channel for a particular use is defined statically in standards authored by ETSI (in Europe), FCC in America, and similar organisations in South Korea, Japan and other parts of the world.

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

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

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

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

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

(i) 802.11 Infrastructure mode (ii) 802.11-OCB mode
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Changes needed on the network stack in OCB mode:

- Physical layer:
  - The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.
  - The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).
  - The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules, if used by the kernel to enforce local specific
restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

MAC layer:

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

Appendix E. Protocol Layering

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

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

Appendix G. IEEE 802.11 Messages Transmitted in OCB mode

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

- The STA may send management frames of subtype Action and, if the STA maintains a TSF Timer, subtype Timing Advertisement;
- The STA may send control frames, except those of subtype PS-Poll, CF-End, and CF-End plus CFAck;
- The STA may send data frames of subtype Data, Null, QoS Data, and QoS Null.
This section describes an example of an IPv6 Packet captured over a IEEE 802.11-OCB link.

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

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

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

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

Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.
H.1. Capture in Monitor Mode

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

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

Radiotap Header v0

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

IEEE 802.11 Data Header

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

Logical-Link Control Header

+-----------------+-----------------+-----------------|
| DSAP |I| SSAP |C| Control field | Org. code... |
+-----------------+-----------------+-----------------|
| ... Organizational Code | Type |
+-----------------+-----------------+-----------------|
IPv6 Base Header

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

Source Address

Destination Address

Router Advertisement

+----------------------------------+
| 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.

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

H.2. Capture in Normal Mode

The same IPv6 Router Advertisement packet described above (monitor mode) is captured on the Host, in the Normal mode, and depicted below.
One notices that the Radiotap Header, the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On the other hand, a new header named Ethernet II Header is present.

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

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

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

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

Appendix I. Extra Terminology

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

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

DSRCS (Dedicated Short-Range Communications Services): a term defined outside the IETF. The use of radio techniques to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments. DSRCS systems may also transmit status and instructional messages related to the unit involved. [Ref. 47 CFR 90.7 - Definitions]
OBU (On-Board Unit): a term defined outside the IETF. An On-Board Unit is a DSRCS transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of the respective chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of the respective chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands. - [CFR 90.7 - Definitions].

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

Authors’ Addresses

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

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

Nabil Benamar
Moulay Ismail University
Morocco

Phone: +212670832236
Email: n.benamar@est.umi.ac.ma
Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

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

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

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr
Abstract

This document provides methods and settings, and describes limitations, for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link with minimal change to existing stacks. Optimizations and usage of IPv6 over more complex scenarios is not covered and is subject of future work.

Status of This Memo

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

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

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

This Internet-Draft will expire on December 9, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

1. Introduction ........................................... 3
2. Terminology ........................................... 3
3. Communication Scenarios where IEEE 802.11-OCB Links are Used 4
4. IPv6 over 802.11-OCB ..................................... 4
   4.1. Maximum Transmission Unit (MTU) ..................... 4
   4.2. Frame Format ....................................... 4
   4.3. Link-Local Addresses ............................... 5
   4.4. Stateless Autoconfiguration ......................... 5
   4.5. Address Mapping ..................................... 6
   4.5.1. Address Mapping -- Unicast ....................... 6
   4.5.2. Address Mapping -- Multicast ..................... 6
   4.6. Subnet Structure .................................... 7
5. Security Considerations .................................. 8
   5.1. Privacy Considerations .............................. 8
   5.1.1. Privacy Risks of Meaningful info in Interface IDs .. 9
   5.2. MAC Address and Interface ID Generation ............ 9
   5.3. Pseudonym Handling .................................. 10
6. IANA Considerations ..................................... 10
7. Contributors ............................................ 10
8. Acknowledgements ....................................... 11
9. References ............................................. 11
   9.1. Normative References ................................ 11
   9.2. Informative References .............................. 14
Appendix A. 802.11p ........................................... 16
Appendix B. Aspects introduced by the OCB mode to 802.11 .... 16
Appendix C. Changes Needed on a software driver 802.11a to become a 802.11-OCB driver .... 21
Appendix D. Protocol Layering ................................ 22
Appendix E. Design Considerations ............................. 23
Appendix F. IEEE 802.11 Messages Transmitted in OCB mode .... 23
Appendix G. Examples of Packet Formats ........................ 23
   G.1. Capture in Monitor Mode ............................. 24
   G.2. Capture in Normal Mode .............................. 27
Appendix H. Extra Terminology ................................ 29
Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links .................................. 30
Authors’ Addresses ........................................ 32
1. Introduction

This document provides a baseline with limitations for using IPv6 to communicate among nodes in range of one another over a single IEEE 802.11-OCB link [IEEE-802.11-2016] (a.k.a "802.11p" see Appendix A, Appendix B and Appendix C) with minimal change to existing stacks. This document describes the layering of IPv6 networking on top of the IEEE Std 802.11 MAC layer or an IEEE Std 802.3 MAC layer with a frame translation underneath. The resulting stack operates over 802.11-OCB and provides at least P2P connectivity using IPv6 ND and link-local addresses. ND Extensions and IPWAVE optimizations for vehicular communications are not in scope. The expectation is that further specs will elaborate for more complex vehicular networking scenarios.

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

- Exceptions due to different operation of IPv6 network layer on 802.11 than on Ethernet. The operation of IP on Ethernet is described in [RFC1042], [RFC2464] .

- Exceptions due to the OCB nature of 802.11-OCB compared to 802.11. This has impacts on security, privacy, subnet structure and movement detection. For security and privacy recommendations see Section 5 and Section 4.4. The subnet structure is described in Section 4.6. The movement detection on OCB links is not described in this document.

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

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

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

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

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

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

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

The IEEE 802.11-OCB Networks are used for vehicular communications, as 'Wireless Access in Vehicular Environments'. In particular, we refer the reader to [I-D.ietf-ipwave-vehicular-networking], that lists some scenarios and requirements for IP in Intelligent Transportation Systems.

The link model is the following: STA --- 802.11-OCB --- STA. In vehicular networks, STAs can be IP-RSUs and/or IP-OBUs. All links are assumed to be P2P and multiple links can be on one radio interface. While 802.11-OCB is clearly specified, and a legacy IPv6 stack can operate on such links, the use of the operating environment (vehicular networks) brings in new perspectives.

4. IPv6 over 802.11-OCB

4.1. Maximum Transmission Unit (MTU)

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

4.2. Frame Format

IP packets MUST be transmitted over 802.11-OCB media as QoS Data frames whose format is specified in IEEE 802.11 spec [IEEE-802.11-2016].
The IPv6 packet transmitted on 802.11-OCB are immediately preceded by a Logical Link Control (LLC) header and an 802.11 header. In the LLC header, and in accordance with the EtherType Protocol Discrimination (EPD, see Appendix D), the value of the Type field MUST be set to 0x86DD (IPv6). The mapping to the 802.11 data service MUST use a ‘priority’ value of 1, which specifies the use of QoS with a ‘Background’ user priority.

To simplify the Application Programming Interface (API) between the operating system and the 802.11-OCB media, device drivers MAY implement IPv6 over Ethernet per RFC 2464 and then a frame translation from 802.3 to 802.11 in order to minimize the code changes.

4.3. Link-Local Addresses

There are several types of IPv6 addresses [RFC4291], [RFC4193], that MAY be assigned to an 802.11-OCB interface. Among these types of addresses only the IPv6 link-local addresses MAY be formed using an EUI-64 identifier, in particular during transition time.

If the IPv6 link-local address is formed using an EUI-64 identifier, then the mechanism of forming that address is the same mechanism as used to form an IPv6 link-local address on Ethernet links. This mechanism is described in section 5 of [RFC2464].

4.4. Stateless Autoconfiguration

The steps a host takes in deciding how to autoconfigure its interfaces in IP version 6 are described in [RFC4862]. This section describes the formation of Interface Identifiers for IPv6 addresses of type ‘Global’ or ‘Unique Local’. For Interface Identifiers for IPv6 address of type ‘Link-Local’ see Section 4.3.

The RECOMMENDED method for forming stable Interface Identifiers (IID) is described in [RFC8064]. The method of forming IIDs described in section 4 of [RFC2464] MAY be used during transition time, in particular for IPv6 link-local addresses.

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

Semantically opaque Interface Identifiers, instead of meaningful Interface Identifiers derived from a valid and meaningful MAC address ([RFC2464], section 4), help avoid certain privacy risks (see the
If semantically opaque Interface Identifiers are needed, they MAY be generated using the method for generating semantically opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration given in [RFC7217]. Typically, an opaque Interface Identifier is formed starting from identifiers different than the MAC addresses, and from cryptographically strong material. Thus, privacy sensitive information is absent from Interface IDs, because it is impossible to calculate back the initial value from which the Interface ID was first generated (intuitively, it is as hard as mentally finding the square root of a number, and as impossible as trying to use computers to identify quickly whether a large number is prime).

Some applications that use IPv6 packets on 802.11-OCB links (among other link types) may benefit from IPv6 addresses whose Interface Identifiers don’t change too often. It is RECOMMENDED to use the mechanisms described in RFC 7217 to permit the use of Stable Interface Identifiers that do not change within one subnet prefix. A possible source for the Net-Iface Parameter is a virtual interface name, or logical interface name, that is decided by a local administrator.

4.5. Address Mapping

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

4.5.1. Address Mapping -- Unicast

This draft is scoped for AR and DAD per RFC 4861 [RFC4861].

4.5.2. Address Mapping -- Multicast

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

Transmitting IPv6 packets to multicast destinations over 802.11 links proved to have some performance issues [I-D.ietf-mboned-ieee802-mcast-problems]. These issues may be exacerbated in OCB mode. A future improvement to this specification SHOULD consider solutions for these problems.
4.6. Subnet Structure

A subnet may be formed over 802.11-OCB interfaces of vehicles that are in close range (not by their in-vehicle interfaces). A Prefix List conceptual data structure ([RFC4861] section 5.1) is maintained for each 802.11-OCB interface.

An IPv6 subnet on which Neighbor Discovery protocol (ND) can be mapped on an OCB network iff all nodes share a single broadcast Domain, which is generally the case for P2P OCB links; The extension to IPv6 ND operating on a subnet that covers multiple OCB links and not fully overlapping (NBMA) is not in scope.

The structure of this subnet is ephemeral, in that it is strongly influenced by the mobility of vehicles: the hidden terminal effects appear; the 802.11 networks in OCB mode may be considered as ‘ad-hoc’ networks with an addressing model as described in [RFC5889]. On another hand, the structure of the internal subnets in each car is relatively stable.

As recommended in [RFC5889], when the timing requirements are very strict (e.g. fast drive through IP-RSU coverage), no on-link subnet prefix should be configured on an 802.11-OCB interface. In such cases, the exclusive use of IPv6 link-local addresses is RECOMMENDED.

Additionally, even if the timing requirements are not very strict (e.g. the moving subnet formed by two following vehicles is stable, a fixed IP-RSU is absent), the subnet is disconnected from the Internet (a default route is absent), and the addressing peers are equally qualified (impossible to determine that some vehicle owns and distributes addresses to others) the use of link-local addresses is RECOMMENDED.

The baseline Neighbor Discovery protocol (ND) [RFC4861] MUST be supported over 802.11-OCB links. Transmitting ND packets may prove to have some performance issues see Section 4.5.2, and Appendix I. These issues may be exacerbated in OCB mode. Solutions for these problems SHOULD consider the OCB mode of operation. Future solutions to OCB should consider solutions for avoiding broadcast. The best of current knowledge indicates the kinds of issues that may arise with ND in OCB mode; they are described in Appendix I.

Protocols like Mobile IPv6 [RFC6275], [RFC3963] and DNAv6 [RFC6059], which depend on timely movement detection, might need additional tuning work to handle the lack of link-layer notifications during handover. This is for further study.
5. Security Considerations

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

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

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

The potential attack vectors are: MAC address spoofing, IP address and session hijacking, and privacy violation Section 5.1. A previous work at SAVI WG presents some threats [RFC6959], while SeND presented in [RFC3971] and [RFC3972] is a solution against address theft but it is complex and not deployed.

More IETF protocols are available in the toolbox of the IP security protocol designer. Certain ETSI protocols related to security protocols in Intelligent Transportation Systems are described in [ETSI-sec-archi].

5.1. Privacy Considerations

As with all Ethernet and 802.11 interface identifiers ([RFC7721]), the identifier of an 802.11-OCB interface may involve privacy, MAC address spoofing and IP address hijacking risks. A vehicle embarking an IP-OBU whose egress interface is 802.11-OCB may expose itself to eavesdropping and subsequent correlation of data; this may reveal data considered private by the vehicle owner; there is a risk of being tracked. In outdoors public environments, where vehicles typically circulate, the privacy risks are more important than in indoors settings. It is highly likely that attacker sniffers are deployed along routes which listen for IEEE frames, including IP packets, of vehicles passing by. For this reason, in the 802.11-OCB deployments, there is a strong necessity to use protection tools such
as dynamically changing MAC addresses Section 5.2, semantically opaque Interface Identifiers and stable Interface Identifiers Section 4.4. This may help mitigate privacy risks to a certain level.

5.1.1. Privacy Risks of Meaningful info in Interface IDs

The privacy risks of using MAC addresses displayed in Interface Identifiers are important. The IPv6 packets can be captured easily in the Internet and on-link in public roads. For this reason, an attacker may realize many attacks on privacy. One such attack on 802.11-OCB is to capture, store and correlate Company ID information present in MAC addresses of many cars (e.g. listen for Router Advertisements, or other IPv6 application data packets, and record the value of the source address in these packets). Further correlation of this information with other data captured by other means, or other visual information (car color, others) MAY constitute privacy risks.

5.2. MAC Address and Interface ID Generation

In 802.11-OCB networks, the MAC addresses MAY change during well defined renumbering events. In the moment the MAC address is changed on an 802.11-OCB interface all the Interface Identifiers of IPv6 addresses assigned to that interface MUST change.

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

A ‘randomized’ MAC address has the following characteristics:

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

To meet the randomization requirements for the 46 remaining bits, a hash function may be used. For example, the SHA256 hash function may be used with input a 256 bit local secret, the ‘nominal’ MAC Address of the interface, and a representation of the date and time of the renumbering event.
A randomized Interface ID has the same characteristics of a randomized MAC address, except the length in bits. An Interface ID SHOULD be of length specified in other documents.

5.3. Pseudonym Handling

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

- Particular challenges arise when the pseudonymization mechanism used relies on (randomized) re-addressing.
- A proper pseudonymization tool operated by a trusted third party may be needed to ensure both aspects simultaneously (privacy protection on one hand and trust between participants on another hand).
- This is discussed in Section 4.4 and Section 5 of this document.
- Pseudonymity is also discussed in [I-D.ietf-ipwave-vehicular-networking] in its sections 4.2.4 and 5.1.2.

6. IANA Considerations

No request to IANA.

7. Contributors

Christian Huitema, Tony Li.

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

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

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

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

The authors would like to thank Alexandre Petrescu for initiating this work and for being the lead author until the version 43 of this draft.

The authors would like to thank Pascal Thubert for reviewing, proofreading and suggesting modifications of this document.

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

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

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

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

Human Rights Protocol Considerations review by Amelia Andersdotter.

9. References

9.1. Normative References


9.2. Informative References

[ETSI-sec-archi]

[I-D.ietf-ipwave-vehicular-networking]

[I-D.ietf-mboned-ieee802-mcast-problems]

[IEEE-1609.2]

[IEEE-1609.3]

[IEEE-1609.4]
Appendix A. 802.11p

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

Appendix B. Aspects introduced by the OCB mode to 802.11

In the IEEE 802.11-OCB mode, all nodes in the wireless range can directly communicate with each other without involving authentication or association procedures. In OCB mode, the manner in which channels are selected and used is simplified compared to when in BSS mode. Contrary to BSS mode, at link layer, it is necessary to set statically the same channel number (or frequency) on two stations that need to communicate with each other (in BSS mode this channel set operation is performed automatically during 'scanning').
manner in which stations set their channel number in OCB mode is not 
specified in this document. Stations STA1 and STA2 can exchange IP 
packets only if they are set on the same channel. At IP layer, they 
then discover each other by using the IPv6 Neighbor Discovery 
protocol. The allocation of a particular channel for a particular 
use is defined statically in standards authored by ETSI (in Europe), 
FCC in America, and similar organisations in South Korea, Japan and 
other parts of the world.

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

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

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

The message exchange diagram in Figure 1 illustrates a comparison 
between traditional 802.11 and 802.11 in OCB mode. The ‘Data’ 
messages can be IP packets such as HTTP or others. Other 802.11 
management and control frames (non IP) may be transmitted, as 
specified in the 802.11 standard. For information, the names of 
these messages as currently specified by the 802.11 standard are 
listed in Appendix F.
The interface 802.11-OCB was specified in IEEE Std 802.11p (TM) -2010 [IEEE-802.11p-2010] as an amendment to IEEE Std 802.11 (TM) -2007, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, this amendment has been integrated in IEEE 802.11(TM) -2012 and -2016 [IEEE-802.11-2016].

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

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

(i) 802.11 Infrastructure mode  (ii) 802.11-OCB mode

Figure 1: Difference between messages exchanged on 802.11 (left) and 802.11-OCB (right)
The 802.11-OCB links are specified to be compatible as much as possible with the behaviour of 802.11a/b/g/n and future generation IEEE WLAN links. From the IP perspective, an 802.11-OCB MAC layer offers practically the same interface to IP as the 802.11a/b/g/n and 802.3. A packet sent by an IP-OBU may be received by one or multiple IP-RSUs. The link-layer resolution is performed by using the IPv6 Neighbor Discovery protocol.

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

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

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

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

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

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

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

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

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

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

Changes needed on the network stack in OCB mode:

- Physical layer:
  * The chip must use the Orthogonal Frequency Multiple Access (OFDM) encoding mode.
  * The chip must be set in half-mode rate mode (the internal clock frequency is divided by two).
  * The chip must use dedicated channels and should allow the use of higher emission powers. This may require modifications to the local computer file that describes regulatory domains rules, if used by the kernel to enforce local specific restrictions. Such modifications to the local computer file must respect the location-specific regulatory rules.

- MAC layer:
  * All management frames (beacons, join, leave, and others) emission and reception must be disabled except for frames of subtype Action and Timing Advertisement (defined below).
* No encryption key or method must be used.

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

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

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

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

Appendix D. Protocol Layering

A more theoretical and detailed view of layer stacking, and interfaces between the IP layer and 802.11-OCB layers, is illustrated in Figure 2. The IP layer operates on top of the EtherType Protocol Discrimination (EPD); this Discrimination layer is described in IEEE Std 802.3-2012; the interface between IPv6 and EPD is the LLC_SAP (Link Layer Control Service Access Point).

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

Figure 2: EtherType Protocol Discrimination
Appendix E. Design Considerations

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

Appendix F. IEEE 802.11 Messages Transmitted in OCB mode

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

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

Appendix G. Examples of Packet Formats

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

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

We describe an experiment of capturing an IPv6 packet on an 802.11-OCB link. In topology depicted in Figure 3, the packet is an IPv6 Router Advertisement. This packet is emitted by a Router on its 802.11-OCB interface. The packet is captured on the Host, using a network protocol analyzer (e.g. Wireshark); the capture is performed in two different modes: direct mode and 'monitor' mode. The topology used during the capture is depicted below.

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

![Figure 3: Topology for capturing IP packets on 802.11-OCB]

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

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

G.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

<table>
<thead>
<tr>
<th>Type/Subtype and Frame Ctrl</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receiver Address...</td>
<td></td>
</tr>
<tr>
<td>... Receiver Address</td>
<td>Transmitter Address...</td>
</tr>
<tr>
<td>... Transmitter Address</td>
<td></td>
</tr>
<tr>
<td>BSS Id...</td>
<td></td>
</tr>
<tr>
<td>... BSS Id</td>
<td>Frag Number and Seq Number</td>
</tr>
</tbody>
</table>

Logical-Link Control Header

<table>
<thead>
<tr>
<th>DSAP</th>
<th>I</th>
<th>SSAP</th>
<th>C</th>
<th>Control field</th>
<th>Org. code...</th>
</tr>
</thead>
<tbody>
<tr>
<td>... Organizational Code</td>
<td>Type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv6 Base Header

<table>
<thead>
<tr>
<th>Version</th>
<th>Traffic Class</th>
<th>Flow Label</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Payload Length</td>
<td>Next Header</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Destination Address

Routing Advertisement
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 33:33:00:00:00:01 (all-nodes multicast address). The value of the BSS Id field is ff:ff:ff:ff:ff:ff, which is recognized by the network protocol analyzer as being "broadcast". The Fragment number and sequence number fields are together set to 0x90C6.

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

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

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

The Ethernet Type field in the logical-link control header is set to 0x86dd which indicates that the frame transports an IPv6 packet. In the IEEE 802.11 data, the destination address is 33:33:00:00:00:01 which is the corresponding multicast MAC address. The BSS id is a broadcast address of ff:ff:ff:ff:ff:ff. Due to the short link duration between vehicles and the roadside infrastructure, there is no need in IEEE 802.11-OCB to wait for the completion of association and authentication procedures before exchanging data. IEEE 802.11-OCB enabled nodes use the wildcard BSSID (a value of all 1s) and may start communicating as soon as they arrive on the communication channel.
G.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...
| ...
| 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, the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On the other hand, a new header named Ethernet II Header is present.

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

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

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

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

Appendix H. Extra Terminology

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

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

DSRCS (Dedicated Short-Range Communications Services): a term defined outside the IETF. The use of radio techniques to transfer data over short distances between roadside and mobile units, between mobile units, and between portable and mobile units to perform operations related to the improvement of traffic flow, traffic safety, and other intelligent transportation service applications in a variety of environments. DSRCS systems may also transmit status and instructional messages related to the units involved. [Ref. 47 CFR 90.7 - Definitions]
OBU (On-Board Unit): a term defined outside the IETF. An On-Board Unit is a DSRC transceiver that is normally mounted in or on a vehicle, or which in some instances may be a portable unit. An OBU can be operational while a vehicle or person is either mobile or stationary. The OBUs receive and contend for time to transmit on one or more radio frequency (RF) channels. Except where specifically excluded, OBU operation is permitted wherever vehicle operation or human passage is permitted. The OBUs mounted in vehicles are licensed by rule under part 95 of the respective chapter and communicate with Roadside Units (RSUs) and other OBUs. Portable OBUs are also licensed by rule under part 95 of the respective chapter. OBU operations in the Unlicensed National Information Infrastructure (UNII) Bands follow the rules in those bands. - [CFR 90.7 - Definitions].

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

Appendix I. Neighbor Discovery (ND) Potential Issues in Wireless Links

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861][RFC4862] was designed for point-to-point and transit links such as Ethernet, with the expectation of a cheap and reliable support for multicast from the lower layer. Section 3.2 of RFC 4861 indicates that the operation on Shared Media and on non-broadcast multi-access (NBMA) networks require additional support, e.g., for Address Resolution (AR) and duplicate address detection (DAD), which depend on multicast. An infrastructureless radio network such as OCB shares properties with both Shared Media and NBMA networks, and then adds its own complexity, e.g., from movement and interference that allow only transient and non-transitive reachability between any set of peers.

The uniqueness of an address within a scoped domain is a key pillar of IPv6 and the base for unicast IP communication. RFC 4861 details the DAD method to avoid that an address is duplicated. For a link local address, the scope is the link, whereas for a Globally Reachable address the scope is much larger. The underlying assumption for DAD to operate correctly is that the node that owns an
IPv6 address can reach any other node within the scope at the time it claims its address, which is done by sending a NS multicast message, and can hear any future claim for that address by another party within the scope for the duration of the address ownership.

In the case of OCB, there is a potentially a need to define a scope that is compatible with DAD, and that cannot be the set of nodes that a transmitter can reach at a particular time, because that set varies all the time and does not meet the DAD requirements for a link local address that could possibly be used anytime, anywhere. The generic expectation of a reliable multicast is not ensured, and the operation of DAD and AR (Address Resolution) as specified by RFC 4861 cannot be guaranteed. Moreover, multicast transmissions that rely on broadcast are not only unreliable but are also often detrimental to unicast traffic (see [draft-ietf-mboned-ieee802-mcast-problems]).

Early experience indicates that it should be possible to exchange IPv6 packets over OCB while relying on IPv6 ND alone for DAD and AR (Address Resolution) in good conditions. However, this does not apply if TBD TBD TBD. In the absence of a correct DAD operation, a node that relies only on IPv6 ND for AR and DAD over OCB should ensure that the addresses that it uses are unique by means others than DAD. It must be noted that deriving an IPv6 address from a globally unique MAC address has this property but may yield privacy issues.

RFC 8505 provides a more recent approach to IPv6 ND and in particular DAD. RFC 8505 is designed to fit wireless and otherwise constrained networks whereby multicast and/or continuous access to the medium may not be guaranteed. RFC 8505 Section 5.6 "Link-Local Addresses and Registration" indicates that the scope of uniqueness for a link local address is restricted to a pair of nodes that use it to communicate, and provides a method to assert the uniqueness and resolve the link-Layer address using a unicast exchange.

RFC 8505 also enables a router (acting as a 6LR) to own a prefix and act as a registrar (acting as a 6LBR) for addresses within the associated subnet. A peer host (acting as a 6LN) registers an address derived from that prefix and can use it for the lifetime of the registration. The prefix is advertised as not onlink, which means that the 6LN uses the 6LR to relay its packets within the subnet, and participation to the subnet is constrained to the time of reachability to the 6LR. Note that RSU that provides internet connectivity MAY announce a default router preference [RFC 4191], whereas a car that does not provide that connectivity MUST NOT do so. This operation presents similarities with that of an access point, but at Layer-3. This is why RFC 8505 well-suited for wireless in general.
Support of RFC 8505 is may be implemented on OCB. OCB nodes that support RFC 8505 would support the 6LN operation in order to act as a host, and may support the 6LR and 6LBR operations in order to act as a router and in particular own a prefix that can be used by RFC 8505-compliant hosts for address autoconfiguration and registration.

Authors’ Addresses

Nabil Benamar  
Moulay Ismail University  
Morocco  
Phone: +212670832236  
Email: n.benamar@est.umi.ac.ma

Jerome Haerri  
Eurecom  
Sophia-Antipolis 06904  
France  
Phone: +33493008134  
Email: Jerome.Haerri@eurecom.fr

Jong-Hyouk Lee  
Sangmyung University  
31, Sangmyeongdae-gil, Dongnam-gu  
Cheonan 31066  
Republic of Korea  
Email: jonghyouk@smu.ac.kr

Thierry Ernst  
YoGoKo  
France  
Email: thierry.ernst@yogoko.fr
Problem Statement for IP Wireless Access in Vehicular Environments
draft-ietf-ipwave-problem-statement-00

Abstract

This document provides a problem statement for IP Wireless Access in Vehicular Environments (IPWAVE), that is, vehicular networks. This document addresses the extension of IPv6 as the network layer protocol in vehicular networks. It deals with networking issues in one-hop communication between a Road-Side Unit (RSU) and a vehicle, that is, "vehicle-to-infrastructure" (V2I) communication. It also deals with one-hop communication between two neighboring vehicles, that is, "vehicle-to-vehicle" (V2V) communication. Major issues about IPv6 in vehicular networks include neighbor discovery protocol, stateless address autoconfiguration, and DNS configuration for Internet connectivity. When a vehicle and an RSU have an internal network (respectively), the document discusses internetworking issues between two internal networks through either V2I or V2V communication. Those issues include prefix discovery, prefix exchange, service discovery, security, and privacy.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."
The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 4, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

1.  Introduction .................................................. 3
2.  Requirements Language ....................................... 4
3.  Terminology .................................................. 4
4.  Overview ...................................................... 5
5.  Internetworking between Vehicle Network and RSU Network .... 6
   5.1.  V2I-Based Internetworking ............................... 6
   5.2.  The Use Cases of V2I-Based Internetworking ............. 7
6.  Internetworking between Two Vehicle Networks ................ 8
   6.1.  V2V-Based Internetworking ............................... 8
   6.2.  The Use Cases of V2V-Based Internetworking ............. 9
7.  IPv6 Addressing ............................................. 10
8.  Neighbor Discovery .......................................... 10
9.  IP Address Autoconfiguration ................................ 11
10. DNS Naming Service ........................................... 11
11. IP Mobility Management ...................................... 12
12. Service Discovery ............................................ 12
13. Security Considerations ..................................... 13
14. Contributors .................................................. 13
15. Acknowledgments .............................................. 13
16. References .................................................... 14
   16.1. Normative References .................................. 14
   16.2. Informative References ................................. 15

Jeong, et al. Expires January 4, 2018
1. Introduction

Recently, Vehicular Ad Hoc Networks (VANET) have been focusing on intelligent services in road networks, such as driving safety, efficient driving, and entertainment. For VANET, Dedicated Short-Range Communications (DSRC) [DSRC-WAVE] was standardized as Wireless Access in Vehicular Environments (WAVE) standards by IEEE. The WAVE standards include IEEE 802.11p [IEEE-802.11p] for WAVE Media Access Control (MAC) and Physical Layer (PHY), IEEE 1609.0 for WAVE architecture [WAVE-1609.0], IEEE 1609.2 for WAVE security services [WAVE-1609.2], IEEE 1609.3 for WAVE networking services [WAVE-1609.3], and IEEE 1609.4 for WAVE multi-channel operation [WAVE-1609.4]. 802.11p extends IEEE 802.11a [IEEE-802.11a] by consideration of vehicular characteristics such as a vehicle’s velocity and collision avoidance. IEEE 802.11p has been published as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012.

Now the deployment of VANET is indicated in real road environments along with the popularity of smart devices (e.g., smartphone and tablet). Many automobile vendors (e.g., Benz, BMW, Ford, Honda, and Toyota) now consider automobiles as computer systems instead of mechanical machines, since many current vehicles are operating with many sensors and software. Google has advanced self-driving vehicles with many special software modules and hardware devices to support computer-vision-based object recognition, machine-learning-based decision-making, and GPS navigation.

Vehicular networking research is enabling vehicles to communicate with each other and infrastructure nodes in the Internet by using TCP/IP, IP address autoconfiguration, routing, handover, and mobility management [ID-VN-Survey]. IPv6 [RFC2460] is suitable for vehicular networks since the protocol has abundant address space and autoconfiguration features, and can be extended by way of new protocol headers.

This document identifies issues of IPv6-based vehicle-to-infrastructure (V2I) networking and vehicle-to-vehicle (V2V) networking, such as IPv6 addressing [RFC4291], neighbor discovery [RFC4861], address autoconfiguration [RFC4862], and DNS naming service [RFC8106][RFC3646][ID-DNSNA]. This document also identifies issues of internetworking between two internal networks when a vehicle and/or an RSU have an internal network. Those issues include prefix discovery, prefix exchange, and service discovery in the inter-connected internal networks. In addition, the document analyzes the characteristics of vehicular networks to consider the design of V2I or V2V networking.
2. Requirements Language

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].

3. Terminology

This document uses the terminology described in [RFC4861] and [RFC4862]. In addition, five new terms are defined below:

- **Road-Side Unit (RSU):** A node that has a wireless communication device (e.g., DSRC) to communicate with vehicles and is connected to the Internet as a router or switch for packet forwarding. An RSU is deployed either at an intersection or in a road segment.

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

- **Fixed Network:** An RSU can have an internal network consisting of multiple subnets. This internal network is a fixed network since the RSU is fixed in the road network.

- **Moving Network:** A vehicle can have an internal network consisting of multiple subnets. This internal network is called a moving network since the vehicle is moving in the road network.

- **Traffic Control Center (TCC):** A node that maintains road infrastructure information (e.g., RSUs, traffic signals, and loop detectors), vehicular traffic statistics (e.g., average vehicle speed and vehicle inter-arrival time per road segment), and vehicle information (e.g., a vehicle’s identifier, position, direction, speed, and trajectory as a navigation path). TCC is included in a vehicular cloud for vehicular networks. Exemplary functions of TCC include the management of evacuation routes, the monitoring of pedestrians and bike traffic, the monitoring of real-time transit operations, and real-time responsive traffic signal systems. Thus, TCC is the nerve center of most freeway management systems such that data is collected, processed, and fused with other operational and control data, and is also synthesized to produce "information" distributed to stakeholders, other agencies, and traveling public. TCC is called Traffic Management Center (TMC) in the US. TCC can communicate with road infrastructure nodes (e.g., RSUs, traffic signals, and loop detectors) to share measurement data and management information by
an application-layer protocol.

4. Overview

This document provides a problem statement of IPv6-based V2I and V2V networking. The main focus is one-hop networking between a vehicle and an RSU or between two neighboring vehicles. However, this document does not address all multi-hop networking scenarios of vehicles and RSUs. Also, the problems focus on the network layer (i.e., IPv6 protocol stack) rather than the MAC layer and the transport layer (e.g., TCP, UDP, and SCTP).

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

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

Figure 1: The Network Configuration for Vehicular Networking
5. Internetworking between Vehicle Network and RSU Network

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

5.1. V2I-Based Internetworking

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

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

Once the network parameter discovery and prefix exchange operations are performed, unicast of packets can be supported between the vehicle’s moving network and the RSU’s fixed network. The DNS naming service should be supported for the DNS name resolution for hosts or servers residing either in the vehicle’s moving network or the RSU’s fixed network.

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

This document addresses the internetworking between the vehicle’s moving network and the RSU’s fixed network in Figure 2 and the
required enhancement of IPv6 protocol suite for the V2I networking service.

Figure 2: Internetworking between Vehicle Network and RSU Network

5.2. The Use Cases of V2I-Based Internetworking

The use cases of V2I networking include navigation service, fuel-efficient speed recommendation service, and accident notification service.

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

The emergency communication between accident vehicles (or emergency
vehicles) and TCC can be performed via either RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, such as emergency calls. The current RAN is mainly constructed by 4G-LTE, but DSRC-based vehicular networks can be used in near future.

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I networking can reduce the collision of a pedestrian and a vehicle, which have a smartphone, in a road network. Vehicles and pedestrians can communicate with each other via an RSU that delivers scheduling information for wireless communication to save the smartphones’ battery.

6. Internetworking between Two Vehicle Networks

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

6.1. V2V-Based Internetworking

In Figure 3, the prefix assignment for each subnet inside each vehicle’s mobile network is done through a prefix delegation protocol.
Figure 3 shows internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (RDNSS2), the two hosts (Host3 and Host4), and the two routers (Router3 and Router4). Vehicle1’s Router1 and Vehicle2’s Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking.

This document describes the internetworking between the moving networks of two neighboring vehicles in Figure 3 and the required enhancement of IPv6 protocol suite for the V2V networking service.

6.2. The Use Cases of V2V-Based Internetworking

The use cases of V2V networking include context-aware navigator for driving safety, cooperative adaptive cruise control in an urban roadway, and platooning in a highway. These are three techniques...
that will be important elements for self-driving.

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely by letting the drivers recognize dangerous obstacles and situations, including neighboring vehicles that might cause a collision.

Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps vehicles to adapt their speed autonomously according to the mobility of their predecessor and successor vehicles in an urban roadway or a highway.

Platooning [Truck-Platooning] allows a series of vehicles (e.g., trucks) to move together with a very short inter-distance. This platooning can maximize the throughput of vehicular traffic in a highway.

7. IPv6 Addressing

This section discusses IP addressing for the V2I and V2V networking. There are two approaches for IPv6 addressing in vehicular networks. The first is to use unique local IPv6 unicast addresses (ULAs) for vehicular networks [RFC4193]. The other is to use global IPv6 addresses for the interoperability with the Internet [RFC4291]. The former approach is often used by Mobile Ad Hoc Networks (MANET) for an isolated subnet. This approach can support the emergency notification service and navigation service in road networks. However, for general Internet services (e.g., email access, web surfing and entertainment services), the latter approach is required.

For global IP addresses, there are two choices: a multi-link subnet approach for multiple RSUs and a single subnet approach per RSU. In the multi-link subnet approach, which is similar to ULA for MANET, RSUs play a role of layer-2 (L2) switches and the router interconnected with the RSUs is required. The router maintains the location of each vehicle belonging to an RSU for L2 switching. In the single subnet approach per RSU, which is similar to the legacy subnet in the Internet, each RSU plays the role of a (layer-3) router.

8. Neighbor Discovery

Neighbor Discovery (ND) is a core part of IPv6 protocol suite [RFC4861]. This section discusses an extension of ND for V2I networking. The vehicles are moving fast within the communication coverage of an RSU. The external link between the vehicle and the RSU can be used for V2I networking, as shown in Figure 2.
ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval should be adjusted for high-speed vehicles and vehicle density. As vehicles move faster, the NA interval should decrease for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase for the NA messages to collide with other NA messages with lower collision probability.

9. IP Address Autoconfiguration

This section discusses IP address autoconfiguration for V2I networking. For IP address autoconfiguration, high-speed vehicles should also be considered. The legacy IPv6 stateless address autoconfiguration [RFC4862], as shown in Figure 1, may not perform well. This is because vehicles can travel through the communication coverage of the RSU faster than the completion of address autoconfiguration (with Router Advertisement and Duplicate Address Detection (DAD) procedures).

To mitigate the impact of vehicle speed on address configuration, the RSU can perform IP address autoconfiguration including the DAD proactively as an ND proxy on behalf of the vehicles. If vehicles periodically report their movement information (e.g., position, trajectory, speed, and direction) to TCC, TCC can coordinate the RSUs under its control for the proactive IP address configuration of the vehicles with the mobility information of the vehicles. DHCPv6 (or Stateless DHCPv6) can be used for the IP address autoconfiguration [RFC3315][RFC3736].

In the case of a single subnet per RSU, the delay to change IPv6 address through DHCPv6 procedure is not suitable since vehicles move fast. Some modifications are required for the high-speed vehicles that quickly crosses the communication coverages of multiple RSUs. Some modifications are required for both stateless address autoconfiguration and DHCPv6. Mobile IPv6 (MIPv6) can be used for the fast update of a vehicle’s care-of address for the current RSU to communicate with the vehicle [RFC6275].

10. DNS Naming Service

This section suggests a DNS naming service for V2I networking. The DNS naming service consists of the DNS name resolution and DNS name autoconfiguration.

The DNS name resolution translates a DNS name into the corresponding IPv6 address through a recursive DNS server (RDNSS) within the vehicle’s moving network and DNS servers in the Internet [RFC1034][RFC1035], which are located outside the VANET. The RDNSSes
can be advertised by RA DNS Option or DHCP DNS Option into the subnets within the vehicle’s moving network.

The DNS name autoconfiguration makes a unique DNS name for hosts within a vehicle’s moving network and registers it into a DNS server within the vehicle’s moving network [ID-DNSNA]. With Vehicle Identification Number (VIN), a unique DNS suffix can be constructed as a DNS domain for the vehicle’s moving network. Each host can generate its DNS name and register it into the local RDNSS in the vehicle’s moving network.

11. IP Mobility Management

This section discusses an IP mobility support in V2I networking. In a single subnet per RSU, vehicles continually cross the communication coverages of adjacent RSUs. During this crossing, TCP/UDP sessions can be maintained through IP mobility support, such as MIPv6 [RFC6275], Proxy MIPv6 [RFC5213][RFC5949], and Distributed Mobility Management (DMM) [RFC7333][RFC7429]. Since vehicles move fast along roadways, high speed should be enabled by the parameter configuration in the IP mobility management. With the periodic reports of the movement information from the vehicles, TCC can coordinate RSUs and other network components under its control for the proactive mobility management of the vehicles along the movement of the vehicles.

To support the mobility of a vehicle’s moving network, Network Mobility Basic Support Protocol (NEMO) can be used [RFC3963]. Like MIPv6, the high speed of vehicles should be considered for a parameter configuration in NEMO.

12. Service Discovery

Vehicles need to discover services (e.g., road condition notification, navigation service, and entertainment) provided by infrastructure nodes in a fixed network via RSU, as shown in Figure 2. During the passing of an intersection or road segment with an RSU, vehicles should perform this service discovery quickly.

Since with the existing service discovery protocols, such as DNS-based Service Discovery (DNS-SD) [RFC6763] and Multicast DNS (mDNS) [RFC6762], the service discovery will be performed with message exchanges, the discovery delay may hinder the prompt service usage of the vehicles from the fixed network via RSU. One feasible approach is a piggyback service discovery during the prefix exchange of network prefixes for the networking between a vehicle’s moving network and an RSU’s fixed network. That is, the message of the prefix exchange can include service information, such as each service’s IP address, transport layer protocol, and port number.
IPv6 ND can be extended for the prefix and service discovery [ID-Vehicular-ND]. Vehicles and RSUs can announce the network prefixes and services in their internal network via ND messages containing ND options with the prefix and service information. Since it does not need any additional service discovery protocol in the application layer, this ND-based approach can provide vehicles and RSUs with the rapid discovery of the network prefixes and services.

13. Security Considerations

Security and privacy are paramount in the V2I and V2V networking in VANET. Only authorized vehicles should be allowed to use the V2I and V2V networking in VANET. A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device’s identifier generation can be used to authenticate a vehicle and the user through a road infrastructure node, such as an RSU connected to an authentication server in TCC. Transport Layer Security (TLS) certificates can also be used for secure vehicle communications.

A security scheme providing authentication and access control should be provided in vehicular networks [VN-Security]. With this scheme, the security and privacy can be supported for safe and reliable data services in vehicular networks.

To prevent an adversary from tracking a vehicle by with its MAC address or IPv6 address, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the communications between a vehicle and an RSU.

To protect packets exchanged between a vehicle and an RSU, packets should be encrypted. To assure confidentiality, efficient encryption and decryption algorithms can be used along with a key management scheme such as Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [Securing-VCOMM].

14. Contributors

IPWAVE is a group effort. The following people actively contributed to the problem statement text: Nabil Benamar (Moulay Ismail University), Rex Buddenberg (Naval Postgraduate School), Sandra Cespedes (Universidad de Chile), Thierry Ernst (YoGoKo), Jerome Haerri (Eurecom), Richard Roy (MIT), and Francois Simon (Pilot).

15. Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of
Internet-Draft          IPWAVE Problem Statement               July 2017

Education (2017R1B1A1B03035885). This work was supported in part by the Global Research Laboratory Program (2013K1A1A2A02078326) through NRF and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning.

16. References

16.1. Normative References


Internet-Draft          IPWAVE Problem Statement               July 2017


16.2. Informative References


Moustafa, H., Bourdon, G., and Y. Gourhant, "Providing Authentication and Access Control in


[CA-Cuise-Control] California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control"


Authors’ Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 440-746
Republic of Korea
Phone: +82 31 299 4957
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Alex Petrescu
CEA, LIST
CEA Saclay
Gif-sur-Yvette, Ile-de-France 91190
France
Phone: +33169089223
EMail: Alexandre.Petrescu@cea.fr

Tae (Tom) Oh
Department of Information Sciences and Technologies
Rochester Institute of Technology
One Lomb Memorial Drive
Rochester, NY 14623-5603
USA
Phone: +1 585 475 7642
EMail: Tom.Oh@rit.edu
IP Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases
draft-ietf-ipwave-vehicular-networking-08

Abstract

This document discusses the problem statement and use cases of IP-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document surveys use cases using V2V, V2I, and V2X networking. Second, it analyzes proposed protocols for IP-based vehicular networking and highlights the limitations and difficulties found on those protocols. Third, it presents a problem exploration for key aspects in IP-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document discusses a problem statement to evaluate the gap between the state-of-the-art techniques and requirements in IP-based vehicular networking.

Status of This Memo

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

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

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

This Internet-Draft will expire on September 25, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Terminology .................................................. 4
3. Use Cases ...................................................... 5
   3.1. V2V ....................................................... 5
   3.2. V2I ....................................................... 7
   3.3. V2X ....................................................... 7
4. Analysis for Existing Protocols ............................... 8
   4.1. Existing Protocols for Vehicular Networking .......... 8
      4.1.1. IP Address Autoconfiguration .................... 8
      4.1.2. Routing Protocol .................................. 9
      4.1.3. Mobility Management .............................. 10
      4.1.4. DNS Naming Service ............................... 11
      4.1.5. Service Discovery .................................. 12
      4.1.6. Security and Privacy ............................. 12
   4.2. General Problems ........................................ 13
      4.2.1. Vehicular Network Architecture .................. 14
      4.2.2. Latency ........................................... 19
      4.2.3. Security ........................................... 20
      4.2.4. Pseudonym Handling .............................. 20
5. Problem Exploration ........................................... 20
   5.1. Neighbor Discovery ...................................... 20
      5.1.1. Link Model ........................................ 21
      5.1.2. MAC Address Pseudonym ........................... 22
      5.1.3. Prefix Dissemination/Exchange ................... 22
      5.1.4. Routing ........................................... 22
   5.2. Mobility Management ................................... 23
   5.3. Security and Privacy ................................... 24
6. Security Considerations ...................................... 24
7. Informative References ....................................... 25

Appendix A. Relevant Topics to IPWAVE Working Group .......... 33
   A.1. Vehicle Identity Management ........................... 33
   A.2. Multihop V2X ........................................... 33
   A.3. Multicast ................................................ 33
   A.4. DNS Naming Services and Service Discovery ............ 34
   A.5. IPv6 over Cellular Networks ............................ 34
      A.5.1. Cellular V2X (C-V2X) Using 4G-LTE ............... 34
1. Introduction

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

For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety services based on the DSRC in terms of standards for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC of the DSRC, while IEEE 1609.2 [WAVE-1609.2] covers security aspects, IEEE 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE 1609.4 [WAVE-1609.4] specifies the multi-channel operation. Note that IEEE 802.11p was a separate standard, but was later enrolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set in 2012 [IEEE-802.11-OCB].

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC3944], MIPv6 [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213][RFC5844]) can be applied (or easily modified) to vehicular networks. In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. Note that a GN protocol is useful to route an event or notification message to vehicles around a geographic position, such as an accident area in a roadway. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].
This document discusses problem statements and use cases related to IP-based vehicular networking for Intelligent Transportation Systems (ITS), which is denoted as IP Wireless Access in Vehicular Environments (IPWAVE). First, it surveys the use cases for using V2V, V2I, and V2X networking in the ITS. Second, for literature review, it analyzes proposed protocols for IP-based vehicular networking and highlights the limitations and difficulties found on those protocols. Third, for problem statement, it presents a problem exploration with key aspects in IPWAVE, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect of the problem statement, it analyzes the gap between the state-of-the-art techniques and the requirements in IP-based vehicular networking. It also discusses potential topics relevant to IPWAVE Working Group (WG), such as Vehicle Identities Management, Multihop V2X Communications, Multicast, DNS Naming Services, Service Discovery, and IPv6 over Cellular Networks. Therefore, with the problem statement, this document will open a door to develop key protocols for IPWAVE that will be essential to IP-based vehicular networks.

2. Terminology

This document uses the following definitions:

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

- **LiDAR**: Acronym for "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.

- **Mobility Anchor (MA)**: A node that maintains IP addresses and mobility information of vehicles in a road network to support their address autoconfiguration and mobility management with a binding table. It has end-to-end connections with RSUs under its control.

- **On-Board Unit (OBU)**: A node that has (e.g., IEEE 802.11-OCB and Cellular V2X (C-V2X) [TS-23.285-3GPP]) for wireless communications with other OBUs and RSUs, and may be connected to in-vehicle devices or networks. An OBU is mounted on a vehicle. It is assumed that a radio navigation receiver (e.g., Global Positioning System (GPS)) is included in a vehicle with an OBU for efficient navigation.

- **OCB**: Acronym for "Outside the Context of a Basic Service Set" [IEEE-802.11-OCB].
Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in car parking area.

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

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

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

V2I2P: Acronym for "Vehicle to Infrastructure to Pedestrian".

V2I2V: Acronym for "Vehicle to Infrastructure to Vehicle".

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

3. Use Cases

This section provides use cases of V2V, V2I, and V2X networking. The use cases of the V2X networking exclude the ones of the V2V and V2I networking, but include Vehicle-to-Pedestrian (V2P) and Vehicle-to-Device (V2D).

3.1. V2V

The use cases of V2V networking discussed in this section include

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

o Cooperative environment sensing.

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

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

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

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

Cooperative-environment-sensing use cases suggest that vehicles can share environmental information from various vehicle-mounted sensors, such as radars, LiDARs and cameras with other vehicles and pedestrians. [Automotive-Sensing] introduces a millimeter-wave vehicular communication for massive automotive sensing. Data generated by those sensors can be substantially large, and these data shall be routed to different destinations. In addition, from the perspective of driverless vehicles, it is expected that driverless vehicles can be mixed with driver-operated vehicles. Through cooperative environment sensing, driver-operated vehicles can use environmental information sensed by driverless vehicles for better interaction with the context.
3.2. V2I

The use cases of V2I networking discussed in this section include:

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

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

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

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

3.3. V2X

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

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I2P networking can reduce the collision of a vehicle and a pedestrian carrying a smartphone equipped with the access technology with an RSU (e.g., WiFi). Vehicles and pedestrians can also communicate with each other via an RSU that delivers scheduling information for wireless communication in order to save the smartphones’ battery through sleeping mode.
For Vehicle-to-Pedestrian (V2P), a vehicle and a pedestrian’s smartphone can directly communicate with each other via V2X without the relaying of an RSU as in a V2V scenario such that the pedestrian’s smartphone is regarded as a vehicle with a wireless media interface to be able to communicate with another vehicle. In Vehicle-to-Device (V2D), a device can be a mobile node such as bicycle and motorcycle, and can communicate directly with a vehicle for collision avoidance.

4. Analysis for Existing Protocols

4.1. Existing Protocols for Vehicular Networking

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

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

4.1.1. IP Address Autoconfiguration

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

A server-based address autoconfiguration such as VAC [Address-Autoconf] takes some delay for a vehicle to join a new cluster (i.e., a connected VANET) and communicate with neighboring vehicles. This delay may prevent vehicles from exchanging safety
messages with each other in a prompt way. It will be good for a vehicle to maintain its IP address even when it joins another cluster. A geographical-position-based address autoconfiguration, such as a prefix allocation per lane [Address-Assigment] and a prefix allocation per geographic region [GeoSAC], causes the frequent change of a vehicle’s IP address and requires the DAD for the uniqueness test of a new IP address. This is significant overhead for high-speed moving vehicles. It will be efficient for a vehicle to be able to use its IP address while moving across the clusters and geographical regions. For the cross-layer identity management with multiple wireless interfaces [Identity-Management], it will be necessary to maintain an upper-layer session (e.g., TCP session) of a vehicle with multiple IP addresses corresponing to the multiple wireless interfaces.

4.1.2. Routing Protocol

For vehicular routing, Abboud et al. proposed a cluster-based routing [Cluster-Based-Routing]. Vehicles construct clusters along with their location and speed information for fast data dissemination among the clusters. They consist of cluster headers, cluster gateways and cluster members for intra-cluster and inter-cluster communications. Tsukada et al. presented a work that aims at combining IPv6 networking and a Car-to-Car Network (called C2CNet) routing protocol proposed by the Car-to-Car Communication Consortium (C2C-CC). Note that C2CNet is the network layer of the C2C-CC communication system and uses a geographic routing protocol for vehicular networks [VANET-Geo-Routing]. Abrougui et al. presented a gateway discovery scheme for vehicles to access the Internet via a gateway, called Location-Aided Gateway Advertisement and Discovery (LAGAD) mechanism [LAGAD]. A vehicle (as a packet source) multihop away from a gateway can discover the gateway and deliver its packets to the gateway through the packet forwarding of intermediate vehicles (as relay vehicles) in a connected VANET. Those intermediate vehicles are located between the packet source vehicle and the gateway.

For data packet routing in vehicular networks, multihop V2V and multihop V2I communications are required. For multihop V2V communications within a connected VANET, a cluster-based routing like [Cluster-Based-Routing] can play a role of efficient data forwarding through a virtual backbone of cluster headers and cluster gateways. For this, an efficient cluster formation is performed through sharing the mobility information (e.g., position, direction, and speed) of vehicles. But the pure VANET-based clustering will cause significant control messages and need some delay for cluster formation, so vehicles can perform clustering through infrastructure nodes (e.g.,
RSUs and base stations) via cellular links, which guarantees always-network-connection.

For multihop V2I communications, a gateway discovery scheme like LAGAD [LAGAD] can be used through a connected VANET having a connection with an Internet gateway. However, this reactive gateway discovery causes much control messages for the discovery and need some delay until a packet source vehicle can transmit its packets toward the gateway. Thus, a proactive gateway discovery is required over a connected VANET where vehicles share routes towards gateways (e.g., distance vector information to gateways) in a proactive manner.

4.1.3. Mobility Management

For mobility management, Chen et al. tackled the issue of network fragmentation in VANET environments [IP-Passing-Protocol] by proposing a protocol that can postpone the time to release IP addresses to the DHCP server and select a faster way to get the vehicle’s new IP address, when the vehicle density is low or the speeds of vehicles are highly variable. Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support the mobility of high-speed mobile vehicles, which is based on both DMM and PMIPv6 [H-DMM]. They also proposed a hybrid centralized-distributed mobility management for network mobility called H-NEMO to support the efficient mobility of mobile nodes and mobile routers between different subnets, which is based on both DMM and PMIPv6 [H-NEMO].

[NEMO-LMS] proposed an architecture to enable IP mobility for moving networks using a network-based mobility scheme based on PMIPv6. Chen et al. proposed a network mobility protocol to reduce handoff delay and maintain Internet connectivity to moving vehicles in a highway [NEMO-VANET]. Lee et al. proposed P-NEMO, which is a PMIPv6-based IP mobility management scheme to maintain the Internet connectivity at the vehicle as a mobile network, and provides a make-before-break mechanism when vehicles switch to a new access network [PMIP-NEMO-Analysis]. Peng et al. proposed a novel mobility management scheme for integration of VANET and fixed IP networks [VNET-MM]. This scheme uses both a road network layout and the wireless coverage of multiple base stations in order to improve the connectivity of vehicles to the Internet and decrease the overhead of mobility management. Nguyen et al. extended their previous works (i.e., H-DMM [H-DMM] and H-NEMO [H-NEMO]) on a vehicular DMM by using a Software-Defined Networking (SDN) architecture, which separates the control plane and the data plane in network functionality [SDN-DMM].
A vehicle can have an internal network for its in-vehicle devices and passengers’ mobile devices. In this case, vehicular networks need to support not only the host mobility for the vehicle, but also the network mobility of such an internet network within the vehicle. The current mobility management schemes, such as [H-DMM] and [H-NEMO], are not enough to support both the host mobility and network mobility in an efficient way. An efficient mobility management scheme can take advantage of a vehicle’s mobility information (e.g., position, direction, and speed) and partial or full trajectory (i.e., a navigation path in a road network) in order to perform operations for mobility management proactively. For this proactive mobility management, an SDN-based mobility management scheme like [SDN-DMM] will be promising because SDN controllers can proactively set up forwarding tables for traffic flows of vehicles with their mobility and trajectory information.

4.1.4. DNS Naming Service

For DNS naming service, Multicast DNS (mDNS) [RFC6762] allows devices in one-hop communication range to resolve each other’s DNS name into the corresponding IP address in multicast. DNS Name Autoconfiguration (DNSNA) [ID-DNSNA] proposes a DNS naming service for Internet-of-Things (IoT) devices in a large-scale network.

A DNS name resolution service needs to support DNS name resolution for in-vehicle devices and passengers’ mobile devices within a vehicle’s internal network, which can be called intra-vehicle DNS name resolution. Also, it needs to support DNS name resolution between devices (e.g., cooperative cruise control device) existing in different vehicles, which can be called inter-vehicle DNS name resolution. In addition, it need to support DNS name resolution in hosts or servers as corresponding nodes in the Internet, which can be called global DNS name resolution.

For the intra-vehicle DNS name resolution and inter-vehicle DNS name resolution, both mDNS [RFC6762] and DNSNA [ID-DNSNA] can be used, but they perform DNS name resolution in a reactive way. That is, when a DNS query is given by a querier, it will be multicasted to devices through mDNS or be unicasted to a dedicated DNS server through DNSNA, respectively.

For the inter-vehicle DNS name resolution in fast-moving vehicles, a proactive DNS resolution can be performed by the help of an RSU that collects the DNS information of vehicles and disseminate it to vehicles under its coverage.

For the global DNS name resolution, a vehicle can use an RSU’s DNS server (or a DNS server close to an RSU in the wired network) to
perform a DNS resolution for the sake of the vehicle’s device during its travel. When the DNS resolution is finished by the RSU’s DNS server, the DNS server can forward the DNS resolution result to the vehicle through the current RSU providing the vehicle with the Internet connectivity.

4.1.5. Service Discovery

To discover instances of a demanded service in vehicular networks, DNS-based Service Discovery (DNS-SD) [RFC6763] with either DNSNA [ID-DNSNA] or mDNS [RFC6762] provides vehicles with service discovery by using standard DNS queries. Vehicular ND [ID-Vehicular-ND] proposes an extension of IPv6 ND for the prefix and service discovery with new ND options.

For vehicular networks, DNSNA can use a dedicated DNS server residing in an RSU or close to an RSU in the wired network [ID-DNSNA]. In this case, in-vehicle devices can register their services (e.g., cooperative cruise control service and navigation service) into the DNS server. When the DNS server can receive a service discovery query from vehicles via an RSU, it can resolve it quickly for them. In DNSNA, these DNS query and response messages are delivered in unicast rather than multicast, so the wireless channel will be utilized efficiently for DNS resolution including service discovery. Thus, DNSNA will provide a more efficient service discovery to vehicles in a high-vehicle-density environment than mDNS [RFC6762] and Vehicular ND [ID-Vehicular-ND]. This is because a DNS query for service discovery is unicasted by DNSNA, but it is multicasted by both mDNS and Vehicular ND.

In a V2V scenario such as the case where a dedicated DNS server in an RSU is not available for the registration and sharing of service information, Vehicular ND can provide vehicles with rapid service discovery by letting vehicles proactively advertise their service information with Neighbor Advertisement (NA) messages. Thus, considering both V2I and V2V scenarios, an efficient service discovery scheme can be designed.

4.1.6. Security and Privacy

For security and privacy, Fernandez et al. proposed a secure vehicular IPv6 communication scheme using Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) for vehicular networks. This scheme provides the secure communication channel between a home agent and a mobile router to support the network mobility of a vehicle’s internal network [Securing-VCOMM]. Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks.
The vehicular networks consist of VANETs as a front end and an access network as a back end via an access point. The security scheme provides vehicles with an efficient AAA service for the network connectivity during their movement in the road network.

Security services in vehicular networks need to support an efficient AAA for the accommodation of only valid vehicles and a secure communication with IKEv2 and IPsec between vehicles or between a vehicle and the corresponding node in the Internet. For the efficiency, these security services need to take advantage of a vehicular network architecture having a TCC and RSUs as well as a vehicle’s mobility and trajectory information.

4.2. General Problems

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

Figure 1 shows an architecture for V2I and V2V networking in a road network. As shown in this figure, RSUs as routers and vehicles with OBU have wireless media interfaces for VANET. Also, it is assumed that such the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking.

Especially, for IPv6 packets transporting over IEEE 802.11-OCB, [IPv6-over-802.11-OCB] specifies several details, such as Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. Especially, an Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC
layer and IPv6 network layer, which is located between IEEE 802.11-OCB’s logical link control layer and IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IP-based vehicular networks.

In Figure 1, three RSUs (RSU1, RSU2, and RSU3) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of RSUs and vehicles in the road network. A Mobility Anchor (MA) is located in the TCC as its key component for the mobility management of vehicles. Two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and one vehicle (Vehicle3) is wirelessly connected to RSU2. The wireless networks of RSU1 and RSU2 belong to a multi-link subnet (denoted as Subnet1) with the same network prefix. Thus, these three vehicles are within the same subnet. On the other hand, another vehicle (Vehicle4) is wirelessly connected to RSU4, belonging to another subnet (denoted as Subnet2). That is, the first three vehicles (i.e., Vehicle1, Vehicle2, and Vehicle3) and the last vehicle (i.e., Vehicle4) are located in the two different subnets.

In wireless subnets in vehicular networks (e.g., Subnet 1 and Subnet 2 in Figure 1), vehicles can construct a connected VANET (as an arbitrary graph topology) and can communicate with each other via V2V communication. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the same subnet along their IPv6 addresses, which are based on the same prefix. On the other hand, Vehicle3 can communicate with Vehicle4 via RSU2 and RSU3 employing V2I (i.e., V2I2V) communication because they are within the two different subnets along with their IPv6 addresses, which are based on the two different prefixes.

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

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

1. An efficient mechanism for the IPv6 address assignment and DAD
2. An on-demand IP mobility management based on PMIPv6 [RFC5213]
3. One-hop and two-hop communication scheme for V2I networking

Note that VIP-WAVE supports at most two-hop V2I communication for simple forwarding operations in VANET. This is because the multi-hop V2I communication with more than two hops requires an additional VANET routing protocol. Such a multi-hop V2I communication will be required for vehicles in a highway with sparsely deployed RSUs in order to provide them with the Internet connectivity via V2I.

Baccelli et al. provided an analysis of the operation of IPv6 as it has been described by the IEEE WAVE standards 1609 [IPv6-WAVE]. This analysis confirms that the use of the standard IPv6 protocol stack in WAVE is not sufficient. It recommends that the IPv6 addressing assignment should follow considerations for ad-hoc link models, defined in [RFC5889] for nodes’ mobility and link variability. However, this ad-hoc link model is not clearly defined to support the efficient V2V and V2I for vehicles with a wireless interface configured with an IPv6 address.

Petrescu et al. proposed the joint IP networking and radio architecture for V2V and V2I communication in [Joint-IP-Networking]. The radio architecture uses Wi-Fi for wireless link rather than IEEE 802.11-OCB. The proposed architecture considers an IP topology in a similar way as a radio link topology, in the sense that an IP subnet would correspond to the range of 1-hop vehicular communication. This architecture defines three types of vehicles: Leaf Vehicle, Range Extending Vehicle, and Internet Vehicle. Leaf Vehicle is like a vehicle with OBU and has one external WiFi interface along with an MR. This MR supports the network mobility of a user’s mobile device and in-vehicle devices in the vehicle’s internal network. Range Extending Vehicles has two external Wi-Fi interfaces to connect two Wi-Fi subnets of cars in a train. Internet Vehicle has one Wi-Fi interface for a car’s subnet and one Wireless Metropolitan Area Network (WMAN) interface for the Internet connectivity. However, this architecture is not suitable for vehicles with a small size and with a wireless interface for V2V and V2I in vehicular links.
4.2.1.1. V2I-based Internetworking

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

As shown in Figure 2, the vehicle’s moving network and the RSU’s fixed network are self-contained networks having multiple subnets and having an edge router for the communication with another vehicle or RSU. Internetworking between two internal networks via V2I communication requires an exchange of network prefix and other parameters through a prefix discovery mechanism, such as ND-based prefix discovery [ID-Vehicular-ND]. For the ND-based prefix discovery, network prefixes and parameters should be registered into a vehicle’s router and an RSU router with an external network interface in advance.

The network parameter discovery collects networking information for an IP communication between a vehicle and an RSU or between two
neighboring vehicles, such as link layer, MAC layer, and IP layer information. The link layer information includes wireless link layer parameters, such as wireless media (e.g., IEEE 802.11-OCB and LTE-V2X) and a transmission power level. The MAC layer information includes the MAC address of an external network interface for the internetworking with another vehicle or RSU. The IP layer information includes the IP address and prefix of an external network interface for the internetworking with another vehicle or RSU.

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle’s moving network and the RSU’s fixed network. DNS services should be supported to enable name resolution for hosts or servers residing either in the vehicle’s moving network or the RSU’s fixed network. It is assumed that the DNS names of in-vehicle devices and their service names are registered into a DNS server in a vehicle or an RSU, as shown in Figure 2. For service discovery, those DNS names and service names can be advertised to neighboring vehicles through either DNS-based service discovery mechanisms [RFC6762][RFC6763][ID-DNSNA] and ND-based service discovery [ID-Vehicular-ND]. For the ND-based service discovery, service names should be registered into a vehicle’s router and an RSU router with an external network interface in advance. For this service discovery, each vehicle and each RSU should have its dedicated DNS server within its internal network, respectively, as shown in Figure 2.

Figure 2 shows internetworking between the vehicle’s moving network and the RSU’s fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Fixed Network1) inside RSU1. RSU1 has the DNS Server (DNS2), one host (Host3), the two routers (Router3 and Router4), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1’s Router1 (called mobile router) and RSU1’s Router3 (called fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for I2V networking.

4.2.1.2. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles via V2V communication.
Figure 3 shows internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (DNS3), the two hosts (Host4 and Host5), and the two routers (Router5 and Router6). Vehicle1’s Router1 (called mobile router) and Vehicle2’s Router5 (called mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking.

4.2.2. Latency

The communication delay (i.e., latency) between two vehicles should be bounded to a certain threshold (e.g., 500 ms) for collision-avoidance message exchange [CASD]. For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. The real implementations for such applications are not
available yet. Thus, the feasibility of IP-based safety applications is not tested yet in the real world.

4.2.3. Security

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

4.2.4. Pseudonym Handling

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

5. Problem Exploration

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

5.1. Neighbor Discovery

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

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval should be adjusted for high-speed vehicles and vehicle density. As vehicles move faster, the NA interval should decrease (e.g., from 1 sec to 0.5 sec) for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase (e.g.,
from 0.5 sec to 1 sec) for the NA messages to reduce collision probability with other NA messages.

5.1.1. Link Model

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

There is a relationship between a link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IP link or extended IP links via ND proxy. Note that a subnet prefix can be used by spanning multiple links into a multi-link subnet with an extended subnet concept [RFC6775]. Also, note that IPv6 Stateless Address Autoconfiguration (SLAAC) can be performed in the multiple links where each of them is not assigned with a unique subnet prefix, that is, all of them are configured with the same subnet prefix [RFC4861][RFC4862].

A vehicular link model needs to consider a multi-hop V2V (or V2I) over a multi-link subnet as shown in Figure 1. In this figure, vehicles in Subnet1 having RSU1 and RSU2 construct a multi-link subnet called Subnet1 with VANETs and RSUs. Vehicle1 and Vehicle3 can communicate with each other via multi-hop V2V or multi-hop V2I2V. When two vehicles (e.g., Vehicle1 and Vehicle3 in Figure 1) are connected in a VANET, they can communicate with each other via VANET rather than RSUs. On the other hand, when two vehicles (e.g., Vehicle1 and Vehicle3) are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V.

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

In the ETSI standards, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities (e.g., MAC address) and the corresponding IPv6 addresses [Identity-Management]. Whenever the network interface identifier changes, the IPv6 address based on the network interface identifier should be updated, and the uniqueness of the address should be performed through the DAD procedure. For vehicular networks with high-mobility, this DAD should be performed efficiently with minimum overhead.

For the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, with a mobility management scheme (e.g., MIPv6 and PMIPv6), the new IP address for the transport-layer session can be notified to an appropriate end point, and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address. This mobility management overhead for pseudonyms should be minimized for efficient operations in vehicular networks having lots of vehicles.

5.1.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes in within the internal networks of two vehicular nodes (e.g., vehicle and RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is required. It is assumed that a vehicular node has an external network interface and its internal network, as shown in Figure 2 and Figure 3. The vehicular ND (VND) [ID-Vehicular-ND] can support the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) of vehicular nodes with a vehicular prefix information option. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without a vehicular ad hoc routing protocol (e.g., AODV [RFC3561] and OLSRv2 [RFC7181]).

5.1.4. Routing

For multihop V2V communications in a multi-link subnet (as a connected VANET), a vehicular ad hoc routing protocol (e.g., AODV and OLSRv2) may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. Instead of the vehicular ad hoc routing protocol, Vehicular ND along with a prefix discovery option can be used to let vehicles exchange their prefixes in a multihop fashion [ID-Vehicular-ND]. With the exchanged prefixes, they can compute their routing table (or IPv6 ND’s neighbor
Also, an efficient, rapid DAD should be supported in a multi-link subnet to prevent or reduce IPv6 address conflicts in such a subnet by using a multi-hop DAD optimization [ID-Vehicular-ND][RFC6775] or an IPv6 geographic-routing-based address autoconfiguration [GeoSAC].

5.2. Mobility Management

The seamless connectivity and timely data exchange between two end points requires an efficient mobility management including location management and handover. Most of vehicles are equipped with a GPS receiver as part of a dedicated navigation system or a corresponding smartphone App. The GPS receiver may not provide vehicles with accurate location information in adverse, local environments such as building area and tunnel. The location precision can be improved by the assistance from the RSUs or a cellular system with a navigation system.

With this GPS navigator, an efficient mobility management is possible by vehicles periodically reporting their current position and trajectory (i.e., navigation path) to RSUs and a Mobility Anchor (MA) in TCC. The RSUs and MA can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the efficient mobility management (e.g., proactive handover). For a better proactive handover, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]), can be used to determine the moment of a handover between RSUs along with mobility information [ID-Vehicular-ND].

With the prediction of the vehicle mobility, MA can support RSUs to perform DAD, data packet routing, horizontal handover (i.e., handover in wireless links using a homogeneous radio technology), and vertical handover (i.e., handover in wireless links using heterogeneous radio technologies) in a proactive manner. Even though a vehicle moves into the wireless link under another RSU belonging to a different subnet, the RSU can proactively perform the DAD for the sake of the vehicle, reducing IPv6 control traffic overhead in the wireless link [ID-Vehicular-ND]. To prevent a hacker from impersonating RSUs as bogus RSUs, RSUs and MA should have secure channels via IPsec.

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

5.3. Security and Privacy

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device’s identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., RSU) connected to an authentication server in TCC. Also, Transport Layer Security (TLS) certificates can be used for secure E2E vehicle communications.

For secure V2I communication, a secure channel between a mobile router in a vehicle and a fixed router in an RSU should be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym should be provided to the vehicle; that is, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicular nodes (e.g., vehicle and RSU) in terms of transport layer for a long-living higher-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IP addresses, because an adversary can see the change of the MAC and IP addresses and track the vehicle with those addresses.

6. Security Considerations

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

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

[Address-Assigment]

[Address-Autoconf]

[Automotive-Sensing]

[Broadcast-Storm]

[CA-Cruise-Control]

[CASD]

[Cluster-Based-Routing]


[Intro-to-Algorithms]

[IP-Passing-Protocol]

[IPv6-over-802.11-OCB]

[IPv6-WAVE]

[ISO-ITS-IPv6]

[Joint-IP-Networking]

[LAGAD]

[Multicast-802]


Internet-Draft          IPWAVE Problem Statement              March 2019


Appendix A. Relevant Topics to IPWAVE Working Group

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

A.1. Vehicle Identity Management

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

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

A.2. Multihop V2X

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

A.3. Multicast

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

In general IEEE 802 wireless media, some performance issues about multicast are found in [Multicast-802]. Since several procedures and functions based on IPv6 use multicast for control-plane messages, such as Neighbor Discovery (ND) and Service Discovery, [Multicast-802] describes that the ND process may fail due to unreliable wireless link, causing failure of the DAD process. Also, the Router Advertisement messages can be lost in multicasting.
A.4. DNS Naming Services and Service Discovery

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

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

A.5. IPv6 over Cellular Networks

Recently, 3GPP has announced a set of new technical specifications, such as Release 14 (3GPP-R14) [TS-23.285-3GPP], which proposes an architecture enhancements for V2X services using the modified sidelink interface that originally is designed for the LTE-Device-to-Device (D2D) communications. 3GPP-R14 specifies that the V2X services only support IPv6 implementation. 3GPP is also investigating and discussing the evolved V2X services in the next generation cellular networks, i.e., 5G new radio (5G-NR), for advanced V2X communications and automated vehicles’ applications.

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

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

The 3GPP technical specification of [TS-23.285-3GPP] states that both IP based and non-IP based V2X messages are supported, and only IPv6 is supported for IP based messages. Moreover, [TS-23.285-3GPP] instructs that a UE autoconfigures a link-local IPv6 address by following SLAAC in [RFC4862], but without sending Neighbor Solicitation and Neighbor Advertisement messages for DAD. This is because a unique prefix is allocated to each node by the 3GPP network, so the IPv6 addresses cannot be duplicate.
A.5.2. Cellular V2X (C-V2X) Using 5G

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

Appendix B. Changes from draft-ietf-ipwave-vehicular-networking-07

The following changes are made from draft-ietf-ipwave-vehicular-networking-07:

- This version is revised based on the comments from Charlie Perkins and Sri Gundavelli.
- In Section 4.1, the existing protocols relevant to IP vehicular networking are summarized and analyzed with pros and cons. This subsection addresses the requirements for IP vehicular networking.
- In Figure 1, a vehicular network architecture is modified to clarify a multi-link subnet consisting of vehicular wireless links, and to provide efficient vehicular communications for V2I & V2V to vehicles whose wireless interface is configured with a global IP address.

Appendix C. Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

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

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

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

The following are co-authors of this document:

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

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

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

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

Jerome Haerri
Communication Systems Department
EURECOM
Sophia-Antipolis
France

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

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

Jeong, Ed.             Expires September 25, 2019              [Page 36]
Abstract

This document discusses the problem statement and use cases of IP-based vehicular networking for Intelligent Transportation Systems (ITS). The main scenarios of vehicular communications are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications. First, this document explains use cases using V2V, V2I, and V2X networking. Next, it makes a problem statement about key aspects in IP-based vehicular networking, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect, this document specifies requirements in IP-based vehicular networking, and suggests the direction of solutions satisfying those requirements.

Status of This Memo

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

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

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

This Internet-Draft will expire on November 25, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1.  Introduction

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

For direct inter-vehicular wireless connectivity, IEEE has amended WiFi standard 802.11 to enable driving safety services based on the DSRC in terms of standards for the Wireless Access in Vehicular Environments (WAVE) system. The Physical Layer (L1) and Data Link Layer (L2) issues are addressed in IEEE 802.11p [IEEE-802.11p] for the PHY and MAC of the DSRC, while IEEE 1609.2 [WAVE-1609.2] covers security aspects, IEEE 1609.3 [WAVE-1609.3] defines related services at network and transport layers, and IEEE 1609.4 [WAVE-1609.4] specifies the multi-channel operation. Note that IEEE 802.11p was a separate standard, but was later enrolled into the base 802.11 standard (IEEE 802.11-2012) as IEEE 802.11 Outside the Context of a Basic Service Set in 2012 [IEEE-802.11-OCB].

Along with these WAVE standards, IPv6 [RFC8200] and Mobile IP protocols (e.g., MIPv4 [RFC3544], MIPv6 [RFC6275], and Proxy MIPv6 (PMIPv6) [RFC5213][RFC5844]) can be applied (or easily modified) to vehicular networks. In Europe, ETSI has standardized a GeoNetworking (GN) protocol [ETSI-GeoNetworking] and a protocol adaptation sub-layer from GeoNetworking to IPv6 [ETSI-GeoNetwork-IP]. Note that a GN protocol is useful to route an event or notification message to vehicles around a geographic position, such as an accident area in a roadway. In addition, ISO has approved a standard specifying the IPv6 network protocols and services to be used for Communications Access for Land Mobiles (CALM) [ISO-ITS-IPv6].

This document explains use cases and a problem statement about IP-based vehicular networking for ITS, which is named IP Wireless Access in Vehicular Environments (IPWAVE). First, it introduces the use cases for using V2V, V2I, and V2X networking in the ITS. Next, it makes a problem statement about key aspects in IPWAVE, such as IPv6 Neighbor Discovery, Mobility Management, and Security & Privacy. For each key aspect of the problem statement, this document specifies requirements in IP-based vehicular networking, and proposes the direction of solutions fulfilling those requirements. Therefore, with the problem statement, this document will open a door to develop key protocols for IPWAVE that will be essential to IP-based vehicular networks in near future.

2. Terminology

This document uses the following definitions:

- **DMM**: Acronym for "Distributed Mobility Management" [RFC7333][RFC7429].
LiDAR: Acronym for "Light Detection and Ranging". It is a scanning device to measure a distance to an object by emitting pulsed laser light and measuring the reflected pulsed light.

Mobility Anchor (MA): A node that maintains IP addresses and mobility information of vehicles in a road network to support their address autoconfiguration and mobility management with a binding table. It has end-to-end connections with RSUs under its control.

On-Board Unit (OBU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and Cellular V2X (C-V2X) [TS-23.285-3GPP]) for wireless communications with other OBUs and RSUs, and may be connected to in-vehicle devices or networks. An OBU is mounted on a vehicle.

OCB: Acronym for "Outside the Context of a Basic Service Set" [IEEE-802.11-OCB].

Road-Side Unit (RSU): A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in car parking area.

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

Vehicle: A node that has an OBU for wireless communication with other vehicles and RSUs. It has a radio navigation receiver of Global Positioning System (GPS) for efficient navigation.

Vehicular Ad Hoc Network (VANET): A network that consists of vehicles interconnected by wireless communication. Since VANET is a connected network component, two vehicles in a VANET can communicate with each other through ad hoc routing via other vehicles as relays even where they are out of one-hop wireless communication range.

Vehicular Cloud: A cloud infrastructure for vehicular networks, having compute nodes, storage nodes, and network nodes.
Vehicle Detection Loop (i.e., Loop Detector): An inductive device used for detecting vehicles passing or arriving at a certain point, for instance, at an intersection with traffic lights or at a ramp toward a highway. The relatively crude nature of the loop’s structure means that only metal masses above a certain size are capable of triggering the detection.

V2I2P: Acronym for "Vehicle to Infrastructure to Pedestrian".

V2I2V: Acronym for "Vehicle to Infrastructure to Vehicle".

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

3. Use Cases

This section explains use cases of V2V, V2I, and V2X networking. The use cases of the V2X networking exclude the ones of the V2V and V2I networking, but include Vehicle-to-Pedestrian (V2P) and Vehicle-to-Device (V2D).

3.1. V2V

The use cases of V2V networking discussed in this section include

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

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

Context-Aware Safety Driving (CASD) navigator [CASD] can help drivers to drive safely by letting the drivers recognize dangerous obstacles and situations. That is, CASD navigator displays obstacles or neighboring vehicles relevant to possible collisions in real-time through V2V networking. CASD provides vehicles with a class-based automatic safety action plan, which considers three situations, such as the Line-of-Sight unsafe, Non-Line-of-Sight unsafe, and safe situations. This action plan can be performed among vehicles through V2V networking.
Cooperative Adaptive Cruise Control (CACC) [CA-Cruise-Control] helps vehicles to adapt their speed autonomously through V2V communication among vehicles according to the mobility of their predecessor and successor vehicles in an urban roadway or a highway. Thus, CACC can help adjacent vehicles to efficiently adjust their speed in an interactive way through V2V networking in order to avoid collision.

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

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

3.2. V2I

The use cases of V2I networking discussed in this section include

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

A navigation service, such as the Self-Adaptive Interactive Navigation Tool (called SAINT) [SAINT], using V2I networking interacts with TCC for the large-scale/long-range road traffic optimization and can guide individual vehicles for appropriate navigation paths in real time. The enhanced version of SAINT [SAINTplus] can give the fast moving paths to emergency vehicles (e.g., ambulance and fire engine) to let them reach an accident spot while providing other vehicles near the accident spot with efficient detour paths.
A TCC can recommend an energy-efficient speed to a vehicle driving in different traffic environments. [Fuel-Efficient] studies fuel-efficient route and speed plans for platooned trucks.

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

3.3. V2X

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

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

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

4. Vehicular Networks

This section describes a vehicular network architecture supporting V2V, V2I, and V2X communications in vehicular networks. Also, it describes an internal network within a vehicle or RSU, and the internetworking between the internal networks via DSRC links.
4.1. Vehicular Network Architecture

Figure 1 shows an architecture for V2I and V2V networking in a road network. As shown in this figure, RSUs as routers and vehicles with OBU have wireless media interfaces for VANET. Also, it is assumed that such the wireless media interfaces are autoconfigured with a global IPv6 prefix (e.g., 2001:DB8:1:1::/64) to support both V2V and V2I networking.

Especially, for IPv6 packets transporting over IEEE 802.11-OCB, [IPv6-over-802.11-OCB] specifies several details, such as Maximum Transmission Unit (MTU), frame format, link-local address, address mapping for unicast and multicast, stateless autoconfiguration, and subnet structure. Especially, an Ethernet Adaptation (EA) layer is in charge of transforming some parameters between IEEE 802.11 MAC
layer and IPv6 network layer, which is located between IEEE 802.11-OCB’s logical link control layer and IPv6 network layer. This IPv6 over 802.11-OCB can be used for both V2V and V2I in IP-based vehicular networks.

In Figure 1, three RSUs (RSU1, RSU2, and RSU3) are deployed in the road network and are connected to a Vehicular Cloud through the Internet. A Traffic Control Center (TCC) is connected to the Vehicular Cloud for the management of RSUs and vehicles in the road network. A Mobility Anchor (MA) is located in the TCC as its key component for the mobility management of vehicles. Two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and one vehicle (Vehicle3) is wirelessly connected to RSU2. The wireless networks of RSU1 and RSU2 belong to two different subnets (denoted as Subnet1 and Subnet2), respectively. Also, another vehicle (Vehicle4) is wireless connected to RSU3, belonging to another subnet (denoted as Subnet3).

In wireless subnets in vehicular networks (e.g., Subnet1 and Subnet2 in Figure 1), vehicles can construct a connected VANET (with an arbitrary graph topology) and can communicate with each other via V2V communication. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication because they are within the wireless communication range for each other. On the other hand, Vehicle3 can communicate with Vehicle4 via the vehicular infrastructure (i.e., RSU2 and RSU3) by employing V2I (i.e., V2I2V) communication because they are not within the wireless communication range for each other.

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

4.2. V2I-based Internetworking

This section discusses the internetworking between a vehicle’s internal network (i.e., moving network) and an RSU’s internal network (i.e., fixed network) via V2I communication.
Nowadays, a vehicle’s internal network tends to be Ethernet to interconnect electronic control units in a vehicle. It can also support WiFi and Bluetooth to accommodate a driver’s and passenger’s mobile devices (e.g., smartphone and tablet). In this trend, it is reasonable to consider a vehicle’s internal network (i.e., moving network) and also the interaction between the internal network and an external network within another vehicle or RSU.

As shown in Figure 2, the vehicle’s moving network and the RSU’s fixed network are self-contained networks having multiple subnets and having an edge router for the communication with another vehicle or RSU. Internetworking between two internal networks via V2I communication requires an exchange of network prefix and other parameters through a prefix discovery mechanism, such as ND-based prefix discovery [ID-Vehicular-ND]. For the ND-based prefix discovery, network prefixes and parameters should be registered into a vehicle’s router and an RSU router with an external network interface in advance.
The network parameter discovery collects networking information for an IP communication between a vehicle and an RSU or between two neighboring vehicles, such as link layer, MAC layer, and IP layer information. The link layer information includes wireless link layer parameters, such as wireless media (e.g., IEEE 802.11-OCB and LTE-V2X) and a transmission power level. The MAC layer information includes the MAC address of an external network interface for the internetworking with another vehicle or RSU. The IP layer information includes the IP address and prefix of an external network interface for the internetworking with another vehicle or RSU.

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle’s moving network and the RSU’s fixed network. DNS services should be supported to enable name resolution for hosts or servers residing either in the vehicle’s moving network or the RSU’s fixed network. It is assumed that the DNS names of in-vehicle devices and their service names are registered into a DNS server in a vehicle or an RSU, as shown in Figure 2.

Figure 2 shows internetworking between the vehicle’s moving network and the RSU’s fixed network. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Fixed Network1) inside RSU1. RSU1 has the DNS Server (DNS2), one host (Host3), the two routers (Router3 and Router4), and the collection of servers (Server1 to ServerN) for various services in the road networks, such as the emergency notification and navigation. Vehicle1’s Router1 (called mobile router) and RSU1’s Router3 (called fixed router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for I2V networking. Thus, one host (Host1) in Vehicle1 can communicate with one server (Server1) in RSU1 for a vehicular service through Vehicle1’s moving network, a wireless link between Vehicle1 and RSU1, and RSU1’s fixed network.

4.3. V2V-based Internetworking

This section discusses the internetworking between the moving networks of two neighboring vehicles via V2V communication.
Figure 3 shows internetworking between the two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (DNS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (DNS3), the two hosts (Host4 and Host5), and the two routers (Router5 and Router6). Vehicle1’s Router1 (called mobile router) and Vehicle2’s Router5 (called mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking. Thus, one host (Host1) in Vehicle1 can communicate with one host (Host4) in Vehicle1 for a vehicular service through Vehicle1’s moving network, a wireless link between Vehicle1 and Vehicle2, and Vehicle2’s moving network.
Figure 4 shows multihop internetworking between the moving networks of two vehicles in the same VANET. For example, Host1 in Vehicle1 can communicate with Host6 in Vehicle3 via Router 5 in Vehicle2 that is an intermediate vehicle being connected to Vehicle1 and Vehicle3 in a linear topology as shown in the figure.

5. Problem Statement

This section makes a problem statement about key topics for IPWAVE WG, such as neighbor discovery, mobility management, and security & privacy.

5.1. Neighbor Discovery

IPv6 Neighbor Discovery (IPv6 ND) [RFC4861][RFC4862] is a core part of the IPv6 protocol suite. IPv6 ND is designed for point-to-point links and transit links (e.g., Ethernet). It assumes an efficient and reliable support of multicast from the link layer for various network operations such as MAC Address Resolution (AR) and Duplicate Address Detection (DAD).

IPv6 ND needs to be extended to vehicular networking (e.g., V2V, V2I, and V2X) in terms of DAD and ND-related parameters (e.g., Router Lifetime). The vehicles are moving fast within the communication coverage of a vehicular node (e.g., vehicle and RSU). Before the vehicles can exchange application messages with each other, they need to be configured with a link-local IPv6 address or a global IPv6 address, and recognize each other in the aspect of IPv6 ND.
The legacy DAD assumes that a node with an IPv6 address can reach any other node with the scope of its address at the time it claims its address, and can hear any future claim for that address by another party within the scope of its address for the duration of the address ownership. However, the partitioning and merging of VANETs makes this assumption frequently invalid in vehicular networks.

The vehicular networks need to support a vehicular-network-wide DAD by defining a scope that is compatible with the legacy DAD, and two vehicles can communicate with each other when there exists a communication path over VANET or a combination of VANETs and RSUs, as shown in Figure 1. By using the vehicular-network-wide DAD, vehicles can assure that their IPv6 addresses are unique in the vehicular network whenever they are connected to the vehicular infrastructure or become disconnected from it in the form of VANET. Even though a unique IPv6 address can be derived from a globally unique MAC address, this derivation yields a privacy issue of a vehicle as an IPv6 node. The vehicular infrastructure having RSUs and an MA can participate in the vehicular-network-wide DAD for the sake of vehicles [RFC6775][RFC8505].

ND time-related parameters such as router lifetime and Neighbor Advertisement (NA) interval should be adjusted for high-speed vehicles and vehicle density. As vehicles move faster, the NA interval should decrease (e.g., from 1 sec to 0.5 sec) for the NA messages to reach the neighboring vehicles promptly. Also, as vehicle density is higher, the NA interval should increase (e.g., from 0.5 sec to 1 sec) for the NA messages to reduce collision probability with other NA messages.

When ND is used in vehicular networks, the communication delay (i.e., latency) between two vehicles should be bounded to a certain threshold (e.g., 500 ms) for collision-avoidance message exchange [CASD]. For IP-based safety applications (e.g., context-aware navigation, adaptive cruise control, and platooning) in vehicular network, this bounded data delivery is critical. The real implementations for such applications are not available yet. Thus, ND needs to appropriately operate to support IP-based safety applications.

5.1.1. Link Model

IPv6 protocols work under certain assumptions for the link model that do not necessarily hold in a vehicular wireless link [VIP-WAVE] [RFC5889]. For instance, some IPv6 protocols assume symmetry in the connectivity among neighboring interfaces. However, interference and different levels of transmission power may cause unidirectional links to appear in vehicular wireless links. As a result, a new vehicular
link model is required for a dynamically changing vehicular wireless link.

There is a relationship between a link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. In an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix and with on-link bit set can communicate with each other on an IP link.

A VANET can have multiple links between pairs of vehicles within wireless communication range, as shown in Figure 4. When two vehicles belong to the same VANET, but they are out of wireless communication range, they cannot communicate directly with each other. Assume that a global-scope IPv6 prefix is assigned to VANETs in vehicular networks. Even though two vehicles in the same VANET configure their IPv6 addresses with the same IPv6 prefix, they may not communicate with each other not in a one hop in the same VANET because of the multihop network connectivity. Thus, in this case, the concept of a on-link IPv6 prefix does not hold because two vehicles with the same on-link IPv6 prefix cannot communicate directly with each other. Also, when two vehicles are located in two different VANETs with the same IPv6 prefix, they cannot communicate with each other. When these two VANETs are converged into one VANET, the two vehicles can communicate with each other in a multihop fashion. Therefore, a vehicular link model should consider the frequent partitioning and merging of VANETs due to vehicle mobility.

An IPv6 prefix can be used in a multi-link subnet as an extended subnet. IPv6 Stateless Address Autoconfiguration (SLAAC) needs to be performed even in the multiple links where all of the links are configured with the same subnet prefix [RFC4861][RFC4862]. Thus, a vehicular link model can consider a multi-hop V2V (or V2I) over a multi-link subnet in a vehicular network having multiple VANETs and RSUs, as shown in Figure 1. For example, in this figure, vehicles (i.e., Vehicle1, Vehicle2, and Vehicle3) in Subnet1 and Subnet2 having RSU1 and RSU2, respectively, construct a multi-link subnet with VANETs and RSUs. Vehicle1 and Vehicle3 can also communicate with each other via either multi-hop V2V or multi-hop V2I2V. When two vehicles (e.g., Vehicle1 and Vehicle3 in Figure 1) are connected in a VANET, it will be more efficient for them to communicate with each other via VANET rather than RSUs. On the other hand, when two vehicles (e.g., Vehicle1 and Vehicle3) are far away from the communication range in separate VANETs and under two different RSUs, they can communicate with each other through the relay of RSUs via V2I2V.

Therefore, IPv6 ND needs to be extended for an efficient Vehicular Neighbor Discovery (VND) to support the concept of an IPv6 link.
corresponding to an IPv6 prefix even in a multi-link subnet consisting of multiple vehicles and RSUs [ID-Vehicular-ND].

5.1.2. MAC Address Pseudonym

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

In the ETSI standards, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities (e.g., MAC address) and the corresponding IPv6 addresses [Identity-Management]. Whenever the network interface identifier changes, the IPv6 address based on the network interface identifier should be updated, and the uniqueness of the address should be performed through the DAD procedure. For vehicular networks with high-mobility, this DAD should be performed efficiently with minimum overhead.

For the continuity of an end-to-end (E2E) transport-layer (e.g., TCP, UDP, and SCTP) session, with a mobility management scheme (e.g., MIPv6 and PMIPv6), the new IP address for the transport-layer session can be notified to an appropriate end point, and the packets of the session should be forwarded to their destinations with the changed network interface identifier and IPv6 address. This mobility management overhead for pseudonyms should be minimized for efficient operations in vehicular networks having lots of vehicles.

5.1.3. Prefix Dissemination/Exchange

A vehicle and an RSU can have their internal network, as shown in Figure 2 and Figure 3. In this case, nodes in within the internal networks of two vehicular nodes (e.g., vehicle and RSU) want to communicate with each other. For this communication on the wireless link, the network prefix dissemination or exchange is required. It is assumed that a vehicular node has an external network interface and its internal network, as shown in Figure 2 and Figure 3. The vehicular ND (VND) [ID-Vehicular-ND] can support the communication between the internal-network nodes (e.g., an in-vehicle device in a vehicle and a server in an RSU) of vehicular nodes with a vehicular prefix information option. Thus, this ND extension for routing functionality can reduce control traffic for routing in vehicular networks without a vehicular ad hoc routing protocol (e.g., AODV [RFC3561] and OLSRv2 [RFC7181]).
5.1.4. Routing

For multihop V2V communications in a VANET (or a multi-link subnet), a vehicular ad hoc routing protocol (e.g., AODV and OLSRv2) may be required to support both unicast and multicast in the links of the subnet with the same IPv6 prefix. However, it will be costly to run both vehicular ND and a vehicular ad hoc routing protocol in terms of control traffic overhead. As a feasible approach, Vehicular ND can be extended to accommodate routing functionality with a prefix discovery option. In this case, there is no need to run a separate vehicular ad hoc routing protocol in VANETs. The ND extension can allow vehicles to exchange their prefixes in a multihop fashion [ID-Vehicular-ND]. With the exchanged prefixes, they can compute their routing table (or IPv6 ND’s neighbor cache) for the multi-link subnet with a distance-vector algorithm [Intro-to-Algorithms].

Also, an efficient, rapid DAD needs to be supported in a vehicular network having multiple VANETs (or a multi-link subnet) to prevent or reduce IPv6 address conflicts in such a subnet. A feasible approach is to use a multi-hop DAD optimization for the efficient vehicular-network-wide DAD [RFC6775][RFC8505].

5.2. Mobility Management

The seamless connectivity and timely data exchange between two end points requires an efficient mobility management including location management and handover. Most of vehicles are equipped with a GPS receiver as part of a dedicated navigation system or a corresponding smartphone App. The GPS receiver may not provide vehicles with accurate location information in adverse, local environments such as building area and tunnel. The location precision can be improved by the assistance from the RSUs or a cellular system with a GPS receiver for location information.

With a GPS navigator, an efficient mobility management will be possible by vehicles periodically reporting their current position and trajectory (i.e., navigation path) to the vehicular infrastructure (having RSUs and an MA in TCC) [ID-Vehicular-MM]. This vehicular infrastructure can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory) for the efficient mobility management (e.g., proactive handover). For a better proactive handover, link-layer parameters, such as the signal strength of a link-layer frame (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]), can be used to determine the moment of a handover between RSUs along with mobility information.
With the prediction of the vehicle mobility, the vehicular infrastructure needs to support RSUs to perform efficient DAD, data packet routing, horizontal handover (i.e., handover in wireless links using a homogeneous radio technology), and vertical handover (i.e., handover in wireless links using heterogeneous radio technologies) in a proactive manner [ID-Vehicular-MM]. For example, when a vehicle is moving into the wireless link under another RSU belonging to a different subnet, the RSU can proactively perform the DAD for the sake of the vehicle, reducing IPv6 control traffic overhead in the wireless link. To prevent a hacker from impersonating RSUs as bogus RSUs, RSUs and MA in the vehicular infrastructure need to have secure channels via IPsec.

Therefore, with a proactive handover and a multihop DAD in vehicular networks, RSUs needs to efficiently forward data packets from the wired network (or the wireless network) to a moving destination vehicle along its trajectory. As a result, a moving vehicle can communicate with its corresponding vehicle in the vehicular network or a host/server in the Internet along its trajectory.

5.3. Security and Privacy

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

Security and privacy are paramount in the V2I, V2V, and V2X networking in vehicular networks. Only authorized vehicles should be allowed to use vehicular networking. Also, in-vehicle devices and mobile devices in a vehicle need to communicate with other in-vehicle devices and mobile devices in another vehicle, and other servers in an RSU in a secure way.

A Vehicle Identification Number (VIN) and a user certificate along with in-vehicle device’s identifier generation can be used to efficiently authenticate a vehicle or a user through a road infrastructure node (e.g., RSU) connected to an authentication server in TCC. Also, Transport Layer Security (TLS) certificates can be used for secure E2E vehicle communications.
For secure V2I communication, a secure channel between a mobile router in a vehicle and a fixed router in an RSU should be established, as shown in Figure 2. Also, for secure V2V communication, a secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

To prevent an adversary from tracking a vehicle with its MAC address or IPv6 address, MAC address pseudonym should be provided to the vehicle; that is, each vehicle should periodically update its MAC address and the corresponding IPv6 address as suggested in [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the E2E communications between two vehicular nodes (e.g., vehicle and RSU) in terms of transport layer for a long-living higher-layer session. However, if this pseudonym is performed without strong E2E confidentiality, there will be no privacy benefit from changing MAC and IP addresses, because an adversary can see the change of the MAC and IP addresses and track the vehicle with those addresses.

6. Security Considerations

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

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

7. Informative References

[Automotive-Sensing]

[CA-Cruise-Control]
Internet-Draft          IPWAVE Problem Statement                May 2019


[VIP-WAVE]

[WAVE-1609.0]

[WAVE-1609.2]

[WAVE-1609.3]

[WAVE-1609.4]
Appendix A. Changes from draft-ietf-ipwave-vehicular-networking-08

The following changes are made from draft-ietf-ipwave-vehicular-networking-08:

- This version is revised based on the comments from Charlie Perkins and Sri Gundavelli.
- This version focuses on the problem statement about IP-based vehicular networking, such as IPv6 neighbor discovery, mobility management, and security & privacy.

Appendix B. Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

This work was supported in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2019-2017-0-01633) supervised by the IITP (Institute for Information & communications Technology Promotion).

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

Appendix C. Contributors

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

The following are co-authors of this document:

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

Phone: +212 6 70 83 22 36
EMail: benamar73@gmail.com
Survey on IP-based Vehicular Networking for Intelligent Transportation Systems
draft-ietf-ipwave-vehicular-networking-survey-00

Abstract

This document surveys the general problem area on IP-based vehicular networks, which are considered a key component of Intelligent Transportation Systems (ITS). The main topics of vehicular networking are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) networking. This document deals with some critical aspects in vehicular networking, such as IP address autoconfiguration, vehicular network architecture, routing, mobility management, and security. This document also surveys standard activities for vehicular networks. In addition, this document surveys the use cases of IP-based vehicular networking for ITS. Finally, this document summarizes and analyzes the previous research activities that use IPv4 or IPv6 for vehicular networking.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 4, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

1. Introduction ............................................... 4
2. Requirements Language ..................................... 4
3. Terminology .................................................. 4
4. IP Address Autoconfiguration ............................... 5
   4.1. Automatic IP Address Configuration in VANETs .......... 5
   4.2. Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network .......... 6
   4.4. Cross-layer Identities Management in ITS Stations ... 7
   4.5. Key Observations ....................................... 8
5. Vehicular Network Architecture ............................. 8
   5.1. VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks ............................... 8
   5.2. IPv6 Operation for WAVE - Wireless Access in Vehicular Environments ........................................... 9
   5.3. A Framework for IP and non-IP Multicast Services for Vehicular Networks ....................................... 10
   5.4. Joint IP Networking and Radio Architecture for Vehicular Networks ............................................. 11
   5.5. Mobile Internet Access in FleetNet ..................... 12
   5.6. A Layered Architecture for Vehicular Delay-Tolerant Networks .................................................. 13
   5.7. Key Observations ....................................... 13
6. Vehicular Network Routing ........................................ 14
   6.1. An IP Passing Protocol for Vehicular Ad Hoc Networks with Network Fragmentation ............... 14
   6.2. Experimental Evaluation for IPv6 over VANET Geographic Routing .................................. 15
   6.3. Key Observations ............................................. 15
7. Mobility Management in Vehicular Networks ......................... 16
   7.1. A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users ........ 16
   7.2. A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility ........ 16
   7.3. NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios ............ 17
   7.4. Network Mobility Protocol for Vehicular Ad Hoc Networks ............................................. 18
   7.5. Performance Analysis of PMIPv6-Based Network MObility for Intelligent Transportation Systems .......... 18
   7.6. A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks and Fixed IP Networks ................. 19
   7.7. SDN-based Distributed Mobility Management for 5G Networks ........................................... 19
   7.8. IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions ........ 21
   7.9. Key Observations ............................................. 22
8. Vehicular Network Security ...................................... 22
   8.1. Securing Vehicular IPv6 Communications .............................................................. 22
   8.2. Providing Authentication and Access Control in Vehicular Network Environment .................... 23
   8.3. Key Observations ............................................. 23
9. Standard Activities for Vehicular Networks ......................... 24
10. The Use Cases of Vehicular Networking ............................ 26
   10.1. The Use Cases of V2I Networking ......................................................... 26
   10.2. The Use Cases of V2V Networking ......................................................... 27
11. Summary and Analysis ............................................. 28
12. Security Considerations .......................................... 29
13. Contributors ...................................................... 29
14. Acknowledgements .................................................. 29
15. References ........................................................ 29
   15.1. Normative References .............................................. 29
   15.2. Informative References .............................................. 30
1. Introduction

Nowadays vehicular networks have been focused on the driving safety, driving efficiency, and entertainment in road networks. For the driving safety, IEEE has standardized Wireless Access in Vehicular Environments (WAVE) standards, such as IEEE 802.11p [IEEE-802.11p], IEEE 1609.2 [WAVE-1609.2], IEEE 1609.3 [WAVE-1609.3], and IEEE 1609.4 [WAVE-1609.4]. Note that IEEE 802.11p has been finalized as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012. Along with these WAVE standards, IPv6 and Mobile IP protocols (e.g., MIPv4 and MIPv6) can be extended to vehicular networks.

This document surveys the general problem area on IP-based vehicular networking for Intelligent Transportation Systems (ITS), such as IP address autoconfiguration, vehicular network architecture, vehicular network routing (for multi-hop V2V, V2I, and I2V), mobility management, and security. Also, this document surveys standard activities for vehicular networks. In addition, this document surveys the use cases of IP-based vehicular networking for ITS. Finally, this document summarizes and analyzes the previous research activities using IPv4 or IPv6 for vehicular networking.

Based on the survey of this document, we can specify the requirements for vehicular networks for the intended purposes, such as the driving safety, driving efficiency, and entertainment. As a consequence, this will make it possible to design the network architecture and protocols for vehicular networking.

2. Requirements Language

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].

3. Terminology

This document defines the following new terms:

- **Road-Side Unit (RSU)**: A node that has Dedicated Short-Range Communications (DSRC) device for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is deployed either at an intersection or in a road segment.

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

- Traffic Control Center (TCC): A node that maintains road infrastructure information (e.g., RSUs, traffic signals, and loop detectors), vehicular traffic statistics (e.g., average vehicle speed and vehicle inter-arrival time per road segment), and vehicle information (e.g., a vehicle’s identifier, position, direction, speed, and trajectory as a navigation path). TCC is included in a vehicular cloud for vehicular networks. Exemplary functions of TCC include the management of evacuation routes, the monitoring of pedestrians and bike traffic, the monitoring of real-time transit operations, and real-time responsive traffic signal systems. Thus, TCC is the nerve center of most freeway management systems such that data is collected, processed, and fused with other operational and control data, and is also synthesized to produce "information" distributed to stakeholders, other agencies, and traveling public. TCC is called Traffic Management Center (TMC) in the US. TCC can communicate with road infrastructure nodes (e.g., RSUs, traffic signals, and loop detectors) to share measurement data and management information by an application-layer protocol.

4. IP Address Autoconfiguration

This section surveys IP address autoconfiguration schemes for vehicular networks.

4.1. Automatic IP Address Configuration in VANETs

Fazio et al. proposed a vehicular address configuration called VAC for automatic IP address configuration in Vehicular Ad Hoc Networks (VANET) [Address-Autoconf]. VAC uses a distributed dynamic host configuration protocol (DHCP). This scheme uses a leader playing a role of a DHCP server within a cluster having connected vehicles within a VANET. In a connected VANET, vehicles are connected with each other with the communication range. In this VANET, VAC dynamically elects a leader-vehicle to quickly provide vehicles with unique IP addresses. The leader-vehicle maintains updated information on configured addresses in its connected VANET. It aims at the reduction of the frequency of IP address reconfiguration due to mobility.

VAC defines the concept of SCOPE as a delimited geographic area where IP addresses are guaranteed to be unique. When it is allocated an IP address from a leader-vehicle with a scope, a vehicle is guaranteed to have a unique IP address while moving within the scope of the leader-vehicle. If it moves out of the scope of the leader vehicle,
it needs to ask for another IP address from another leader-vehicle so that its IP address can be unique within the scope of the new leader-vehicle. This approach may allow for less frequent change of an IP address than the address allocation from a fixed Internet gateway.

Thus, VAC can support a feasible address autoconfiguration for V2V scenarios, but the overhead to guarantee the uniqueness of IP addresses is not ignorable under high-speed mobility.

4.2. Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network

Kato et al. proposed an IPv6 address assignment scheme using lane and position information [Address-Assignment]. In this addressing scheme, each lane of a road segment has a unique IPv6 prefix. When it moves in a lane in a road segment, a vehicle autoconfigures its IPv6 address with its MAC address and the prefix assigned to the lane. A group of vehicles constructs a connected VANET within the same subnet such that their IPv6 addresses have the same prefix. Whenever it moves to another lane, a vehicle updates its IPv6 address with the prefix corresponding to the new lane and also joins the group corresponding to the lane.

However, this address autoconfiguration scheme may have much overhead in the case where vehicles change their lanes frequently in highway.

4.3. GeoSAC: Scalable Address Autoconfiguration for VANET Using Geographic Networking Concepts

Baldessari et al. proposed an IPv6 scalable address autoconfiguration scheme called GeoSAC for vehicular networks [GeoSAC]. GeoSAC uses geographic networking concepts such that it combines the standard IPv6 Neighbor Discovery (ND) and geographic routing functionality. It matches geographically-scoped network partitions to individual IPv6 multicast-capable links. In the standard IPv6, all nodes within the same link must communicate with each other, but due to the characteristics of wireless links, this concept of a link is not clear in vehicular networks. GeoSAC defines a link as a geographic area having a network partition. This geographic area can have a connected VANET. Thus, vehicles within the same VANET in a specific geographic area are regarded as staying in the same link, that is, an IPv6 multicast link.

This paper identifies four key requirements of IPv6 address autoconfiguration for vehicular networks: (i) the configuration of globally valid addresses, (ii) a low complexity for address autoconfiguration, (iii) a minimum signaling overhead of address autoconfiguration, (iv) the support of network mobility through
movement detection, (v) an efficient gateway selection from multiple RSUs, (vi) a fully distributed address autoconfiguration for network security, (vii) the authentication and integrity of signaling messages, and (viii) the privacy protection of vehicles' users.

To support the proposed link concept, GeoSAC performs ad hoc routing for geographic networking in a sub-IP layer called Car-to-Car (C2C) NET. Vehicles within the same link can receive an IPv6 router advertisement (RA) message transmitted by an RSU as a router, so they can autoconfigure their IPv6 address based on the IPv6 prefix contained in the RA and perform Duplicate Address Detection (DAD) to verify the uniqueness of the autoconfigured IP address by the help of the geographic routing within the link.

For location-based applications, to translate between a geographic area and an IPv6 prefix belonging to an RSU, this paper takes advantage of an extended DNS service, using GPS-based addressing and routing along with geographic IPv6 prefix format [GeoSAC].

Thus, GeoSAC can support the IPv6 link concept through geographic routing within a specific geographic area.

4.4. Cross-layer Identities Management in ITS Stations

ITS and vehicular networks are built on the concept of an ITS station (e.g., vehicle and RSU), which is a common reference model inspired from the Open Systems Interconnection (OSI) standard [Identities-Management]. In vehicular networks using multiple access network technologies through a cross-layer architecture, a vehicle with an OBU may have multiple identities corresponding to the access network interfaces. Wetterwald et al. conducted a comprehensive study of the cross-layer identity management in vehicular networks using multiple access network technologies, which constitutes a fundamental element of the ITS architecture [Identities-Management].

Besides considerations related to the case where ETSI GeoNetworking [ETSI-GeoNetworking] is used, this paper analyzes the major requirements and constraints weighing on the identities of ITS stations, e.g., privacy and compatibility with safety applications and communications. The concerns related to security and privacy of the users need to be addressed for vehicular networking, considering all the protocol layers simultaneously. In other words, for security and privacy constraints to be met, the IPv6 address of a vehicle should be derived from a pseudonym-based MAC address and renewed simultaneously with that changing MAC address. This dynamically changing IPv6 address can prevent the ITS station from being tracked by a hacker. However, this address renewal cannot be applied at any time because in some situations, the continuity of the knowledge
about the surrounding vehicles is required.

Also, this paper defines a cross-layer framework that fulfills the requirements on the identities of ITS stations and analyzes systematically, layer by layer, how an ITS station can be identified uniquely and safely, whether it is a moving station (e.g., car and bus using temporary trusted pseudonyms) or a static station (e.g., RSU and central station). This paper has been applied to the specific case of the ETSI GeoNetworking as the network layer, but an identical reasoning should be applied to IPv6 over 802.11 in Outside the Context of a Basic Service Set (OCB) mode now.

4.5. Key Observations

High-speed mobility should be considered for a light-overhead address autoconfiguration. A cluster leader can have an IPv6 prefix [Address-Autoconf]. Each lane in a road segment can have an IPv6 prefix [Address-Assignment]. A geographic region under the communication range of an RSU can have an IPv6 prefix [GeoSAC].

IPv6 ND should be extended to support the concept of a link for an IPv6 prefix in terms of multicast. Ad Hoc routing is required for the multicast in a connected VANET with the same IPv6 prefix [GeoSAC]. A rapid DAD should be supported to prevent or reduce IPv6 address conflicts.

In the ETSI GeoNetworking, for the sake of security and privacy, an ITS station (e.g., vehicle) can use pseudonyms for its network interface identities and the corresponding IPv6 addresses [Identities-Management]. For the continuity of an end-to-end transport session, the cross-layer identity management should be performed carefully.

5. Vehicular Network Architecture

This section surveys vehicular network architectures based on IP along with various radio technologies.

5.1. VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks

Cespedes et al. proposed a vehicular IP in WAVE called VIP-WAVE for I2V and V2I networking [VIP-WAVE]. IEEE 1609.3 specified a WAVE stack of protocols and includes IPv6 as a network layer protocol in data plane [WAVE-1609.3]. The standard WAVE does not support DAD, seamless communications for Internet services, and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU). To overcome these limitations of the standard WAVE for IP-
based networking, VIP-WAVE enhances the standard WAVE by the following three schemes: (i) an efficient mechanism for the IPv6 address assignment and DAD, (ii) on-demand IP mobility based on Proxy Mobile IPv6 (PMIPv6), and (iii) one-hop and two-hop communications for I2V and V2I networking.

In WAVE, IPv6 ND protocol is not recommended due to the overhead of ND against the timely and prompt communications in vehicular networking. By WAVE service advertisement (WAS) management frame, an RSU can provide vehicles with IP configuration information (e.g., IPv6 prefix, prefix length, gateway, router lifetime, and DNS server) without using ND. However, WAVE devices may support readdressing to provide pseudonymity, so a MAC address of a vehicle may be changed or randomly generated. This update of the MAC address may lead to the collision of an IPv6 address based on a MAC address, so VIP-WAVE includes a light-weight, on-demand ND to perform DAD.

For IP-based Internet services, VIP-WAVE adopts PMIPv6 for network-based mobility management in vehicular networks. In VIP-WAVE, RSU plays a role of mobile anchor gateway (MAG) of PMIPv6, which performs the detection of a vehicle as a mobile node in a PMIPv6 domain and registers it into the PMIPv6 domain. For PMIPv6 operations, VIP-WAVE requires a central node called local mobility anchor (LMA), which assigns IPv6 prefixes to vehicles as mobile nodes and forwards data packets to the vehicles moving in the coverage of RSUs under its control through tunnels between MAGs and itself.

For two-hop communications between a vehicle and an RSU, VIP-WAVE allows an intermediate vehicle between the vehicle and the RSU to play a role of a packet relay for the vehicle. When it becomes out of the communication range of an RSU, a vehicle searches for another vehicle as a packet relay by sending a relay service announcement. When it receives this relay service announcement and is within the communication range of an RSU, another vehicle registers itself into the RSU as a relay and notifies the relay-requester vehicle of a relay maintenance announcement.

Thus, VIP-WAVE is a good candidate for I2V and V2I networking, supporting an enhanced ND, handover, and two-hop communications through a relay.

5.2. IPv6 Operation for WAVE - Wireless Access in Vehicular Environments

Baccelli et al. provided an analysis of the operation of IPv6 as it has been described by the IEEE WAVE standards 1609 [IPv6-WAVE]. Although the main focus of WAVE has been the timely delivery of safety related information, the deployment of IP-based entertainment
applications is also considered. Thus, in order to support entertainment traffic, WAVE supports IPv6 and transport protocols such as TCP and UDP.

In the analysis provided in [IPv6-WAVE], it is identified that the IEEE 1609.3 standard’s recommendations for IPv6 operation over WAVE are rather minimal. Protocols on which the operation of IPv6 relies for IP address configuration and IP-to-link-layer address translation (e.g., IPv6 NP protocol) are not recommended in the standard. Additionally, IPv6 works under certain assumptions for the link model that do not necessarily hold in WAVE. For instance, IPv6 assumes symmetry in the connectivity among neighboring interfaces. However, interference and different levels of transmission power may cause unidirectional links to appear in a WAVE link model. Also, in an IPv6 link, it is assumed that all interfaces which are configured with the same subnet prefix are on the same IP link. Hence, there is a relationship between link and prefix, besides the different scopes that are expected from the link-local and global types of IPv6 addresses. Such a relationship does not hold in a WAVE link model due to node mobility and highly dynamic topology.

Baccellii et al. concluded that the use of the standard IPv6 protocol stack, as the IEEE 1609 family of specifications stipulate, is not sufficient. Instead, the addressing assignment should follow considerations for ad-hoc link models, defined in [RFC5889], which are similar to the characteristics of the WAVE link model. In terms of the supporting protocols for IPv6, such as ND, DHCP, or stateless auto-configuration, which rely largely on multicast, do not operate as expected in the case where the WAVE link model does not have the same behavior expected for multicast IPv6 traffic due to nodes’ mobility and link variability. Additional challenges such as the support of pseudonymity through MAC address change along with the suitability of traditional TCP applications are discussed by the authors since they require the design of appropriate solutions.

5.3. A Framework for IP and non-IP Multicast Services for Vehicular Networks

Jemaa et al. presented a framework that enables deploying multicast services for vehicular networks in Infrastructure-based scenarios [Vehicular-Network-Framework]. This framework deals with two phases: (i) Initialization or bootstrapping phase that includes a geographic multicast auto-configuration process and a group membership building method and (ii) Multicast traffic dissemination phase that includes a network selecting mechanism on the transmission side and a receiver-based multicast delivery in the reception side. To this end, authors define a distributed mechanism that allows the vehicles to configure a common multicast address: Geographic Multicast Address Auto-
configuration (GMAA), which allows a vehicle to configure its own address without signaling. A vehicle may also be able to change the multicast address to which it is subscribed when it changes its location.

This framework suggests a network selecting approach that allows IP and non-IP multicast data delivery in the sender side. Then, to meet the challenges of multicast address auto-configuration, the authors propose a distributed geographic multicast auto-addressing mechanism for multicast groups of vehicles, and a simple multicast data delivery scheme in hybrid networks from a server to the group of moving vehicles. However, this study lacks simulations related to performance assessment.

5.4. Joint IP Networking and Radio Architecture for Vehicular Networks

Petrescu et al. defined the joined IP networking and radio architecture for V2V and V2I communication in [Joint-IP-Networking]. The paper proposes to consider an IP topology in a similar way as a radio link topology, in the sense that an IP subnet would correspond to the range of 1-hop vehicular communication. The paper defines three types of vehicles: Leaf Vehicle (LV), Range Extending Vehicle (REV), and Internet Vehicle (IV). The first class corresponds to the largest set of communicating vehicles (or network nodes within a vehicle), while the role of the second class is to build an IP relay between two IP-subnet and two sub-IP networks. Finally, the last class corresponds to vehicles being connected to Internet. Based on these three classes, the paper defines six types of IP topologies corresponding to V2V communication between two LVs in direct range, or two LVs over a range extending vehicle, or V2I communication again either directly via an IV, via another vehicles being IV, or via an REV connecting to an IV.

Considering a toy example of a vehicular train, where LV would be in-wagon communicating nodes, REV would be inter-wagon relays, and IV would be one node (e.g., train head) connected to Internet. Petrescu et al. defined the required mechanisms to build subnetworks, and evaluated the protocol time that is required to build such networks. Although no simulation-based evaluation is conducted, the initial analysis shows a long initial connection overhead, which should be alleviated once the multi-wagon remains stable. However, this approach does not describe what would happen in the case of a dynamic multi-hop vehicular network, where such overhead would end up being too high for V2V/V2I IP-based vehicular applications.

One other aspect described in this paper is to join the IP-layer relaying with radio-link channels. This paper suggests to separate different subnetworks in different WiFi/ITS-G5 channels, which could
be advertised by the REV. Accordingly, the overall interference could be controlled within each subnetwork. This statement is similar to multi-channel topology management proposals in multi-hop sensor networks, yet adapted to an IP topology.

In conclusion, this paper proposes to classify an IP multi-hop vehicular network in three classes of vehicles: Leaf Vehicle (LV), Range Extending Vehicle (REV), and Internet Vehicle (IV). It suggests that the generally complex multi-hop IP vehicular topology could be represented by only six different topologies, which could be further analyzed and optimized. A prefix dissemination protocol is proposed for one of the topologies.

5.5. Mobile Internet Access in FleetNet

Bechler et al. described the FleetNet project approach to integrate Internet Access in future vehicular networks [FleetNet]. The paper is most probably one of the first paper to address this aspect, and in many ways, introduces concepts that will be later used in MIPv6 or other subsequent IP mobility management schemes. The paper describes a V2I architecture consisting of Vehicles, Internet Gateways (IGW), Proxy, and Corresponding Nodes (CN). Considering that vehicular networks are required to use IPv6 addresses and also the new wireless access technology ITS-G5 (new at that time), one of the challenges is to bridge the two different networks (i.e., VANET and IP4/IPv6 Internet). Accordingly, the paper introduces a Fleetnet Gateway (FGW), which allows vehicles in IPv6 to access the IPv4 Internet and to bridge two types of networks and radio access technologies. Another challenge is to keep the active addressing and flows while vehicles move between FGWs. Accordingly, the paper introduces a proxy node, a cranked-up MIP Home Agent, which can re-route flows to the new FGW as well as acting as a local IPv4-IPv6 NAT.

The authors from the paper mostly observed two issues that VANET brings into the traditional IP mobility. First, VANET vehicles must mostly be addressed from the Internet directly, and do not specifically have a Home Network. Accordingly, VANET vehicles require a globally (predefined) unique IPv6 address, while an IPv6 co-located care-of address (CCoA) is a newly allocated IPv6 address every time a vehicle would enter a new IGW radio range. Second, VANET links are known to be unreliable and short, and the extensive use of IP tunneling on-the-air was judged not efficient. Accordingly, the first major architecture innovation proposed in this paper is to re-introduce a foreign agent (FA) in MIP located at the IGW, so that the IP-tunneling would be kept in the back-end (between a Proxy and an IGW) and not on the air. Second, the proxy has been extended to build an IP tunnel and be connected to the right FA/IWG for an IP flow using a global IPv6 address.
This is a pioneer paper, which contributed to changing MIP and led to the new IPv6 architecture currently known as Proxy-MIP and the subsequent DMM-PMIP. Three key messages can be yet kept in mind. First, unlike the Internet, vehicles can be more prominently directly addressed than the Internet traffic, and do not have a Home Network in the traditional MIP sense. Second, IP tunneling should be avoided as much as possible over the air. Third, the protocol-based mobility (induced by the physical mobility) must be kept hidden to both the vehicle and the correspondent node (CN).

5.6. A Layered Architecture for Vehicular Delay-Tolerant Networks

Soares et al. addressed the case of delay tolerant vehicular network [Vehicular-DTN]. For delay tolerant or disruption tolerant networks, rather than building a complex VANET-IP multi-hop route, vehicles may also be used to carry packets closer to the destination or directly to the destination. The authors built the well-accepted DTN Bundle architecture and protocol to propose a VANET extension. They introduced three types of VANET nodes: (i) terminal nodes (requiring data), (ii) mobile nodes (carrying data along their routes), and (iii) relay nodes (storing data at cross-roads of mobile nodes as data hotspot).

The major innovation in this paper is to propose a DTN VANET architecture separating a Control plane and a Data plane. The authors claimed it to be designed to allow full freedom to select the most appropriate technology, as well as allow to use out-of-band communication for small Control plane packets and use DTN in-band for the Data plane. The paper then further describes the different layers from the Control and the Data planes. One interesting aspect is the positioning of the Bundle layer between L2 and L3, rather than above TCP/IP as for the DTN Bundle architecture. The authors claimed this to be required first to keep bundle aggregation/disaggregation transparent to IP, as well as to allow bundle transmission over multiple access technologies (described as MAC/PHY layers in the paper).

Although the DTN architectures evolved since the paper has been written, this paper addresses IP mobility management from a different approach. An important aspect is to separate the Control plane from the Data plane to allow a large flexibility in a Control plane to coordinate a heterogeneous radio access technology (RAT) Data plane.

5.7. Key Observations

Unidirectional links exist and must be considered. Control Plane must be separated from Data Plane. ID/Pseudonym change requires a lightweight DAD. IP tunneling should be avoided. Vehicles do not...
have a Home Network. Protocol-based mobility must be kept hidden to both the vehicle and the correspondent node (CN). An ITS architecture may be composed of three types of vehicles: Leaf Vehicle, Range Extending Vehicle, and Internet Vehicle.

6. Vehicular Network Routing

This section surveys routing in vehicular networks.

6.1. An IP Passing Protocol for Vehicular Ad Hoc Networks with Network Fragmentation

Chen et al. tackled the issue of network fragmentation in VANET environments [IP-Passing-Protocol]. The paper proposes a protocol that can postpone the time to release IP addresses to the DHCP server and select a faster way to get the vehicle’s new IP address, when the vehicle density is low or the speeds of vehicles are varied. In such circumstances, the vehicle may not be able to communicate with the intended vehicle either directly or through multi-hop relays as a consequence of network fragmentation.

The paper claims that although the existing IP passing and mobility solutions may reduce handoff delay, but they cannot work properly on VANET especially with network fragmentation. This is due to the fact that messages cannot be transmitted to the intended vehicles. When network fragmentation occurs, it may incur longer handoff latency and higher packet loss rate. The main goal of this study is to improve existing works by proposing an IP passing protocol for VANET with network fragmentation.

The paper makes the assumption that on the highway, when a vehicle moves to a new subnet, the vehicle will receive broadcast packet from the target Base Station (BS), and then perform the handoff procedure. The handoff procedure includes two parts, such as the layer-2 handoff (new frequency channel) and the layer-3 handover (a new IP address). The handoff procedure contains movement detection, DAD procedure, and registration. In the case of IPv6, the DAD procedure is time consuming and may cause the link to be disconnected.

This paper proposes another handoff mechanism. The handoff procedure contains the following phases. The first is the information collecting phase, where each mobile node (vehicle) will broadcast its own and its neighboring vehicles’ locations, moving speeds, and directions periodically. The remaining phases are, the fast IP acquiring phase, the cooperation of vehicle phase, the make before break phase, and the route redirection phase.

Simulations results show that for the proposed protocol, network
fragmentation ratio incurs less impact. Vehicle speed and density has great impact on the performance of the IP passing protocol because vehicle speed and vehicle density will affect network fragmentation ratio. A longer IP lifetime can provide a vehicle with more chances to acquire its IP address through IP passing. Simulation results show that the proposed scheme can reduce IP acquisition time and packet loss rate, so extend IP lifetime with extra message overhead.

6.2. Experimental Evaluation for IPv6 over VANET Geographic Routing

Tsukada et al. presented a work that aims at combining IPv6 networking and a Car-to-Car Network routing protocol (called C2CNet) proposed by the Car2Car Communication Consortium (C2C-CC), which is an architecture using a geographic routing protocol [VANET-Geo-Routing]. In C2C-CC architecture, C2CNet layer is located between IPv6 and link layers. Thus, an IPv6 packet is delivered with outer C2CNet header, which introduces the challenge of how to support the communication types defined in C2CNet in IPv6 layer.

The main goal of GeoNet is to enhance these specifications and create a prototype software implementation interfacing with IPv6. C2CNet is specified in C2C-CC as a geographic routing protocol.

In order to assess the performance of this protocol, the authors measured the network performance with UDP and ICMPv6 traffic using iperf and ping6. The test results show that IPv6 over C2CNet does not have too much delay (less than 4ms with a single hop) and is feasible for vehicle communication. In the outdoor testbed, they developed AnaVANET to enable hop-by-hop performance measurement and position trace of the vehicles.

The combination of IPv6 multicast and GeoBroadcast was implemented, however, the authors did not evaluate the performance with such a scenario. One of the reasons is that a sufficiently high number of receivers are necessary to properly evaluate multicast but experimental evaluation is limited in the number of vehicles (4 in this study).

6.3. Key Observations

IP address autoconfiguration should be manipulated to support the efficient networking. Due to network fragmentation, vehicles cannot communicate with each other temporarily. IPv6 ND should consider the temporary network fragmentation. IPv6 link concept can be supported by Geographic routing to connect vehicles with the same IPv6 prefix.
7. Mobility Management in Vehicular Networks

This section surveys mobility management schemes in vehicular networks to support handover.

7.1. A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users

Nguyen et al. proposed a hybrid centralized-distributed mobility management called H-DMM to support highly mobile vehicles [H-DMM]. The legacy DMM is not suitable for high-speed scenarios because it requires additional registration delay proportional to the distance between a vehicle and its anchor network. H-DMM is designed to satisfy a set of requirements, such as service disruption time, end-to-end delay, packet delivery cost, and tunneling cost.

H-DMM adopts a central node called central mobility anchor (CMA), which plays the role of a local mobility anchor (LMA) in PMIPv6. When it enters a mobile access router (MAR) as an access router, a vehicle obtains a prefix from the MAR (called MAR-prefix) according to the legacy DMM protocol. In addition, it obtains another prefix from the CMA (called LMA-prefix) for a PMIPv6 domain. Whenever it performs a handover between the subnets for two adjacent MARs, a vehicle keeps the LMA-prefix while obtaining a new prefix from the new MAR. For a new data exchange with a new CN, the vehicle can select the MAR-prefix or the LMA-prefix for its own source IPv6 address. If the number of active prefixes is greater than a threshold, the vehicle uses the LMA-prefix-based IPv6 address as its source address. In addition, it can continue receiving data packets with the destination IPv6 addresses based on the previous prefixes through the legacy DMM protocol.

Thus, H-DMM can support an efficient tunneling for a high-speed vehicle that moves fast across the subnets of two adjacent MARs. However, when H-DMM asks a vehicle to perform DAD for the uniqueness test of its configured IPv6 address in the subnet of the next MAR, the activation of the configured IPv6 address for networking will take a delay. This indicates that a proactive DAD by a network component (i.e., MAR and LMA) can shorten the address configuration delay of the current DAD triggered by a vehicle.

7.2. A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility

Nguyen et al. proposed H-NEMO, a hybrid centralized-distributed mobility management scheme to handle IP mobility of moving vehicles [H-NEMO]. The standard Network Mobility (NEMO) basic support, which is a centralized scheme for network mobility, provides IP mobility...
for a group of users in a moving vehicle, but also inherits the drawbacks from Mobile IPv6, such as suboptimal routing and signaling overhead in nested scenarios as well as reliability and scalability issues. On the contrary, distributed schemes such as the recently proposed Distributed Mobility Management (DMM) locates the mobility anchor at the network edge and enables mobility support only to traffic flows that require such support. However, in high speed moving vehicles, DMM may suffer from high signaling cost and high handover latency.

The proposed H-NEMO architecture is not designed for a specific wireless technology. Instead, it defines a general architecture and signaling protocol so that a mobile node can obtain mobility from fixed locations or mobile platforms, and also allows the use of DMM or Proxy Mobile IPv6 (PMIPv6), depending on flow characteristics and mobility patterns of the node. For IP addressing allocation, a mobile router (MR) or the mobile node (MN) connected to an MR in a NEMO obtain two sets of prefixes: one from the central mobility anchor and one from the mobile access router (MAR). In this way, the MR/MN may choose a more stable prefix for long-lived flows to be routed via the central mobility anchor and the MAR-prefix for short-lived flows to be routed following the DMM concept. The multi-hop scenario is considered under the concept of a nested-NEMO.

Nguyen et al. did not provide simulation-based evaluations, but they provided an analytical evaluation that considered signaling and packet delivery costs, and showed that H-NEMO outperforms the previous proposals, which are either centralized or distributed ones with NEMO support. In particular cases, such as the signaling cost, H-NEMO is more costly than centralized schemes when the velocity of the node is increasing, but behaves better in terms of packet delivery cost and handover delay.

7.3. NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios

In [NEMO-LMS], authors proposed an architecture to enable IP mobility for moving networks in a network-based mobility scheme based on PMIPv6. In PMIPv6, only mobile terminals are provided with IP mobility. Different from host-based mobility, PMIPv6 shifts the signaling to the network side, so that the mobile access gateway (MAG) is in charge of detecting connection/disconnection of the mobile node, upon which the signaling to the Local Mobility Anchor (LMA) is triggered to guarantee a stable IP addressing assignment when the mobile node performs handover to a new MAG.

Soto et al. proposed NEMO support in PMIPv6 (N-PMIP). In this scheme, the functionality of the MAG is extended to the mobile router.
(MR), also called a mobile MAG (mMAG). The functionality of the mobile terminal remains unchanged, but it can receive an IPv6 prefix belonging to the PMIPv6 domain through the new functionality of the mMAG. Therefore, in N-PMIP, the mobile terminal connects to the MR as if it is connecting to a fixed MAG, and the MR connects to the fixed MAG with the standardized signaling of PMIPv6. When the mobile terminal roams to a new MAG or a new MR, the network forwards the packets through the LMA. Hence, N-PMIP defines an extended functionality in the LMA that enables a recursive lookup. First, it locates the binding entry corresponding to the mMAGr. Next, it locates the entry corresponding to the fixed MAG, after which the LMA can encapsulate packets to the mMAG to which the mobile terminal is currently connected.

The performance of N-PMIP was evaluated through simulations and compared to a NEMO+MIPv6+PMIPv6 scheme, with better results obtained in N-PMIP. The work did not consider the case of multi-hop connectivity in the vehicular scenario. In addition, since the MR should be a trusted entity in the PMIP domain, it requires specific security associations that were not addressed in [NEMO-LMS].

7.4. Network Mobility Protocol for Vehicular Ad Hoc Networks

Chen et al. proposed a network mobility protocol to reduce handoff delay and maintain Internet connectivity to moving vehicles in a highway [NEMO-VANET]. In this work, vehicles can acquire IP addresses from other vehicles through V2V communications. At the time the vehicle goes out of the coverage of the base station, another vehicle may assist the roaming car to acquire a new IP address. Also, cars on the same or opposite lane are entitled to assist the vehicle to perform a pre-handoff.

Authors assumed that the wireless connectivity is provided by WiFi and WiMAX access networks. Also, they considered scenarios in which a single vehicle, i.e., a bus, may need two mobile routers in order to have an effective pre-handoff procedure. Evaluations are performed through simulations and the comparison schemes are the standard NEMO Basic Support protocol and the fast NEMO Basic Support protocol. Authors did not mention applicability of the scheme in other scenarios such as in urban transport schemes.

7.5. Performance Analysis of PMIPv6-Based Network MOBility for Intelligent Transportation Systems

Lee et al. proposed P-NEMO, which is an IP mobility management scheme to maintain the Internet connectivity at the vehicle as a mobile network, and provides a make-before-break mechanism when vehicles switch to a new access network [PMIPv6-NEMO-Analysis]. Since the
standard PMIPv6 only supports mobility for a single node, the solution in [PMIPv6-NEMO-Analysis] adapts the protocol to reduce the signaling when a local network is to be served by the in-vehicle mobile router. To achieve this, P-NEMO extends the binding update lists at both MAG and LMA, so that the mobile router (MR) can receive a home network prefix (HNP) and a mobile network prefix (MNP). The latter prefix enables mobility for the moving network, instead of a single node as in the standard PMIPv6.

An additional feature is proposed by Lee et al. named fast P-NEMO (FP-NEMO). It adopts the fast handover approach standardized for PMIPv6 in [RFC5949] with both predictive and reactive modes. The difference of the proposed feature with the standard version is that by using the extensions provided by P-NEMO, the predictive transferring of the context from the old MAG to the new MAG also includes information for the moving network, i.e., the MNP, so that mobility support can be achieved not only for the mobile router, but also for mobile nodes traveling with the vehicle.

The performance of P-NEMO and F-NEMO is only evaluated through an analytical model that is compared to the standard NEMO-BS. No comparison was provided to other schemes that enable network mobility in PMIPv6 domains, such as the one presented in [NEMO-LMS].

7.6. A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks and Fixed IP Networks

Peng et al. proposed a novel mobility management scheme for integration of VANET and fixed IP networks [Vehicular-Network-MM]. The proposed scheme deals with mobility of vehicles based on a street layout instead of a general two dimensional ad hoc network. This scheme makes use of the information provided by vehicular networks to reduce mobility management overhead. It allows multiple base stations that are close to a destination vehicle to discover the connection to the vehicle simultaneously, which leads to an improvement of the connectivity and data delivery ratio without redundant messages. The performance was assessed by using a road traffic simulator called SUMO (Simulation of Urban Mobility).

7.7. SDN-based Distributed Mobility Management for 5G Networks

Nguyen et al. extended their previous works on a vehicular adapted DMM considering a Software-Defined Networking (SDN) architecture [SDN-DMM]. On one hand, in their previous work, Nguyen et al. proposed DMM-PMIP and DMM-MIP architectures for VANET. The major innovation behind DMM is to distribute the Mobility Functions (MF) through the network instead of concentrating them in one bottleneck MF, or in a hierarchically organized backbone of MF. Highly mobile
vehicular networks impose frequent IP route optimizations that lead to suboptimal routes (detours) between CN and vehicles. The suboptimality critically increases by nested or hierarchical MF nodes. Therefore, flattening the IP mobility architecture significantly reduces detours, as it is the role of the last MF to get the closest next MF (in most cases nearby). Yet, with an MF being distributed throughout the network, a Control plane becomes necessary in order to provide a solution for CN to address vehicles. The various solutions developed by Nguyen at al. not only showed the large benefit of a DMM approach for IPv6 mobility management, but also emphasized the critical role of an efficient Control plane.

One the other hand, SDN recently appeared and gained a big attention from the Internet Networking community due to its capacity to provide a significantly higher scalability of highly dynamic flows, which is required by future 5G dynamic networks. In particular, SDN also suggests a strict separation between a Control plane (SDN-Controller) and a Data plane (OpenFlow Switches) based on the OpenFlow standard. Such an architecture has two advantages that are critical for IP mobility management in VANET. First, unlike traditional routing mechanisms, OpenFlow focuses on flows rather than optimized routes. Accordingly, they can optimize routing based on flows (grouping multiple flows in one route, or allowing one flow to have different routes), and can detect broken flows much earlier than the traditional networking solutions. Second, SDN controllers may dynamically reprogram (reconfigure) OpenFlow Switches (OFS) to always keep an optimal route between CN and a vehicular node.

Nguyen et. al observed the mutual benefits IPv6 DMM could obtain from an SDN architecture, and then proposed an SDN-based DMM for VANET. In their proposed architecture, a PMIP-DMM is used, where MF is OFS for the Data plane, and one or more SDN controllers handle the Control plane. The evaluation and prototype in the paper prove that the proposed architecture can provide a higher scalability than the standard DMM.

This paper makes several observations leading to a strong suggestions that IP mobility management should be based on an SDN architecture. First, SDN will be integrated into future Internet and 5G in a near future. Second, after separating the Identity and Routing addressing, IP mobility management further requires to separate the Control from the Data plane if it needs to remain scalable for VANET. Finally, Flow-based routing (in particular OpenFlow standard) will be required in future heterogeneous vehicular networks (e.g., multi-RAT and multi-protocol) and the SDN coupled with DMM provides a double benefit of dynamic flow detection/reconfiguration and short(-er) route optimizations.
7.8. IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions

Cespedes et al. provided a survey of the challenges for NEMO Basic Support for VANET [Vehicular-IP-MM]. NEMO allows the management of a group of nodes (a mobile network) rather than a single node. However, although a vehicle and even a platoon of vehicles could be seen as a group of nodes, NEMO has not been designed considering the particularities of VANET. For example, NEMO builds a tunnel between an MR (on board of a vehicle) and its HA, which in a VANET context is suboptimal, for instance due to over-the-air tunneling cost, the detour taken to pass by the MR’s HA even if the CN is nearby, or the route optimization when the MR moves to a new AR.

Cespedes et al. first summarize the requirements of IP mobility management, such as reduced power at end-device, reduced handover event, reduced complexity, or reduced bandwidth consumption. VANET adds the following requirements, such as minimum signaling for route optimization (RO), per-flow separability, security and binding privacy protection, multi-homing, and switching HA. As observed, these provide several challenges to IP mobility and NEMO BS for VANET.

Cespedes et al. then describe various optimization schemes available for NEMO BS. Considering a single hop connection to CN, one major optimization direction is to avoid the HA detour and reach the CN directly. In that direction, a few optimizations are proposed, such as creating an IP tunnel between the MR and the CR directly, creating an IP tunnel between the MR and a CR (rather than the HA), a delegation mechanism allowing Visiting Nodes to use MIPv6 directly rather than NEMO or finally intra-NEMO optimization for a direct path within NEMO bypassing HAs.

Specific to VANET, multi-hop connection is possible to the fixed network. In that case, NEMO BS must be enhanced to avoid that the path to immediate neighbors must pass by the respective HAs instead of directly. More specifically, two approaches are proposed to rely on VANET sub-IP multi-hop routing to hide a NEMO complex topology (e.g., Nested NEMO) and provide a direct route between two VANET nodes. Generally, one major challenge is security and privacy when opening a multi-hop route between a VANET and a CN. Heterogeneous multi-hop in a VANET (e.g., relying on various access technologies) corresponds to another challenge for NEMO BS as well.

Cespedes et al. conclude their paper with an overview of critical research challenges, such as Anchor Point location, the optimized usage of geographic information at the subIP as well as at the IP level to improve NEMO BS, security and privacy, and the addressing
allocation schema for NEMO.

In summary, this paper illustrates that NEMO BS for VANET should avoid the HA detour as well as opening IP tunnels over the air. Also, NEMO BS could use geographic information for subIP routing when a direct link between vehicles is required to reach an AR, but also anticipate handovers and optimize ROs. From an addressing perspective, dynamic MNP assignments should be preferred, but should be secured in particular during binding update (BU).

7.9. Key Observations

Mobility Management (MM) solution design varies, depending on scenarios: highway vs. urban roadway. Hybrid schemes (NEMO + PMIP, PMIP + DMM, etc.) usually show better performance than pure schemes. Most schemes assume that IP address configuration is already set up. Most schemes have been tested only at either simulation or analytical level. SDN can be considered as a player in the MM solution.

8. Vehicular Network Security

This section surveys security in vehicular networks.

8.1. Securing Vehicular IPv6 Communications

Fernandez et al. proposed a secure vehicular IPv6 communication scheme using Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [Securing-VCOMM]. This scheme aims at the security support for IPv6 Network Mobility (NEMO) for in-vehicle devices inside a vehicle via a Mobile Router (MR). An MR has multiple wireless interfaces, such as 3G, IEEE 802.11p, WiFi, and WiMAX. The proposed architecture consists of Vehicle ITS Station (Vehicle ITS-S), Roadside ITS Station (Roadside ITS-S), and Central ITS Station (Central ITS-S). Vehicle ITS-S is a vehicle having a mobile Network along with an MR. Roadside ITS-S is an RSU as a gateway to connect vehicular networks to the Internet. Central ITS-S is a TCC as a Home Agent (HA) for the location management of vehicles having their MR.

The proposed secure vehicular IPv6 communication scheme sets up IPsec secure sessions for control and data traffic between the MR in a Vehicle ITS-S and the HA in a Central ITS-S. Roadside ITS-S plays a role of an Access Router (AR) for Vehicle ITS-S’s MR to provide the Internet connectivity for Vehicle ITS-S via wireless interfaces, such as IEEE 802.11p, WiFi, and WiMAX. In the case where Roadside ITS-S is not available to Vehicle ITS-S, Vehicle ITS-S communicates with Central ITS-S via cellular networks (e.g., 3G). The secure communication scheme enhances the NEMO protocol that interworks with
IKEv2 and IPsec in network mobility in vehicular networks.

The authors implemented their scheme and evaluated its performance in a real testbed. This testbed supports two wireless networks, such as IEEE 802.11p and 3G. The in-vehicle devices (or hosts) in Vehicle ITS-S are connected to an MR of Vehicle ITS-S via IEEE 802.11g. The test results show that their scheme supports promising secure IPv6 communications with a low impact on communication performance.

8.2. Providing Authentication and Access Control in Vehicular Network Environment

Moustafa et al. proposed a security scheme providing authentication, authorization, and accounting (AAA) services in vehicular networks [VNET-AAA]. This security scheme aims at the support of safe and reliable data services in vehicular networks. It authenticates vehicles as mobile clients to use the network access and various services that are provided by service providers. Also, it ensures a confidential data transfer between communicating parties (e.g., vehicle and infrastructure node) by using IEEE 802.11i (i.e., WPA2) for secure layer-2 links.

The authors proposed a vehicular network architecture consisting of three entities, such as Access network, Wireless mobile ad hoc networks (MANETs), and Access Points (APs). Access network is the fixed network infrastructure forming the back-end of the architecture. Wireless MANETs are constructed by moving vehicles forming the front-end of the architecture. APs is the IEEE 802.11 WLAN infrastructure forming the interface between the front-end and back-end of the architecture.

For AAA services, the proposed architecture uses a Kerberos authentication model that authenticates vehicles at the entry point with the AP and also authorizes them to the access of various services. Since vehicles are authenticated by a Kerberos Authentication Server (AS) only once, the proposed security scheme can minimize the load on the AS and reduce the delay imposed by layer 2 using IEEE 802.11i.

8.3. Key Observations

The security for vehicular networks should provide vehicles with AAA services in an efficient way. It should consider not only horizontal handover, but also vertical handover since vehicles have multiple wireless interfaces.
9. Standard Activities for Vehicular Networks

This section surveys standard activities for vehicular networks in standards developing organizations.


IEEE 1609 is a suite of standards for Wireless Access in Vehicular Environments (WAVE) developed in the IEEE Vehicular Technology Society (VTS). They define an architecture and a complementary standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications.

IEEE 1609.0 provides a description of the WAVE system architecture and operations (called WAVE reference model) [WAVE-1609.0]. The reference model of a typical WAVE device includes two data plane protocol stacks (sharing a common lower stack at the data link and physical layers): (i) the standard Internet Protocol Version 6 (IPv6) and (ii) the WAVE Short Message Protocol (WSMP) designed for optimized operation in a wireless vehicular environment. WAVE Short Messages (WSM) may be sent on any channel. IP traffic is only allowed on service channels (SCHs), so as to offload high-volume IP traffic from the control channel (CCH).

The Layer 2 protocol stack distinguishes between the two upper stacks by the Ethertype field. Ethertype is a 2-octet field in the Logical Link Control (LLC) header, used to identify the networking protocol to be employed above the LLC protocol. In particular, it specifies the use of two Ethertype values (i.e., two networking protocols), such as IPv6 and WSMP.

Regarding the upper layers, while WAVE communications use standard port numbers for IPv6-based protocols (e.g., TCP, UDP), they use a Provider Service Identifier (PSID) as an identifier in the context of WSMP.


IEEE 1609.3 defines services operating at the network and transport layers, in support of wireless connectivity among vehicle-based devices, and between fixed roadside devices and vehicle-based devices using the 5.9 GHz Dedicated Short-Range Communications/Wireless Access in Vehicular Environments (DSRC/WAVE) mode [WAVE-1609.3].

WAVE Networking Services represent layer 3 (networking) and layer 4.
Internet-Draft    IP-based Vehicular Networking Survey         July 2017

(transport) of the OSI communications stack. The purpose is then to provide addressing and routing services within a WAVE system, enabling multiple stacks of upper layers above WAVE Networking Services and multiple lower layers beneath WAVE Networking Services. Upper layer support includes in-vehicle applications offering safety and convenience to users.

The WAVE standards support IPv6. IPv6 was selected over IPv4 because IPv6 is expected to be a viable protocol into the foreseeable future. Although not described in the WAVE standards, IPv4 has been tunnelled over IPv6 in some WAVE trials.

The document provides requirements for IPv6 configuration, in particular for the address setting. It specifies the details of the different service primitives, among which is the WAVE Routing Advertisement (WRA), part of the WAVE Service Advertisement (WSA). When present, the WRA provides information about infrastructure internetwork connectivity, allowing receiving devices to be configured to participate in the advertised IPv6 network. For example, an RSU can broadcast in the WRA portion of its WSA all the information necessary for an OBU to access an application-service available over IPv6 through the RSU as a router. This feature removes the need for an IPv6 Router Advertisement message, which are based on ICMPv6.


ETSI published a standard specifying the transmission of IPv6 packets over the ETSI GeoNetworking (GN) protocol [ETSI-GeoNetworking] [ETSI-GeoNetwork-IPv6]. IPv6 packet transmission over GN is defined in ETSI EN 302 636-6-1 [ETSI-GeoNetwork-IPv6] using a protocol adaptation sub-layer called "GeoNetworking to IPv6 Adaptation Sub-Layer (GN6ASL)". It enables an ITS station (ITS-S) running the GN protocol and an IPv6-compliant protocol layer to: (i) exchange IPv6 packets with other ITS-S; (ii) acquire globally routable IPv6 unicast addresses and communicate with any IPv6 host located in the Internet by having the direct connectivity to the Internet or via other relay ITS stations; (iii) perform operations as a Mobile Router for network mobility [RFC3963].

The document introduces three types of virtual link, the first one providing symmetric reachability by means of stable geographically scoped boundaries and two others that can be used when the dynamic definition of the broadcast domain is required. The combination of these three types of virtual link in the same station allows running the IPv6 ND protocol including Stateless Address Autoconfiguration (SLAAC) [RFC4862] as well as distributing other IPv6 link-local
multicast traffic and, at the same time, reaching nodes that are outside specific geographic boundaries. The IPv6 virtual link types are provided by the GN6ASL to IPv6 in the form of virtual network interfaces.

The document also describes how to support bridging on top of the GN6ASL, how IPv6 packets are encapsulated in GN packets and delivered, as well as the support of IPv6 multicast and anycast traffic, and neighbor discovery. For latency reasons, the standard strongly recommends to use SLAAC for the address configuration.

Finally, the document includes the required operations to support the change of pseudonym, e.g., changing IPv6 addresses when the GN address is changed, in order to prevent attackers from tracking the ITS-S.


ISO published a standard specifying the IPv6 network protocols and services [ISO-ITS-IPv6]. These services are necessary to support the global reachability of ITS-S, the continuous Internet connectivity for ITS-S, and the handover functionality required to maintain such connectivity. This functionality also allows legacy devices to effectively use an ITS-S as an access router to connect to the Internet. Essentially, this specification describes how IPv6 is configured to support ITS-S and provides the associated management functionality.

The requirements apply to all types of nodes implementing IPv6: personal, vehicle, roadside, or central node. The standard defines IPv6 functional modules that are necessary in an IPv6 ITS-S, covering IPv6 forwarding, interface between IPv6 and lower layers (e.g., LAN interface), mobility management, and IPv6 security. It defines the mechanisms to be used to configure the IPv6 address for static nodes as well as for mobile nodes, while maintaining the addressing reachability from the Internet.

10. The Use Cases of Vehicular Networking

This section surveys the use cases of IP-based vehicular networking for ITS.

10.1. The Use Cases of V2I Networking

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

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

A pedestrian protection service, such as Safety-Aware Navigation Application (called SANA) [SANA], using V2I networking can reduce the collision of a pedestrian and a vehicle, which have a smartphone, in a road network. Vehicles and pedestrians can communicate with each other via an RSU that delivers scheduling information for wireless communication to save the smartphones’ battery.

10.2. The Use Cases of V2V Networking

The use cases of V2V networking include context-aware navigator for driving safety, cooperative adaptive cruise control in an urban roadway, and platooning in a highway. These are three techniques that will be important elements for self-driving.

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

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

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

11. Summary and Analysis

This document surveyed state-of-the-arts technologies for IP-based vehicular networks, such as IP address autoconfiguration, vehicular network architecture, vehicular network routing, and mobility management.

Through this survey, it is learned that IPv6-based vehicular networking can be well-aligned with IEEE WAVE standards for various vehicular network applications, such as driving safety, efficient driving, and entertainment. However, since the IEEE WAVE standards do not recommend to use the IPv6 ND protocol for the communication efficiency under high-speed mobility, it is necessary to adapt the ND for vehicular networks with such high-speed mobility.

The concept of a link in IPv6 does not match that of a link in VANET because of the physical separation of communication ranges of vehicles in a connected VANET. That is, in a linear topology of three vehicles (Vehicle-1, Vehicle-2, and Vehicle-3), Vehicle-1 and Vehicle-2 can communicate directly with each other. Vehicle-2 and Vehicle-3 can communicate directly with each other. However, Vehicle-1 and Vehicle-3 cannot communicate directly with each other due to the out-of-communication range. For the link in IPv6, all of three vehicles are on a link, so they can communicate directly with each other. On the other hand, in VANET, this on-link communication concept is not valid in VANET. Thus, the IPv6 ND should be extended to support this multi-link subnet of a connected VANET through either ND proxy or VANET routing.

For IP-based networking, IP address autoconfiguration is a prerequisite function. Since vehicles can communicate intermittently with TCC via RSUs through V2I communications, TCC can play a role of a DHCP server to allocate unique IPv6 addresses to the vehicles. This centralized address allocation can remove the delay of the DAD procedure for testing the uniqueness of IPv6 addresses.
For routing and mobility management, most of vehicles are equipped with a GPS navigator as a dedicated navigation system or a smartphone App. With this GPS navigator, vehicles can share their current position and trajectory (i.e., navigation path) with TCC. TCC can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory). With the prediction of the vehicle mobility, TCC supports RSUs to perform data packet routing and handover proactively.

12. Security Considerations

Security and privacy are important aspects in vehicular networks. Only valid vehicles should be allowed to participate in vehicular networking. Vehicle Identification Number (VIN) and user certificate can be used to authenticate a vehicle and user through road infrastructure, such as Road-Side Unit (RSU) connected to an authentication server in Traffic Control Center (TCC).

13. Contributors

IPWAVE is a group effort. The following people actively contributed to the survey text: Rex Buddenberg (Naval Postgraduate School), Thierry Ernst (YoGoKo), Bokor Laszlo (Budapest University of Technology and Economics), Jose Santa Lozanoi (Universidad of Murcia), and Richard Roy (MIT).

14. Acknowledgements

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1B1A1B03035885). This work was supported in part by the Global Research Laboratory Program (2013K1A1A2A02078326) through NRF and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning. This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

15. References

15.1. Normative References

 Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

 Baccelli, E. and M. Townsley, "IP
15.2. Informative References


[SDN-DMM] Nguyen, T., Bonnet, C., and J. Harri, "SDN-based Distributed Mobility Management for 5G Networks",


[WAVE-1609.3] IEEE 1609 Working Group, "IEEE
Internet-Draft    IP-based Vehicular Networking Survey         July 2017


Intelligent Transportation Systems, June 2017.


Authors’ Addresses

Jaehoon Paul Jeong  
Department of Software  
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon, Gyeonggi-Do  440-746  
Republic of Korea

Phone: +82 31 299 4957  
Fax: +82 31 290 7996  
EMail: pauljeong@skku.edu  
URI:  http://iotlab.skku.edu/people-jaehoon-jeong.php

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

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

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

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

Jerome Haerri  
Communication Systems Department  
EURECOM  
Sophia-Antipolis  
France

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

This document specifies a vehicular mobility management scheme for IP-based vehicular networks. The vehicular mobility management scheme takes advantage of a vehicular link model based on a multi-link subnet. With a vehicle’s mobility information (e.g., position, speed, and direction) and navigation path (i.e., trajectory), it can provide a moving vehicle with proactive and seamless handoff along with its trajectory.

Status of This Memo

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

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

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

This Internet-Draft will expire on September 29, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must
1. Introduction

This document proposes a mobility management scheme for IP-based vehicular networks, which is called vehicular mobility management (VMM). This vehicular mobility management is tailored for a vehicular network architecture and a vehicular link model described in IPWAVE problem statement document [I-D.IPWAVE-PS].

To support the interaction between vehicles or between vehicles and Road-Side Units (RSUs), Vehicular Neighbor Discovery (VND) is proposed as an enhanced IPv6 Neighbor Discovery (ND) for IP-based vehicular networks [I-D.IPWAVE-VND]. For an efficient IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862], VND adopts an optimized Address Registration using a multihop Duplicate Address Detection (DAD). This multihop DAD enables a vehicle to have a unique IP address in a multi-link subnet that consists of multiple wireless subnets with the same IP prefix, which corresponds to wireless coverage of multiple Road-Side Units (RSUs). Also, VND supports IP packet routing via a connected Vehicular Ad Hoc Network (VANET) by letting vehicles exchange the prefixes of their internal networks through their external wireless interface.

The mobility management in this multi-link subnet needs a new approach from the legacy mobility management schemes. This document aims at an efficient mobility management scheme called vehicular mobility management called VMM to support efficient V2V, V2I, and V2X...
communications in a road network. The VMM takes advantage of the mobility information (e.g., a vehicle’s speed, direction, and position) and trajectory (i.e., navigation path) of each vehicle registered into a Traffic Control Center (TCC) in the vehicular cloud.

2. Requirements Language

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].

3. Terminology

This document uses the terminology described in [RFC4861] and [RFC4862]. In addition, the following new terms are defined as below:

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

- **Mobility Anchor (MA)**: A node that maintains IP addresses and mobility information of vehicles in a road network to support their address autoconfiguration and mobility management with a binding table. It has end-to-end connections with RSUs under its control.

- **On-Board Unit (OBU)**: A node that has a network interface (e.g., IEEE 802.11-OCB and Cellular V2X (C-V2X) [TS-23.285-3GPP]) for wireless communications with other OBUs and RSUs, and may be connected to in-vehicle devices or networks. An OBU is mounted on a vehicle. It is assumed that a radio navigation receiver (e.g., Global Positioning System (GPS)) is included in a vehicle with an OBU for efficient navigation.

- **OCB**: Acronym for "Outside the Context of a Basic Service Set" [IEEE-802.11-OCB].

- **Road-Side Unit (RSU)**: A node that has physical communication devices (e.g., IEEE 802.11-OCB and C-V2X) for wireless communications with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is typically deployed on the road infrastructure, either at an intersection or in a road segment, but may also be located in car parking areas.

- **Traffic Control Center (TCC)**: A node that maintains road infrastructure information (e.g., RSUs, traffic signals, and loop detectors), vehicular traffic statistics (e.g., average vehicle
speed and vehicle inter-arrival time per road segment), and
time). TCC is

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

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

4. Vehicular Network Architecture

This section describes a vehicular network architecture for V2V and
V2I communication. A vehicle and an RSU have their internal networks
including in-vehicle devices or servers, respectively.

4.1. Vehicular Network

A vehicular network architecture for V2I and V2V is illustrated in
Figure 1. In this figure, there is a vehicular cloud having a
Traffic Control Center (TCC). The TCC has Mobility Anchors (MAs) for
the mobility management of vehicles under its control. Each MA is in
charge of the mobility management of vehicles under its prefix
domain, which is a multi-link subnet of RSUs sharing the same prefix
[I-D.IPWAVE-PS]. A vehicular network is a wireless network
consisting of RSUs and vehicles. RSUs are interconnected with each
other through a wired network, and vehicles can construct Vehicular
Ad Hoc Networks (VANET).
In Figure 1, three RSUs are deployed either at intersections or along roadways. They are connected to an MA through wired networks. In the vehicular network, there are two subnets such as Subnet1 and Subnet2. Subnet1 is a multi-link subnet consisting of multiple wireless coverage areas of multiple RSUs, and those areas share the same IPv6 prefix to construct a single logical subnet [I-D.IPWAVE-PS]. That is, the wireless links of RSU1 and RSU2 belong to Subnet1. Thus, since Vehicle2 and Vehicle2 use the same prefix for Subnet1 and they are within the wireless communication range, they can communicate directly with each other. Note that in a multi-link subnet, a vehicle (e.g., Vehicle1 and Vehicle2 in Figure 1) can configure its global IPv6 address through an address registration procedure including a multihop Duplicate Address Detection (DAD),
which is specified in Vehicular Neighbor Discovery (VND) [I-D.IPWAVE-VND].

On the other hand, Subnet2 uses a prefix different from Subnet1’s. Vehicle4 residing in Subnet2 cannot talk to Vehicle3 directly because they belong to different subnets. Vehicles can construct a connected VANET, so they can communicate with each other without the relaying of an RSU, but the forwarding over the VANET. In the case where two vehicles belong to the same multi-link subnet, but they are not connected in the same VANET, they can use RSUs. In Figure 1, even though Vehicle2 are disconnected from Vehicle3, they can communicate indirectly with each other through RSUs such as RSU1 and RSU2.

In Figure 1, it is assumed that Vehicle2 communicates with the corresponding node denoted as CN1 where Vehicle2 is moving in the wireless coverage of RSU1. When Vehicle2 moves out of the coverage of RSU1 and moves into the coverage of RSU2 where RSU1 and RSU2 shares the same prefix, the packets sent by CN1 should be routed toward Vehicle2. Also, when Vehicle2 moves out of the coverage of RSU2 and moves into the coverage of RSU3 where RSU2 and RSU3 use two different prefixes, the packets of CN1 should be delivered to Vehicle2. With a handoff procedure, a sender’s packets can be delivered to a destination vehicle which the destination vehicle is moving in the wireless coverage areas. Thus, this document specifies a mobility management scheme in the vehicular network architecture, as shown in Figure 1.

5. Mobility Management

This section explains the detailed procedure of mobility management of a vehicle in a vehicular network as shown in Figure 1.

5.1. Network Attachment of a Vehicle

A mobility management is required for the seamless communication of vehicles moving between the RSUs. When a vehicle moves into the coverage of another RSU, a different IP address is assigned to the vehicle, resulting in the reconfiguration of transport-layer session information (i.e., an end-point’s IP address) to avoid service disruption. Considering this issue, this document proposes a handoff mechanism for seamless communication.

In [VIP-WAVE], the authors constructed a network-based mobility management scheme using Proxy Mobile IPv6 (PMIPv6) [RFC5213], which is highly suitable to vehicular networks. This document uses a mobility management procedure similar to PMIPv6 along with prefix discovery.
Figure 2 shows the binding update flow when a vehicle entered the subnet of an RSU. RSUs act as Mobility Anchor Gateway (MAG) defined in [VIP-WAVE]. When it receives an RS message from a vehicle containing its mobility information (e.g., position, speed, and direction), an RSU sends its MA a Proxy Binding Update (PBU) message [RFC5213][RFC3775], which contains a Mobility Option for the vehicle’s mobility information. The MA receives the PBU and sets up a Binding Cache Entry (BCE) as well as a bi-directional tunnel (denoted as Bi-Dir Tunnel in Figure 2) between the serving RSU and itself. Through this tunnel, all traffic packets to the vehicle are encapsulated toward the RSU. Simultaneously, the MA sends back a Proxy Binding Acknowledgment (PBA) message to the serving RSU. This serving RSU receives the PBA and sets up a bi-directional tunnel with the MA. After this binding update, the RSU sends back an RA message to the vehicle, which includes the RSU’s prefix for the address autoconfiguration of the vehicle.

When the vehicle receives the RA message, it performs the address registration procedure including a multihop DAD for its global IP address based on the prefix announced by the RA message according to the VND [I-D.IPWAVE-VND].

In PMIPv6, a unique prefix is allocated to each vehicle by an MA (i.e., LMA), but in this document, a unique IP address is allocated to each vehicle by an MA through the multihop-DAD-based address registration. This unique IP address allocation can reduce the waste of IP prefixes by the legacy PMIPv6 because vehicles in a multi-link is allocated with a unique IP address based on the same prefix.
### 5.2. Handoff within One Prefix Domain

When the vehicle changes its location and its current RSU (denoted as c-RSU) detects that the vehicle moves out of its coverage, c-RSU needs to report the movement of the vehicle into the coverage of another RSU to the MA.

<table>
<thead>
<tr>
<th>Vehicle</th>
<th>c-RSU</th>
<th>Mobility Anchor</th>
<th>n-RSU</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>===Bi-Dir Tunnel==</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>----DeReg PBU----&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;-------PBA-------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(------------------RS with Mobility Info-------------------)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>[VMI]</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;-------PBU-------</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-------PBA------&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>===Bi-Dir Tunnel==</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;-------------------RA with prefix----------------------</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3: Handoff of a Vehicle within One Prefix Domain with PMIPv6**

With this report, the MA can change the end-point of the tunnel for the vehicle into the new RSU’s IP address.

Figure 3 shows the handoff of a vehicle within one prefix domain (i.e., a multi-link subnet) with PMIPv6. As shown in the figure, when the MA receives a new PBU from the new RSU, it changes the tunnel’s end-point from the current RSU (c-RSU) to the new RSU (n-RSU). If there is ongoing IP packets toward the vehicle, the MA encapsulates the packets and then forwards them towards n-RSU. Through this network-based mobility management, the vehicle is not
aware of any changes at its network layer and can maintain its transport-layer sessions without any disruption.

```
<table>
<thead>
<tr>
<th>Vehicle</th>
<th>c-RSU</th>
<th>n-RSU</th>
</tr>
</thead>
<tbody>
<tr>
<td>---------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>c-RSU detects leaving</td>
<td>------PBU------&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>===Bi-Dir Tunnel==</td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;-------PBA------</td>
<td></td>
</tr>
<tr>
<td>(--------RS with Mobility Info---------)</td>
<td>[VMI]</td>
<td></td>
</tr>
<tr>
<td>&lt;------------RA with prefix-------------</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Figure 4: Handoff of a Vehicle within One Prefix Domain with DMM**

If c-RSU and n-RSU are adjacent, that is, vehicles are moving in specified routes with fixed RSU allocation, the procedure can be simplified by constructing bidirectional tunnel directly between them (cancel the intervention of MA) to alleviate the traffic flow in MA as well as reduce handoff delay.

Figure 4 shows the handoff of a vehicle within one prefix domain (as a multi-link subnet) with DMM [I-D.DMM-PMIPv6]. RSUs are in charge of detecting when a node joins or moves through its domain. If c-RSU detects that the vehicle is going to leave its coverage and to enter the area of an adjacent RSU, it sends a PBU message to inform n-RSU of the handoff of vehicle. If n-RSU receives the PBU message, it constructs a bidirectional tunnel between c-RSU and itself, and then sends back a PBA message as an acknowledgment to c-RSU. If there are ongoing IP packets toward the vehicle, c-RSU encapsulates the packets and then forwards them to n-RSU. When n-RSU detects the entrance of the vehicle, it directly sends an RA message to the vehicle so that the vehicle can assure that it is still connected to a router for its current prefix. If the vehicle sends an RS message to n-RSU, n-RSU responds to the RA message by sending an RA to the vehicle.
5.3. Handoff between Multiple Prefix Domains

When the vehicle moves from a prefix domain to another prefix domain, a handoff between multiple prefix domains is required. As shown in Figure 1, when Vehicle3 moves from the subnet of RSU2 (i.e., Subnet1) to the subnet of RSU3 (i.e., Subnet2), a multiple domain handoff is performed through the cooperation of RSU2, RSU3, MA1 and MA2.

```
Vehicle          c-RSU               MA1              MA2             n-RSU

==Bi-Dir Tunnel==

---DeReg PBU----> -------PBU------>

<-------PBA-------       -------PBA------>

==Bi-Dir Tunnel==

(----------------------RS with Mobility Info---------------------)

| [VMI] |

<---------------RA with prefix1 (c-RSU)--------------------

<---------------RA with prefix2 (n-RSU)----------------------
```

Figure 5: Handoff of a Vehicle between Multiple Prefix Domains with PMIPv6

Figure 5 shows the handoff of a vehicle between two prefix domains (i.e., two multi-link subnets) with PMIPv6. When the vehicle moves out of its current RSU (denoted as c-RSU) belonging to Subnet1, and moves into the next RSU (n-RSU) belonging to Subnet2, c-RSU detects that the vehicles moves out of its coverage. c-RSU reports the movement of the vehicle into the coverage of another RSU (n-RSU) to MA1. MA1 sends MA2 a PBU message to inform MA2 that the vehicle will enter the coverage of n-RSU belonging to MA2. MA2 send n-RSU a PBA message to inform n-RSU that the vehicle will enter the coverage of n-RSU along with handoff context such as c-RSU’s context information (e.g., c-RSU’s link-local address and prefix called prefix1), and the vehicle’s context information (e.g., the vehicle’s global IP address and MAC address). After n-RSU receives the PBA message including the handoff context from MA2, it sets up a bi-directional tunnel with MA2, and generates RA messages with c-RSU’s context information.
That is, n-RSU pretends to be a router belonging to Subnet1. When the vehicle receives the RA from n-RSU, it can maintain its connection with its corresponding node (i.e., CN1). Note that n-RSU also sends RA messages with its domain prefix called prefix2. The vehicle configures another global IP address with prefix2, and can use it for the communication with neighboring vehicles under the coverage of n-RSU.

If c-RSU and n-RSU are adjacent, that is, vehicles are moving in specified routes with fixed RSU allocation, the procedure can be simplified by constructing bidirectional tunnel directly between them (cancel the intervention of MA) to alleviate the traffic flow in MA as well as reduce handoff delay.

Figure 6: Handoff of a Vehicle within Multiple Prefix Domains with DMM

Figure 6 shows the handoff of a vehicle within two prefix domains (as two multi-link subnets) with DMM [I-D.DMM-PMIPv6]. If c-RSU detects that the vehicle is going to leave its coverage and to enter the area of an adjacent RSU (n-RSU) belonging to a different prefix domain, it sends a PBU message to inform n-RSU that the vehicle will enter the coverage of n-RSU along with handoff context such as c-RSU’s context information (e.g., c-RSU’s link-local address and prefix called prefix1), and the vehicle’s context information (e.g., the vehicle’s global IP address and MAC address). After n-RSU receives the PBA message including the handoff context from c-RSU, it sets up a bi-directional tunnel with c-RSU, and generates RA messages with c-RSU’s...
context information. That is, n-RSU pretends to be a router belonging to Subnet1. When the vehicle receives the RA from n-RSU, it can maintain its connection with its corresponding node (i.e., CN1). Note that n-RSU also sends RA messages with its domain prefix called prefix2. The vehicle configures another global IP address with prefix2, and can use it for the communication with neighboring vehicles under the coverage of n-RSU.

6. Security Considerations

This document shares all the security issues of Vehicular ND [I-D.IPWAVE-VND], Proxy MIPv6 [RFC5213], and DMM [RFC7333][RFC7429][I-D.DMM-PMIPv6].

7. References

7.1. Normative References


7.2. Informative References


Appendix A.  Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

Authors’ Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4957
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

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

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu

Zhong Xiang
Department of Electrical and Computer Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 10 9895 1211
Fax: +82 31 290 7996
EMail: xz618@skku.edu
IPv6 Neighbor Discovery for IP-Based Vehicular Networks
draft-jeong-ipwave-vehicular-neighbor-discovery-06

Abstract

This document specifies a Vehicular Neighbor Discovery (VND) as an extension of IPv6 Neighbor Discovery (ND) for IP-based vehicular networks. An optimized Address Registration and a multihop Duplicate Address Detection (DAD) mechanism are performed for having operation efficiency and also saving both wireless bandwidth and vehicle energy. Also, three new ND options for prefix discovery, service discovery, and mobility information report are defined to announce the network prefixes and services inside a vehicle (i.e., a vehicle’s internal network). Finally, a mobility management scheme is proposed for moving vehicles in vehicular environments to support seamless communication for the continuity of transport-layer sessions (e.g., TCP connections).

Status of This Memo

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

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

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

This Internet-Draft will expire on September 12, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.
This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction ................................. 3
2. Requirements Language ........................ 3
3. Terminology ................................ 3
4. Overview ................................... 4
   4.1. Link Model ................................ 5
   4.2. ND Optimization ......................... 6
   4.3. Design Goals ............................. 6
5. Vehicular Network Architecture .............. 7
   5.1. Vehicular Network ....................... 7
   5.2. V2I Internetworking ..................... 9
   5.3. V2V Internetworking ..................... 10
6. ND Extension for Prefix and Service Discovery .... 11
   6.1. Vehicular Prefix Information Option ...... 11
   6.2. Vehicular Service Information Option ..... 12
   6.3. Vehicular Mobility Information Option ... 13
   6.4. Vehicular Neighbor Discovery ............ 14
   6.5. Message Exchange Procedure for V2I Networking ...... 15
7. Address Registration and Duplicate Address Detection .... 16
   7.1. Address Autoconfiguration ................ 17
   7.2. Address Registration .................... 17
   7.3. Multihop Duplicate Address Detection .... 18
   7.4. Pseudonym Handling ...................... 21
8. Mobility Management .......................... 21
9. Security Considerations ...................... 24
10. References .................................. 24
    10.1. Normative References ................... 24
    10.2. Informative References ................. 25
Appendix A. Changes from draft-jeong-ipwave-vehicular-neighbor-discovery-05 ...................... 27
Appendix B. Acknowledgments .................... 27
Authors’ Addresses ............................ 27
1. Introduction

Vehicular Ad Hoc Networks (VANET) have been researched for Intelligent Transportation System (ITS) such as driving safety, efficient driving and entertainment. Considering the high-speed mobility of vehicular network based on Dedicated Short-Range Communications (DSRC), IEEE 802.11p [IEEE-802.11p] has been specialized and was renamed IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012. IEEE has standardized Wireless Access in Vehicular Environments (WAVE) [DSRC-WAVE] standard which is considered as a key component in ITS. The IEEE 1609 standards such as IEEE 1609.0 [WAVE-1609.0], 1609.2 [WAVE-1609.2], 1609.3 [WAVE-1609.3], 1609.4 [WAVE-1609.4] provide a low-latency and alternative network for vehicular communications. What is more, IP-based vehicular networks specialized as IP Wireless Access in Vehicular Environments (IPWAVE) [IPWAVE-PS] can enable many use cases over vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communications.

VANET features high mobility dynamics, asymmetric and lossy connections, and moderate power constraint (e.g., electric cars and unmanned aerial vehicles). Links among hosts and routers in VANET can be considered as undetermined connectivities with constantly changing neighbors described in [RFC5889]. IPv6 [RFC8200] is selected as the network-layer protocol for Internet applications by IEEE 1609.0 and 1609.3. However, the relatively long-time Neighbor Discovery (ND) process in IPv6 [RFC4861] is not suitable in VANET scenarios.

To support the interaction between vehicles or between vehicles and Rode-Side Units (RSUs), this document specifies a Vehicular Neighbor Discovery (VND) as an extension of IPv6 ND for IP-based vehicular networks. VND provides vehicles with an optimized Address Registration, a multihop Duplicate Address Detection (DAD), and an efficient mobility management scheme to support efficient V2V, V2I, and V2X communications.

2. Requirements Language

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].

3. Terminology

This document uses the terminology described in [RFC4861], [RFC4862], and [RFC6775]. In addition, the following new terms are defined as below:
o WAVE: Acronym for "Wireless Access in Vehicular Environments" [WAVE-1609.0].

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

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

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

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

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

4. Overview

This document proposes an optimized ND with a more adaptive structure for vehicular networks considering fast vehicle mobility and wireless control traffic overhead related to the legacy ND. Furthermore, prefix and service discovery can be implemented as part of the ND’s process along with an efficient Address Registration procedure and DAD mechanism for moving vehicles. This document specifies a set of behaviors between vehicles and RSUs to accomplish these goals.
4.1. Link Model

There is a relationship between a link and a network prefix along with reachability scopes, such as link-local and global scopes. The legacy IPv6 ND protocol [RFC4861] has the following link model. All IPv6 nodes in the same on-link subnet, which use the same subnet prefix with on-link bit set, are reachable with each other by one-hop link. The symmetry of the connectivity among the nodes is preserved, that is, bidirectional connectivity among two on-link nodes. However, a link model in vehicular networks (called vehicular link model) should consider the asymmetry of the connectivity that unidirectional links can exist due to interference in wireless channels and the different levels of transmission power in wireless network interfaces.

The on-link subnet can be constructed by one link (as a basic service set) or multiple links (as an extended service set) called a multi-link subnet [RFC6775]. In the legacy multi-link subnet, an all-node-multicasted packet is copied and related to other links by an ND proxy. On the other hand, in vehicular networks having fast moving vehicles, multiple links can share the same subnet prefix for operation efficiency. For example, if two wireless links under two adjacent RSUs are in the same subnet, a vehicle as an IPv6 host does not need to reconfigure its IPv6 address during handover between those RSUs. However, the packet relay by an RSU as an ND proxy is not required because such a relay can cause a broadcast storm in the extended subnet. Thus, in the multi-link subnet, all-node-multicasting needs to be well-calibrated to either being confined to multicasting in the current link or being disseminated to other links in the same subnet.

In a connected multihop VANET, for the efficient communication, vehicles in the same link of an RSU can communicate directly with each other, not through the serving RSU. This direct wireless communication is similar to the direct wired communication in an on-link subnet using Ethernet as a wired network. The vehicular link model needs to accommodate both the ad-hoc communication between vehicles and infrastructure communication between a vehicle and an RSU in an efficient and flexible way. Therefore, the IPv6 ND should be extended to accommodate the concept of a new IPv6 link model in vehicular networks.

To support multi-link subnet, this specification employs the Shared-Prefix model for prefix assignments. Shared-Prefix model refer to an addressing model where the prefix(es) are shared by more than one node. In this document, we assume that in a specified subnet, all interfaces of RSUs responding for prefix assignments to vehicles hold
same prefix, which ensure vehicles obtain and maintain same prefix in this subnet scope.

4.2. ND Optimization

This document takes advantage of the optimized ND for Low-Power Wireless Personal Area Network (6LoWPAN) [RFC6775] because vehicular environments have common parts with 6LoWPAN, such as the reduction of unnecessary wireless traffic by multicasting and the energy saving in battery. Note that vehicles tend to be electric vehicles whose energy source is from their battery.

In the optimized IPv6 ND for 6LoWPAN, the connections among nodes are assumed to be asymmetric and unidirectional because of changing radio environment and loss signal. The authors proposed an improved IPv6 ND which greatly eliminates link-scope multicast to save energy by constructing new options and a new scheme for address configurations. Similarly, this document proposes an improved IPv6 ND by eliminating many link-scope-multicast-based ND operations, such as DAD for IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862]. Thus, this document suggests an extension of IPv6 ND as vehicular ND tailored for vehicular networks along with new ND options (e.g., prefix discovery, service discovery, and mobility information options).

4.3. Design Goals

The vehicular ND in this document has the following design goals:

- To perform prefix and service discovery through ND procedure;
- To implement host-initiated refresh of Router Advertisement (RA) and remove the necessity for routers to use periodic or unsolicited multicast RA to find hosts;
- To replace Neighbor Unreachable Detection (NUD), create Neighbor Cache Entries (NCE) for all registered vehicles in RSUs and MA by appending Address Registration Option (ARO) in Neighbor Solicitation (NS), Neighbor Advertisement (NA) messages;
- To support a multihop DAD with two new ICMPv6 messages called Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) to eliminate multicast storm and save energy;
- To support multi-hop communication for vehicles outside the coverage of RSUs to communicate with the serving RSU via a relay neighbor; and
To provide a mobility management mechanism for seamless communication during a vehicle’s travel in subnets via RSUs.

5. Vehicular Network Architecture

This section describes a vehicular network architecture for V2V and V2I communication. A vehicle and an RSU have their internal networks including in-vehicle devices or servers, respectively.

5.1. Vehicular Network

A vehicular network architecture for V2I and V2V is illustrated in Figure 1. Three RSUs are deployed along roadside and are connected to an MA through wired links. There are two subnets such as Subnet1 and Subnet2. The wireless links of RSU1 and RSU2 belong to the same subnet named Subnet1, but the wireless link of RSU3 belongs to another subnet named Subnet2. Vehicle2 is wirelessly connected to RSU1 while Vehicle3 and Vehicle4 are connected to RSU2 and RSU3, respectively. Vehicles can directly communicate with each other through V2V connection (e.g., Vehicle1 and Vehicle2) to share driving information. In addition, vehicles not in range of any RSU may connect with RSU in multi-hop connection via relay vehicle (e.g., Vehicle1 can contact RSU1 via Vehicle2). Vehicles are assumed to start the connection to an RSU when they entered the coverage of the RSU.

The document recommends a multi-link subnet involving multiple RSUs as shown in Figure 1. This recommendation aims at the reduction of the frequency with which vehicles have to change their IP address during handover between two adjacent RSUs. To construct this multi-link subnet, shared-prefix model is proposed. That is, for RSUs in the same subnet, the interfaces responsible for prefix assignment for vehicles should hold the same prefix in their global address. This also promises vehicles achieve same prefix in this scope. When they pass through RSUs in the same subnet, vehicles do not need to perform the Address Registration and DAD again because they can use their current IP address in the wireless coverage of the next RSU. Moreover, this proposal accord with the assumption that noes belonging to the same IP prefix are able to communicate with each other directly. On the other hand, if vehicles enter the wireless coverage of an RSU belonging to another subnet with a different prefix, they repeat the Address Registration and DAD procedure to update their IP address with the new prefix.
In Figure 1, RSU1 and RSU2 are deployed in a multi-link subnet with the same prefix address in their interfaces responding for connection with vehicles. When vehicle2 leaves the coverage of RSU1 and enters RSU2, it maintains its address configuration and ignores Address Registration and DAD steps. If vehicle2 moves into the coverage of RSU3, since RSU3 belongs to another subnet and holds a different prefix from RSU1 and RSU2, so vehicle2 must do Address Registration and DAD just as connecting to a new RSU. Note that vehicles and RSUs have their internal networks including in-vehicle devices and servers, respectively. The structures of the internal networks are described in [IPWAVE-PS].
5.2. V2I Internetworking

This subsection explains V2I interntworking between vehicle network and RSU network where vehicle network is an internal network in a vehicle, and RSU network is an internal network in an RSU, as shown in Figure 2.

Figure 2: Internetworking between Vehicle Network and RSU Network

Figure 2 shows the V2I networking of a vehicle and an RSU whose internal networks are Moving Network1 and Fixed Network1, respectively. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). RSU1 has the DNS Server (RDNSS3), one host (Host5), the two routers (Router5 and Router6).

It is assumed that RSU1 has a collection of servers (Server1 to ServerN) for various services in the road networks, such as road emergency notification and navigation services. Vehicle1’s Router1 and RSU1’s Router3 use 2001:DB8:1:1::/64 for an external link (e.g.,
DSRC) for I2V networking for various vehicular services. The vehicular applications, such as road emergency notification and navigation services, can be registered into the DNS Server (i.e., RDNSS) through DNSNA protocol in [ID-DNSNA] along with IPv6 ND DNS options in [RFC8106].

Vehicle1’s Router1 and RSU1’s Router5 can know what vehicular applications exist in their internal network by referring to their own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know what network prefixes exist in their internal network through an intra-domain routing protocol, such as OSPF. Each vehicle and each RSU announce their network prefixes and services through ND options defined in Section 6.

5.3. V2V Internetworking

This subsection explains V2V internetworking between vehicle networks, which are internal networks in vehicles, as shown in Figure 3.

![Diagram of Internetworking between Vehicle Networks](image)

Figure 3: Internetworking between Vehicle Networks
Figure 3 shows the V2V networking of two vehicles whose internal networks are Moving Network1 and Moving Network2, respectively. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). Vehicle2 has the DNS Server (RDNSS2), the two hosts (Host3 and Host4), and the two routers (Router3 and Router4).

It is assumed that Host1 and Host3 are running a Cooperative Adaptive Cruise Control (C-ACC) program for physical collision avoidance. Also, it is assumed that Host2 and Host4 are running a Cooperative On-board Camera Sharing (C-OCS) program for sharing road hazards or obstacles to avoid road accidents. Vehicle1’s Router1 and Vehicle2’s Router3 use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking for various vehicular services. The vehicular applications, such as C-ACC and C-BCS, can be registered into the DNS Server (i.e., RDNSS) through DNSNA protocol in [ID-DNSNA] along with IPv6 ND DNS options in [RFC8106].

Vehicle1’s Router1 and Vehicle2’s Router3 can know what vehicular applications exist in their internal network by referring to their own RDNSS through the DNSNA protocol [ID-DNSNA]. They can also know what network prefixes exist in their internal network through an intra-domain routing protocol, such as OSPF. Each vehicle announces its network prefixes and services through ND options defined in Section 6.

6. ND Extension for Prefix and Service Discovery

This section specifies an IPv6 ND extension for vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I) networking. This section also defines three new ND options for prefix discovery, service discovery, and mobility information report: (i) Vehicular Prefix Information (VPI) option, (ii) Vehicular Service Information (VSI) option, and (iii) Vehicular Mobility Information (VMI) option. It also describes the procedure of the ND protocol with those options.

6.1. Vehicular Prefix Information Option

The VPI option contains IPv6 prefix information in the internal network. Figure 4 shows the format of the VPI option.
Fields:

Type
  8-bit identifier of the VPI option type as assigned by the IANA: TBD

Length
  8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The value is 3.

Prefix Length
  8-bit unsigned integer. The number of leading bits in the Prefix that are valid. The value ranges from 0 to 128.

Distance
  8-bit unsigned integer. The distance between the subnet announcing this prefix and the subnet corresponding to this prefix in terms of the number of hops.

Reserved
  This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Prefix
  An IP address or a prefix of an IP address. The Prefix Length field contains the number of valid leading bits in the prefix. The bits in the prefix after the prefix length are reserved and MUST be initialized to zero by the sender and ignored by the receiver.

6.2. Vehicular Service Information Option

The VSI option contains vehicular service information in the internal network. Figure 5 shows the format of the VSI option.
6.3. Vehicular Mobility Information Option

The VMI option contains one vehicular mobility information of a vehicle or an RSU. Figure 6 shows the format of the VMI option.

Figure 5: Vehicular Service Information (VSI) Option Format

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>8-bit identifier of the VSI option type as assigned by the IANA: TBD</td>
</tr>
<tr>
<td>Length</td>
<td>8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The value is 3.</td>
</tr>
<tr>
<td>Reserved1</td>
<td>This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.</td>
</tr>
<tr>
<td>Protocol</td>
<td>8-bit unsigned integer to indicate the upper-layer protocol, such as transport-layer protocol (e.g., TCP, UDP, and SCTP).</td>
</tr>
<tr>
<td>Reserved2</td>
<td>This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.</td>
</tr>
<tr>
<td>Port Number</td>
<td>16-bit unsigned integer to indicate the port number for the protocol.</td>
</tr>
<tr>
<td>Service Address</td>
<td>128-bit IPv6 address of a node proving this vehicular service.</td>
</tr>
</tbody>
</table>
Fields:

Type   8-bit identifier of the VMI option type as assigned by the IANA: TBD

Length 8-bit unsigned integer. The length of the option (including the Type and Length fields) is in units of 8 octets. The value is 3.

Reserved1 This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Reserved2 This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Mobility Information 128-bit mobility information, such as position, speed, and direction.

6.4. Vehicular Neighbor Discovery

Prefix discovery enables hosts (e.g., vehicles and in-vehicle devices) to distinguish destinations on the same link from those only reachable via RSUs. A vehicle (or its in-vehicle devices) can directly communicate with on-link vehicles (or their in-vehicle devices) without the relay of an RSU, but through V2V communications along with VPI ND option. This VPI option contains IPv6 prefixes in a vehicle’s internal network.

Vehicles announce services in their internal networks to other vehicles through an VSI ND option. The VSI option contains a list of vehicular services in a vehicle’s or an RSU’s internal network.
A vehicle periodically announces an NS message containing VPI and VSI options with its prefixes and services in all-nodes multicast address to reach all neighboring nodes. When it receives this NS message, another neighboring node responds to this NS message by sending an NA message containing the VPI and VSI options with its prefixes and services via unicast towards the NS-originating node.

Therefore, prefix and service discovery can be achieved via ND messages (e.g., NS and NA) by vehicular ND with VPI and VSI options. This VND-based discovery eliminates an additional prefix and service discovery scheme, such as DNS-based Service Discovery [RFC6763] (e.g., Multicast DNS (mDNS) [RFC6762] and DNSNA [ID-DNSNA]), other than ND. That is, vehicles and RSUs can rapidly discover the network prefixes and services of the other party without any additional service discovery protocol.

6.5. Message Exchange Procedure for V2I Networking

This subsection explains a message exchange procedure for vehicular neighbor discovery in V2I networking, where a vehicle communicates with its corresponding node in the Internet via an RSU.

Figure 7 shows an example of message exchange procedure in V2I networking. Detailed steps of the procedure are explained in Section 7 and Section 8.

Note that a vehicle could also perform the prefix and service discovery simultaneously along with Address Registration procedure, as shown in Figure 9.

This document specified that RSUs as routers do not transmit periodical and unsolicited multicast RA messages including a prefix for energy saving in vehicular networks. Vehicles as hosts periodically initiate an RS message according to a time interval (considering its position and an RSU’s coverage). Since they have a digital road map with the information of RSUs (e.g., position and communication coverage), vehicles can know when they will go out of the communication range of an RSU along with the signal strength (e.g., Received Channel Power Indicator (RCPI) [VIP-WAVE]) from the RSU. RSUs replies with a solicited RA in unicast only when they receive an RS message.
7. Address Registration and Duplicate Address Detection

This section explains address configuration, consisting of IP Address Autoconfiguration, Address Registration, and multihop DAD via V2I or V2V.

This document recommends a new Address Registration and DAD scheme in order to avoid multicast flooding and decrease link-scope multicast for energy and wireless channel conservation on a large-scale vehicular network. Host-initiated refresh of RA removes the necessity for routers to use frequent and unsolicited multicast RAs to accommodate hosts. This also enables the same IPv6 address prefix(es) to be used across a subnet.

There are three scenarios feasible in Address Registration scheme:
1. Vehicle enters the subnet for the first time or the current RSU belongs to another subnet: Vehicles need to perform the Address Registration and multihop DAD in the following subsections.

2. Vehicle has already configured its IP addresses with prefix obtained from the previous RSU, and the current RSU located in the same subnet: This means RSUs have the same prefix and the vehicle has no need to repeat the Address Registration and multihop DAD.

3. Vehicle is not in the coverage of RSU but has a neighbor registered in RSU: This document proposes a new V2V scenario for vehicles which are currently not in the range of the RSU. If a user vehicle failed to find an on-link RSU, it starts to look for adjacent vehicle neighbors which can work as relay neighbor to share the prefix obtained from RSU and undertake the DAD of the user vehicle by forwarding DAD messages to RSU.

7.1. Address Autoconfiguration

A vehicle as an IPv6 host creates its link-local IPv6 address and global IPv6 address as follows [RFC4862]. When they receive RS messages from vehicles, RSUs send back RA messages containing prefix information. The vehicle makes its global IPv6 addresses by combining the prefix for its current link and its link-layer address.

The address autoconfiguration does not perform the legacy DAD as defined in [RFC4862]. Instead, a new multihop DAD is performed in Section 7.3.

7.2. Address Registration

After its IP tentative address autoconfiguration with the known prefix from an RSU and its link-layer address, a vehicle starts to register its IP address to the serving RSU along with multihop DAD. Address Register Option (ARO) is used in this step and its format is defined in [RFC6775].

ARO is always host-initiated by vehicles. Information such as registration time and registration status contained in ARO is also included in multihop Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages used between RSU and MA, but ARO is not directly used in these two messages.

An example message exchange procedure of Address Registration is presented in Figure 8. Since Address Registration is performed simultaneously with the multihop DAD, the specific procedure is together described with the DAD mechanism in Section 7.3.
Before it can exchange data, a node should determine whether its IP address is already used by another node or not. In the legacy IPv6 ND, hosts multicast NS messages to all nodes in the same on-link subnet for DAD. Instead of this, an optimized multihop DAD is designed to eliminate multicast messages for energy-saving purpose. For this multihop DAD, Neighbor Cache and DAD Table are maintained by each RSU and an MA, respectively, for the duplicate address inspection during the multihop DAD process. That is, each RSU makes Neighbor Cache Entries (NCE) of all the on-link hosts in its Neighbor Cache. Similarly, the MA stores all the NCEs reported by the RSUs in its DAD Table.

With the multihop DAD, a vehicle can skip the multicast-based DAD in its current wireless link whenever it enters the coverage of another RSU in the same subset, leading to the reduction of traffic overhead in vehicular wireless links.

For the multihop DAD, two new ICMPv6 message types are defined in [RFC6775], such as Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC). Information carried by ARO options are copied into these two messages for the multihop DAD in the MA.
Figure 9: Neighbor Discovery Address Registration with Multihop DAD

Figure 9 presents the procedure of Address Registration and multihop DAD. The detailed steps are explained as follows.

1. A vehicle sends an NS message to the current RSU in unicast, containing the ARO to RSU to register its address.

2. The RSU receives the NS message, and then inspects its Neighbor Cache to check whether it is duplicate or not. If there is no duplicate NCE, a tentative NCE is created for this address, and then the RSU sends a DAR to the MA for the multicast DAD.

3. When the MA receives a DAR from an RSU, it checks whether the register-requested address exists in its DAD Table or not. If an entry with the same address exists in the DAD Table, which means that the address is considered "Duplicate Address", then MA returns a DAC message to notify the RSU of the address duplication. If no entry with the same address exists in the DAD Table, which means that an entry for the address is created, then MA replies a DAC message to the RSU to confirm the uniqueness of the register-requested address to the RSU.

4. If the address duplication is notified by the MA, the RSU deletes the tentative NCE, and sends back an NS to the address-registration vehicle to notify the registration failure. Otherwise, the RSU changes the tentative NCE into a registered NCE in its Neighbor Cache, and then send back an NS to the vehicle to notify the registration success.
Thus, the multihop DAD is processed simultaneously with the Address Registration. Note that the tentative address is not considered assigned to the vehicle until the MA confirms the uniqueness of the register-requested address in the multihop DAD.

<table>
<thead>
<tr>
<th>User Vehicle</th>
<th>Relay Vehicle</th>
<th>RSU</th>
<th>Mobility Anchor</th>
</tr>
</thead>
<tbody>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>-----</td>
<td>-----------------</td>
</tr>
<tr>
<td>RD failed</td>
<td></td>
<td>-----</td>
<td>Same as Figure 9</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>-----</td>
<td>-----------------</td>
</tr>
<tr>
<td>--NS--</td>
<td></td>
<td>-----</td>
<td>Forward NS -----</td>
</tr>
<tr>
<td>&lt;-NA with Prefix Info--</td>
<td></td>
<td>-----</td>
<td>Forward NS -----</td>
</tr>
<tr>
<td>--NS with Address</td>
<td>[ARO+VPI+VSI]</td>
<td>-----</td>
<td>Same as Figure 9</td>
</tr>
<tr>
<td>[ARO+VPI+VSI]</td>
<td></td>
<td>-----</td>
<td>-----------------</td>
</tr>
<tr>
<td>&lt;----- Forward NA ----&gt;</td>
<td></td>
<td>-----</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>&lt;--NA with Address Reg--</td>
<td>[ARO+VPI+VSI]</td>
<td></td>
</tr>
</tbody>
</table>

Figure 10: Address Registration and Multihop DAD via V2V Relay

If a vehicle failed to register a default router, it triggers neighbor discovery to look for vehicle neighbors which can provide relay service using multi-hop communication. In this specification, we assumed vehicles would not emulate V2V communication and trigger relay scenario only if Router Discovery (RD) failed. On the other hand, at most one intermediate vehicle acts as a relay for another vehicle to communicate with the RSU.

Since vehicles have a digital road map with the information of RSUs (e.g., position and communication coverage), they can determine if they are available to serve as relay vehicle. Only vehicles with ability to serve as temporary relays will take action when they receive relay service requests. The user vehicle can process global address configuration, Address Registration and DAD through relay vehicle before it enters the coverage of RSUs. See Figure 10.
When a user vehicle failed to directly register with a RSU, it initiates neighbor discovery to detect vehicle neighbors through V2V communication. Vehicle sends NS messages to connect with neighbors in range. If neighbor can provide relay service, it creates a NCE for user vehicle, setting its own address as relay address, and sends back NA with prefix information received from RSU.

With receipt of NA, user vehicle configures its global address with prefix information as mentioned in Section 7.1. After this, user vehicle takes up to initiate the Address Registration along with DAD process via relay vehicle. NS message is configured as specified in Section 7.2 but indicate the relay vehicle’s address as next-hop for reaching the RSU. In such a case, when relay vehicle receives relay request message, it will forward NS message to RSU. The procedure set up on the rails except MA will include the relay vehicle’s address as relay address in NCE to indicate that at this moment it is not a directly attached vehicle, and set the relay address as next-hop address. Relay vehicle forwards DAD result information message to user vehicle as soon as it received.

7.4. Pseudonym Handling

Considering the privacy protection of a vehicle, a pseudonym mechanism for its link-layer address is requested. This mechanism periodically modifies the link-layer address, leading to the update of the corresponding IP address. A random MAC Address Generation mechanism is proposed in Appendix F.4 of [IEEE-802.11-OCB] by generating the 46 remaining bits of MAC address using a random number generator. When it changes its MAC address, a vehicle should ask the serving RSU to update its own NCE, and to register its IP address into the MA again.

8. Mobility Management

A mobility management is required for the seamless communication of vehicles moving between the RSUs. When a vehicle moves into the coverage of another RSU, a different IP address is assigned to the vehicle, resulting in the reconfiguration of transport-layer session information (i.e., end-point IP address) to avoid service disruption. Considering this issue, this document proposes a handover mechanism for seamless communication.
In [VIP-WAVE], the authors constructed a network-based mobility management scheme using Proxy Mobile IPv6 (PMIPv6) [RFC5213], which is highly suitable to vehicular networks. This document uses a mobility management procedure similar to PMIPv6 along with prefix discovery.

Figure 11 shows the binding update flow when a vehicle entered the subnet of an RSU. RSUs act as Mobility Anchor Gateway (MAG) defined in [VIP-WAVE]. When it receives RS messages from a vehicle containing its mobility information (e.g., position, speed, and direction), an RSU sends its MA a Proxy Binding Update (PBU) message [RFC5213][RFC3775], which contains a Mobility Option for the vehicle’s mobility information. The MA receives the PBU and sets up a Binding Cache Entry (BCE) as well as a bi-directional tunnel (denoted as Bi-Dir Tunnel in Figure 11) between the serving RSU and itself. Through this tunnel, all traffic packets to the vehicle are encapsulated toward the RSU. Simultaneously, the MA sends back a Proxy Binding Acknowledgment (PBA) message to the serving RSU. This serving RSU receives the PBA and sets up a bi-directional tunnel with the MA. After this binding update, the RSU sends back an RA message to the vehicle including its own prefix for the address autoconfiguration.
When the vehicle changes its location, the MA has to change the end-point of the tunnel for the vehicle into the new RSU’s IP address. As shown in Figure 12, when the MA receives a new PBU from the new RSU, it changes the tunnel’s end-point from the current RSU (c-RSU) to the new RSU (n-RSU). If there is ongoing IP packets toward the vehicle, the MA encapsulates the packets and then forwards them towards n-RSU. Through this network-based mobility management, the vehicle is not aware of any changes at its network layer and can maintain its transport-layer sessions without any disruption.

If c-RSU and n-RSU are adjacent, that is, vehicles are moving in specified routes with fixed RSU allocation, the procedure can be simplified by constructing bidirectional tunnel directly between them (cancel the intervention of MA) to alleviate the traffic flow in MA as well as reduce handover delay. See Figure 13.
Since RSUs are in charge of detecting when a node joins or moves through its domain, if c-RSU detects the vehicle is going to leave its coverage and enter the area of adjacent RSU, it sends a PBU message to inform n-RSU about the handover of vehicle and update its mobility information. n-RSU receives the request and construct a bidirectional tunnel between c-RSU and itself, then send back PBA message for acknowledgment. If there are ongoing IP packets, c-RSU encapsulates the packets and then forwards them to n-RSU. When n-RSU detects the entrance of the vehicle, it directly sends RA message to vehicle for connection establishment (or replies solicited RA if vehicle sends request RS message first).

9. Security Considerations

This document shares all the security issues of the neighbor discovery protocol and 6LoWPAN protocol. This document can get benefits from secure neighbor discovery (SEND) [RFC3971] in order to protect ND from possible security attacks.

10. References

10.1. Normative References


10.2. Informative References

[DSRC-WAVE]

[ID-DNSNA]

[IEEE-802.11-OCB]
[IEEE-802.11p]

[IPWAVE-PS]


[VIP-WAVE]

[WAVE-1609.0]

[WAVE-1609.2]

[WAVE-1609.3]

[WAVE-1609.4]
Appendix A. Changes from draft-jeong-ipwave-vehicular-neighbor-discovery-05

The following changes are made from draft-jeong-ipwave-vehicular-neighbor-discovery-05:

- In Section 4.1, a Shared-Prefix model is introduced for prefix assignment specified in this document.
- In Section 4.3, design goals are refined including the cancellation of Neighbor Unreachable Detection, and also the support of multi-hop communication for vehicles not in the coverage of RSUs.
- In Section 5.1, the Vehicular Network Architecture is updated on subnet division and V2V communication.
- In Section 7, a new scenario is added to facilitate vehicles outside the coverage of RSU to do Address Registration and DAD via relay vehicle.
- In Section 8, a simplified mobility management in vehicle handoff for adjacent RSUs is supplemented based on the original proposal.

Appendix B. Acknowledgments

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A1B03035885).

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

Authors' Addresses

Jaehoon Paul Jeong
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4957
Fax: +82 31 290 7996
EMail: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php
Yiwen Chris Shen  
Department of Electrical and Computer Engineering
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon, Gyeonggi-Do 16419  
Republic of Korea  
Phone: +82 31 299 4106  
Fax: +82 31 290 7996  
EMail: chrisshen@skku.edu

Zhong Xiang  
Department of Electrical and Computer Engineering  
Sungkyunkwan University  
2066 Seobu-Ro, Jangan-Gu  
Suwon, Gyeonggi-Do 16419  
Republic of Korea  
Phone: +82 10 9895 1211  
Fax: +82 31 290 7996  
EMail: xz618@skku.edu
Urban Air Mobility Implications for Intelligent Transportation Systems
draft-templin-ipwave-uam-its-00.txt

Abstract

Urban Air Mobility concerns the introduction of manned and unmanned aircraft within urban environments, while Intelligent Transportation Systems have traditionally considered only terrestrial vehicles operating on city streets and highways. This document considers the implications for introduction of low-altitude aircraft within urban environments operating in harmony with ground transportation.

Status of This Memo

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

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

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

This Internet-Draft will expire on September 12, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
1. Introduction

Urban Air Mobility (UAM) concerns the introduction of manned and unmanned aircraft within urban environments. NASA has initiated a program known as the Urban Air Mobility grand challenge with the goal to promote public confidence in UAM safety and facilitate community-wide learning while capturing the public’s imagination [UAM].

Autonomy will play a pivotal role in the acceptance of low-altitude operations for aerial vehicles operating in harmony with traditional ground transportation and pedestrian traffic. The UAM vision therefore builds on evolving works on Unmanned Air Systems (UAS), including the NASA UAS Traffic Management (UTM) service model [UTM].

Use cases for autonomous aircraft in the UAM vision are endless, and include personal air vehicles, flying taxis, parcel delivery, law enforcement and countless others. Major industry leaders such as Airbus [AIRBUS] and Boeing [BOEING] have accordingly begun to articulate their UAM strategies. Programs such as Uber Elevate [UBER] anticipate deployment as early as within the next 2-5 years.

With the advent of the UAM vision and its related initiatives, questions arise as to how the new model will be harmonized with the existing terrestrial mobility environment. Directions for modernizing terrestrial mobility are emerging in programs such as the US Department of Transportation’s Intelligent Transportation Systems [ITS] and anticipate an increasing role for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. The IETF recognizes this need and has formed the IP Wireless Access in Vehicular Environments (IPWAVE) working group with charter to produce a document that will specify the mechanisms for transmission of IPv6.
This document anticipates a need to provide a unified V2V and V2I service for all urban mobility agents, including both terrestrial and airborne. Urban air vehicles will employ Vertical Takeoff And Landing (VTOL) and will operate at altitudes below 400 feet, such that coordinations with terrestrial vehicles will be inevitable and commonplace. This work therefore proposes that urban air vehicles also employ a short-range V2V / V2I communications capability using the same types of wireless networking gear used in the terrestrial domain (e.g., DSRC, C-V2X, etc.).

As stated by the Boeing CEO in a January 23, 2019 press release, think of the urban mobility landscape as evolving from a two dimensional to a three dimensional environment. Vehicles both on the ground and in the air will therefore need to coordinate with one another on a V2V and V2I basis even when supporting communications infrastructure such as cell towers are unavailable or otherwise too congested to support realtime exchanges. The ipwave working group is therefore advised to consider the rapidly emerging and inevitable Urban Air Mobility future.

2. Terminology

Terms such as Intelligent Transportation Systems (ITS), Urban Air Mobility (UAM), Unmanned Air Systems (UAS), UAS Traffic Management (UTM) and many others apply to the emerging urban mobility landscape. IETF keywords per [RFC2119] are not applicable within the scope of this document.

3. Applicability

Urban Air Mobility and Intelligent Transportation System concepts apply within all major urban areas worldwide.

4. Implementation Status

Early prototyping and testing are underway.

5. IANA Considerations

This document introduces no IANA considerations.
6. Security Considerations

Communications networking security is necessary to preserve the confidentiality, integrity and availability necessary for V2V and V2I coordinations.

7. Acknowledgements

Discussions on the IETF ipwave list (its@ietf.org) helped motivate this document.

8. References

8.1. Normative References


8.2. Informative References


Author’s Address
Fred L. Templin (editor)
Boeing Research & Technology
P.O. Box 3707
Seattle, WA  98124
USA

Email: fltemplin@acm.org
TLS Authentication using ETSI TS 103 097 and IEEE 1609.2 certificates
draft-tls-certieee1609-02.txt

Abstract

This document specifies the use of a new certificate type to authenticate TLS entities. The first type enables the use of a certificate specified by the Institute of Electrical and Electronics Engineers (IEEE) and the European Telecommunications Standards Institute (ETSI).

Status of This Memo

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

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

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

This Internet-Draft will expire on April 25, 2019.

Copyright Notice

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

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
1. Introduction

The TLS protocol [RFC8446] [RFC5246] uses X509 and Raw Public Key in order to authenticate servers and clients. This document describes the use of certificates specified either by the Institute of Electrical and Electronics Engineers (IEEE) [IEEE1609.2] or the European Telecommunications Standards Institute (ETSI) [TS103097]. It is worth mentioning that the ETSI TS 103097 certificate is a profile of IEEE 1609.2 certificate and uses the same data structure. These standards are defined in order to secure communications in vehicular environments. Existing authentication methods, such as X509 and Raw Public Key, are designed for Internet use, particularly for flexibility and extensibility, and are not optimized for bandwidth and processing time to support delay-sensitive applications. That is why size-optimized certificates were standardized by ETSI and IEEE to secure data exchange in highly dynamic vehicular environment in Intelligent Transportation System (ITS).
2. Requirements 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 [RFC2119].

3. Extension Overview

This specification extends the Client Hello and Server Hello 
messages, by using the "extension_data" field of the ClientCertType 
Extension and the ServerCertType Extension structures defined in 
RFC7250. In order to negotiate the support of IEEE 1609.2 or ETSI TS 
103097 certificate-based authentication, the clients and the servers 
MAY include the extension of type "client_certificate_type" and 
"server_certificate_type" in the extended Client Hello and 
"EncryptedExtensions". The "extension_data" field of this extension 
SHALL contain a list of supported certificate types proposed by the 
client as provided in the figure below:

/* Managed by IANA */
enum {
    X509(0),
    RawPublicKey(2),
    1609Dot2(?, /* Number 3 will be requested for 1609.2 */
    (255)
} CertificateType;

struct {
    select (certificate_type) {
        / * certificate type defined in this document. */
        case 1609Dot2:
            opaque cert_data<1..2^24-1>;
        / * RawPublicKey defined in RFC 7250 */
        case RawPublicKey:
            opaque ASN.1_subjectPublicKeyInfo<1..2^24-1>;
        / * X.509 certificate defined in RFC 5246 */
        case X.509:
            opaque cert_data<1..2^24-1>;
    }

    Extension extensions<0..2^16-1>;
} CertificateEntry;
In case where the TLS server accepts the described extension, it selects one of the certificate types in the extension described above. Note that a server MAY authenticate the client using other authentication methods. The end-entity certificate’s public key has to be compatible with one of the certificate types listed in the extension described above.

4. TLS Client and Server Handshake

The "client_certificate_type" and "server_certificate_type" extensions MUST be sent in handshake phase as illustrated in Figure 1 below. The same extension shall be sent in Server Hello for TLS 1.2.
In order to indicate the support of IEEE 1609.2 or ETSI TS 103097 certificates, client MUST include an extension of type "client_certificate_type" and "server_certificate_type" in the extended Client Hello message. The Hello extension is described in Section 4.1.2 of TLS 1.3 [RFC8446].
The extension ‘client_certificate_type’ sent in the client hello MAY carry a list of supported certificate types, sorted by client preference. It is a list in the case where the client supports multiple certificate types.

Client MAY respond along with supported certificates by sending a "Certificate" message immediately followed by the "CertificateVerify" message. These specifications are valid for TLS 1.2 and TLS 1.3.

All implementations SHOULD be prepared to handle extraneous certificates and arbitrary orderings from any TLS version, with the exception of the end-entity certificate which MUST be first.

4.2. Server Hello

When the server receives the Client Hello containing the client_certificate_type extension and/or the server_certificate_type extension, the following options are possible:

- The server supports the extension described in this document. It selects a certificate type from the client_certificate_type field in the extended Client Hello and must take into account the client authentication list priority.

- The server does not support the proposed certificate type and terminates the session with a fatal alert of type "unsupported_certificate".

- The server does not support the extension defined in this document. In this case, the server returns the server hello without the extensions defined in this document in case of TLS 1.2.

- The server supports the extension defined in this document, but it does not have any certificate type in common with the client. Then, the server terminates the session with a fatal alert of type "unsupported_certificate".

- The server supports the extensions defined in this document and has at least one certificate type in common with the client. In this case, the server MUST include the client_certificate_type extension in the Server Hello for TLS 1.2 or in Encrypted Extension for TLS 1.3. Then, the server requests a certificate from the client (via the certificate_request message)

It is worth to mention that the TLS client or server public keys are obtained from a certificate chain from a web page.
5. Certificate Verification

Verification of an IEEE 1609.2/ETSI TS 103097 certificates or certificate chain is described in section 5.5.2 of [IEEE1609.2].

6. Examples

Some of exchanged messages examples are illustrated in Figures 2 and 3.

6.1. TLS Server and TLS Client use the 1609Dot2 Certificate

This section shows an example where the TLS client as well as the TLS server use the IEEE 1609.2 certificate. In consequence, both the server and the client populate the client_certificate_type and server_certificate_type with extension IEEE 1609.2 certificates as mentioned in figure 2.

Client                                           Server

ClientHello,                                      ServerHello,  
  client_certificate_type*=1609Dot2,              {EncryptedExtensions}  
  server_certificate_type*=1609Dot2,             {client_certificate_type*=1609Dot2}  
  -------->                                      {server_certificate_type*=1609Dot2}  
                                                {CertificateRequest*}  
                                                {Certificate*}  
                                                {CertificateVerify*}  
                                                {Finished}  

{Certificate*}                                  <-------- [Application Data*]  
{CertificateVerify*}                             
{Finished}                                       
[Application Data]                              <--------> [Application Data]

Figure 2: TLS Client and TLS Server use the IEEE 1609.2 certificate

6.2. TLS Client uses the IEEE 1609.2 certificate and TLS Server uses the X 509 certificate

This example shows the TLS authentication, where the TLS Client populates the server_certificate_type extension with the X509 certificate and Raw Public Key type as presented in figure 3. the client indicates its ability to receive and to validate an X509 certificate from the server. The server chooses the X509 certificate to make its authentication with the Client.
7. Security Considerations

This section provides an overview of the basic security considerations which need to be taken into account before implementing the necessary security mechanisms. The security considerations described throughout [RFC8446] and [RFC5246] apply here as well.

For security considerations in a vehicular environment, the minimal use of any TLS extensions is recommended such as:

The "client_certificate_type" [IANA value 19] extension who’s purpose was previously described in [RFC7250].

The "server_certificate_type" [IANA value 20] extension who’s purpose was previously described in [RFC7250].

The "SessionTicket" [IANA value 35] extension for session resumption.

In addition, servers SHOULD not support renegotiation [RFC5746] which presented Man-In-The-Middle (MITM) type attacks over the past years for TLS 1.2.

8. Privacy Considerations

For privacy considerations in a vehicular environment the use of EEE 1609.2/ETSI TS 103097 certificate is recommended for many reasons:
In order to address the risk of a personal data leakage, messages exchanged for V2V communications are signed using IEEE 1609.2/ETSI TS 103097 pseudonym certificates.

The purpose of these certificates is to provide privacy relying on geographical and/or temporal validity criteria, and minimizing the exchange of private data.

9. IANA Considerations

Existing IANA references have not been updated yet to point to this document.

IANA is asked to register a new value in the "TLS Certificate Types" registry of Transport Layer Security (TLS) Extensions [TLS-Certificate-Types-Registry], as follows:

- Value: TBD Description: 1609Dot2 Reference: [THIS RFC]

10. Acknowledgements

The authors wish to thank Eric Rescota and Ilari Liusvaara for their feedback and suggestions on improving this document. Thanks are due to Sean Turner for his valuable and detailed comments. Special thanks to William Whyte and Maik Seewald for their guidance and support in the early stages of the draft.

11. References

11.1. Normative References


11.2. Informative References


Appendix A. Co-Authors

- Nancy Cam-Winget
  CISCO, USA
  ncamwing@cisco.com

- Houda Labiod
  Telecom Paristech, France
  houda.labiod@telecom-paristech.fr

- Ahmed Serhrouchni
  Telecom ParisTech
  ahmed.serhrouchni@telecom-paristech.fr

Authors’ Addresses

Panos Kampanakis (editor)
Cisco
USA
EMail: pkampana@cisco.com

Mounira Msahli (editor)
Telecom ParisTech
France
EMail: mounira.msahli@telecom-paristech.fr